DEPARTMENT OF DEFENSE
DIRECTORATE FOR FREEDOM OF INFORMATION AND SECURITY REVIEW
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

Ref: 99-F-0194

26 JAN 1999

Mr. Shoji Fukuyoshi
[redacted]

Dear Mr. Fukuyoshi:

This is in response to your Freedom of Information Act (FOIA) request of August 20, 1998.

The Assistant Secretary of Defense, Special Operations and Low-Intensity Conflict (ASD/SOLIC) has provided the enclosed document as responsive to your request. Some of the information has been withheld because it solely concerns the internal rules and practices contained in a Department of Defense (DoD) Handbook on combating terrorism. Release of this information would risk circumvention of portions of the Handbook by providing insight into the operating procedures integral to reducing the risk and vulnerability of DoD personnel, their family members, facilities, and materiel to acts of terrorism. Consequently, Mr. James Q. Roberts, Principle Director, ASD/SOLIC Policy and Missions Directorate, an Initial Denial Authority, has withheld that information pursuant to 5 USC § 552(b)(2)(High).

You may appeal Mr. Robert's decision to withhold the information by submitting your rationale to reverse the initial decision. Any such appeal should be submitted within 60 days of the date of this letter and mailed to the address on the letterhead above.

The Office of the Secretary of Defense incurred expenses totaling $484.00 in processing your request. Of that amount, $69.75 is assessable to you. Assessable fees consist of 465 reproduced pages at $.15 cents a page.

Please indicate the reference number above and remit a check or money order made payable to the U.S. Treasurer in the amount of **$69.75** within 30 days to this Directorate, at the above

#947

address. Please also note the billing date above since payments received later than 30 days after the billing date may incur additional interest charges.

Sincerely,

A. H. Passarella
Director

Enclosure:
As stated

DoD 0-2000.12-H

DEPARTMENT OF DEFENSE

PROTECTION OF DOD PERSONNEL AND ACTIVITIES AGAINST ACTS OF TERRORISM AND POLITICAL TURBULENCE

FEBRUARY 1993

ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT

FOR OFFICIAL USE ONLY

#947

THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301-2500

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT

February 19, 1993

FOREWORD

This Handbook is reissued under the authority of DoD Directive 0-2000.12, "DoD Combatting Terrorism Program," August 27, 1990. Its purpose is to provide information and suggestions for reducing the risk and vulnerability of DoD personnel, their dependents, facilities, and materiel to acts of terrorism.

DoD O-2000.12–H, "Protection of DoD Personnel Against Terrorist Acts," August 20, 1983, is hereby canceled.

This Handbook applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, and the Defense agencies (hereafter referred to collectively as "the DoD Components").

This Handbook is effective immediately. The suggested protective measures in this Handbook are not established as formal DoD guidance, but should be considered for evaluation and implementation by the DoD Components in executing their responsibilities assigned in DoD Directive O-2000.12. All measures that protect DoD assets from terrorist attack, whether or not they are specifically included in this Handbook, should be implemented consistent with local requirements identified by senior military commanders or civilian managers as appropriate. The DoD Components may use this Handbook to develop briefings and to increase antiterrorism awareness as well as for military education and training programs. DoD Components may issue supplementary instructions. Comprehensive documents that are developed from this Handbook must be protected to prevent their misuse outside the Department of Defense.

Release of this publication is subject to approval by the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict). The National Disclosure Policy shall govern disclosure of this document to foreign governments. Applicable portions of this Handbook may be released to DoD dependents and foreign nationals employed by the Department of Defense to provide them with appropriate guidance on protection measures.

Submit recommended changes through channels to:

Assistant Secretary of Defense
(Special Operations and Low-Intensity Conflict)
The Pentagon
Washington, DC 20301-2500

The DoD Components may obtain copies of this Handbook through their publication channels. Other Federal Agencies may obtain copies from this office.

James R. Locher, III

JAMES R. LOCHER, III
Assistant Secretary of Defense
Special Operations and Low-Intensity Conflict

Page

D. International Terrorist Incidents 4-3
E. Intelligence Gathering 4-4

CHAPTER 5 - TERRORIST THREAT ANALYSIS AND WARNING

A. Introduction and Overview 5-1
B. Threat Analysis Organizations 5-1
C. Terrorist Threat Analysis 5-4
D. Terrorist Threat Level 5-11
E. Changes in Terrorist Threat Level Declarations 5-13
F. Threat Warnings 5-14
G. Terrorist Threat Analysis and Warning: Summary Observations 5-15

CHAPTER 6 - ASSESSMENT OF RISK, VULNERABILITY, AND CRITICALITY

A. Integrated Terrorist Threat Estimates 6-1
B. Risk of Terrorist Attack 6-2
C. Vulnerability Assessments 6-9
D. Criticality Assessments 6-13
E. Use of Integrated Terrorist Threat Estimates 6-15

CHAPTER 7 - PHYSICAL SECURITY SYSTEM CONCEPT

A. Introduction 7-1
B. DoD Physical Security Policy 7-2
C. Summary of Physical Security System Functions 7-7

CHAPTER 8 - PHYSICAL SECURITY SYSTEM COMPONENTS

A. Overview 8-1
B. Layered Security Concept 8-1
C. Physical Security System Functional Requirements 8-4
D. Barriers 8-8
E. Intrusion Detection System (IDS) 8-9
F. Lighting Systems 8-17
G. Threat Delay 8-20
H. Assessment and Incident Response Forces 8-20
I. Summary 8-22

CHAPTER 9 - PHYSICAL SECURITY MEASURES FOR AN INSTALLATION

A. Introduction 9-1
B. Installation and Facility Design 9-1

Page

CHAPTER 14 - HOSTAGE SURVIVAL

A. Introduction 14-1
B. Hostage Survival 14-1
C. The Role of the Family 14-9
D. DoD Code of Conduct 14-11
E. Hostage Survival Summary 14-14

CHAPTER 15 - TERRORISM CRISIS MANAGEMENT PLANNING AND EXECUTION

A. Introduction 15-1
B. Terrorist Incident Crisis Management Planning 15-1
C. Initial Response 15-5
D. Follow-On Response 15-7
E. Terrorist Incident Response: Shared Authorities and Jurisdictions 15-8
F. Special Considerations 15-9
G. Terrorist Incident Crisis Management Summary 15-13

CHAPTER 16 - BOMB THREAT AND BOMB RESPONSE PROCEDURES

A. Introduction 16-1
B. Discovering Bombs 16-1
C. Damage and Casualty Mechanisms 16-1
D. Responding to Bomb and/or Improvised Explosive Device Threats 16-3
E. Evacuation Drills 16-6
F. Incident Control Point (ICP) and Cordon 16-6
G. Discovery of a Suspected IED 16-6
H. Reaction to an Exploded IED 16-6
I. Terrorism and Bomb and/or IED Response Summary 16-8

CHAPTER 17 - DoD TERRORIST THREAT CONDITION SYSTEM

A. Introduction 17-1
B. Environment and Force Readiness Descriptors 17-1
C. Selection of THREATCONS 17-4
D. Random Antiterrorism Measures 17-10
E. Implementation of DoD THREATCONS 17-11

CHAPTER 18 - COMBATTING TERRORISM PRACTICES FOR EXPEDITIONARY AND DEPLOYED FORCES

A. Introduction 18-1
B. Protecting Deployed Forces in High-Risk Areas 18-1
C. Tactical Force Protection 18-10
D. Summary 18-10

FIGURES

Figure	Title	Page
1-1	DoD Combatting Terrorism Program Concept	1-4
2-1	Terrorist Group Leadership, Member, and Support Pyramid	2-3
5-1	DoD-Level Determination of Terrorist Threat Level	5-11
6-1	Physical Security Survey Topics	6-12
7-1	Processing Integrated Terrorist Threat Estimates Into Antiterrorism and Force Protection Programs	7-2
7-2	Physical Security Threat Matrix	7-4
7-3	Resource and Asset Priorities	7-6
8-1	Layered Approach to Protection of DoD Assets	8-2
8-2	High Security Illustration of the Layered Security Concept	8-3
8-3	Security Barrier Functions and Illustrative Examples	8-9
8-4	Exterior IDS Sensor Types	8-11
8-5	Selected Interior Intrusion Detection Sensors	8-13
9-1	Generic Pedestrian Access Control Point	9-19
9-2	Installation of a Sewer Pipe Plug	9-20
9-3	External Installation Surveillance Technologies	9-21
9-4	External Installation Combatting Terrorism Surveillance Functions	9-22
9-5	Waterside Terrorist Surveillance and Engagement Zones	9-27
10-1	Reception Area to Access Controlled Facility	10-11
10-2	Safehaven Concept Implemented in a High-Rise Office Building	10-15
11-1	Door Hardening Techniques	11-10
11-2	Safehaven Concept Including Residence Hall Security Barrier	11-12
12-1	General Approach to Personal Travel Security	12-20
12-2	Indications of Package or Letter Bomb	12-28
14-1	Personal History and/or Information Sheet	14-10
14-2	Code of Conduct	14-12
15-1	Initial Security Force Situation Assessment Criteria at Onset of Criminal or Terrorist Incident	15-5
15-2	DoD Management of Terrorist Incident From Initial Response Through Resolution Phases of Crisis	15-9
15-3	Sample JULLS Report Format	15-12

REFERENCES

(a) DoD Directive O-2000.12, "DoD Combatting Terrorism Program," August 27, 1990

(b) DoD Handbook 2000.12-H, "Protection of DoD Personnel Against Terrorist Acts," authorized by DoD Directive O-2000.12, April 1983 (hereby canceled)

(c) Section 1072 (2) of title 10, United States Code

(d) "Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field," dated at Geneva, August 12, 1949, in United States Treaties and International Acts Serial 3362, February 2, 1956

(e) "Convention for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea," dated at Geneva, August 12, 1949, in United States Treaties and International Acts Serial 3363, February 2, 1956

(f) "Convention Relative to the Treatment of Prisoners of War," dated at Geneva, August 12, 1949, in United States Treaties and International Acts Serial 3364, February 2, 1956

(g) "Conventional Relative to the Protection of Civilian Persons in Time of War," dated August 12, 1949, in United States Treaties and International Acts Serial 3365, February 2, 1956

(h) Section 1385 of title 18, United States Code, "The Posse Comitatus Act"

(i) Section 333 of title 10, United States Code

(j) DoD Directive 3025.12, "Employment of Military Resources in the Event of Civil Disturbances," August 19, 1971

(k) Sections 231 and 1361 of title 18, United States Code

(l) Section 797 of title 50, United States Code

(m) Section 3056 of title 18, United States Code

(n) Section 1989 of title 42, United States Code

(o) Section 373[b] of title 21, United States Code

(p) Section 1362 of title 33, United States Code

(q) Section 351[g] of title 18, United States Code

(r) Sections 4401 through 4484 of title 42, United States Code

(s) Section 1855 of title 42, United States Code

(t) Public Law 98-473, "Comprehensive Crime Control Act of 1984," October 12, 1984

(u) Public Law 99-399, "Omnibus Diplomatic Security and Antiterrorism Act of 1986," August 27, 1986

(v) Public Law 98-151, "International Security and Development Assistance Authorizations Act of 1983," November 14, 1983

(w) Public Law 99-83, "International Security Assistance Act ," August 8, 1985

(x) Public Law 101-222, "Anti-Terrorism and Arms Export Amendments Act of 1989," December 12, 1989

(y) Public Law 99-83, "International Security and Development Cooperation Act of 1985 as Amended," August 8, 1985

(z) DoD Directive 5525.7, "Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes," January 22, 1985 (pp. 1-1 through 1-12)

(aa) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 25, 1988

(bb) DoD Directive 5160.54, "DoD Key Assets Protection Program (KAPP)," June 26, 1989

DEFINITIONS

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

2. **AT Awareness.** Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorist acts.

3. **AT Resident Training.** Formal classroom instruction in designated DoD courses that provide specialized instruction on specific combatting terrorism topics; i.e., personal protection, terrorism analysis, regional interest, and AT planning.

4. **Combatting Terrorism.** Actions, include AT and CT, taken to oppose terrorism throughout the entire threat spectrum.

5. **Counterterrorism (CT).** Offensive measures taken to prevent, deter, and respond to terrorism.

6. **DoD-Designated High-physical Threat Countries.** Geographic areas determined to be of significant terrorist threat to DoD travelers, as designated by the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) in coordination with the Assistant Secretary of Defense (International Security Affairs), the Assistant Secretary of Defense (International Security Policy), and the Deputy Under Secretary of Defense (Strategy and Resources).

7. **Domestic Terrorism.** Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

8. **Family Member.** Individuals defined as "dependent" in Section 1072(2) of 10 U.S.C (reference (c)) including spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (under 21, incapable of self support or under 23 and enrolled in a full-time institution).

9. **High-Risk Billet.** Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

10. **High-Risk Personnel.** U.S. personnel and their family members whose grade, assignment, travel itinerary, or symbolic value may make them an especially attractive or accessible terrorist target.

11. **High-Risk Target.** U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target.

12. **International (or Transnational) Terrorism.** Terrorism in which planning and execution of the terrorist act transcends national boundaries. In defining international terrorism, the purpose of the act, the nationalities of the victims, or the resolution of the incident are considered. Those acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists.

ABBREVIATIONS AND ACRONYMS

AFOSI	Air Force Office of Special Investigations
AIQC	Antiterrorist Instructor Qualification Course
ANO	Abu Nidal Organization
ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
AT	Antiterrorism
ATCC	Antiterrorism Coordinating Committee
ATF	Bureau of Alcohol, Tobacco, and Firearms, Treasury Department
BAF	backup alert force
C^3I	command, control, communications and intelligence
CCB	Community Counterterrorism Board
CCTV	closed circuit television
CIA	Central Intelligence Agency
CID	Criminal Investigation Division
CINC	Commander in Chief of a Unified or Specified Command
CINCENT	Commander in Chief, Central Command
CINCEUR	Commander in Chief, European Command
CINCFOR	Commander in Chief, Forces Command
CINCLANT	Commander in Chief, Atlantic Command
CINCPAC	Commander in Chief, Pacific Command
CINCSOC	Commander in Chief, Special Operations Command
CINCSOUTH	Commander in Chief, Southern Command
CINCSPACE	Commander in Chief, Space Command
CINCSTRAT	Commander in Chief, Strategic Command
CINCTRANS	Commander in Chief, U.S. Transportation Command
COMSEC	communications security
CONUS	Continental United States
CO	Contracting Officer
COTR	Contracting Officer's Technical Representative
CRAF	Civil Air Reserve Fleet
CTJTF	Counterterrorism Joint Task Force
DIA	Defense Intelligence Agency
DEA	Drug Enforcement Agency
DEFCON	Defense Readiness Condition
DIW	dead in the water
DIWS	Defense Indications and Warning System
DoD	Department of Defense
DoE	Department of Energy
DoJ	Department of Justice
DoS	Department of State
EEI	essential elements of information
EEFI	essential elements of friendly information
ELN	National Liberation Army, Colombia
EMI	electromagnetic interference
EOD	explosive ordnance disposal
ETA	estimated time of arrival

PAO	public affairs officer
PCC	Policy Coordination Committee
PHOTINT	photographic intelligence
PIRA	Provisional Irish Republican Army
PLFP	Popular Front for the Liberation of Palestine
PLFP-GC	Popular Front for the Liberation of Palestine—General Command
PMO	provost marshal office
POV	privately owned vehicle
PSD	protective security details
RDT&E	Research, Development, Test, and Engineering
RF	reserve force
ROE	rules of engagement
SAC	Special Agent in Charge
SAT	security alert team
SDF	self defense force
SDV	swimmer delivery vehicle
SIGINT	signals intelligence
SJA	staff judge advocate
SOP	standing/standard operating procedure
SOFA	Status of Forces Agreement
SRT	special reaction team
STARC	State Army National Guard Area Command
TAD	temporary additional duty
TDY	temporary duty
THREATCON	terrorist threat conditions
TRANSCOM	U.S. Transportation Command
TRB	tactical response boat
U.S.	United States
USA	United States Army
USACIDC	United States Army Criminal Investigations Command
USAJFKSWC	United States Army J.F. Kennedy Special Warfare School
USAMPS	United States Army Military Police School
USAF	United States Air Force
USCG	United States Coast Guard
USMC	United States Marine Corps
USN	United States Navy
VIP	very important person

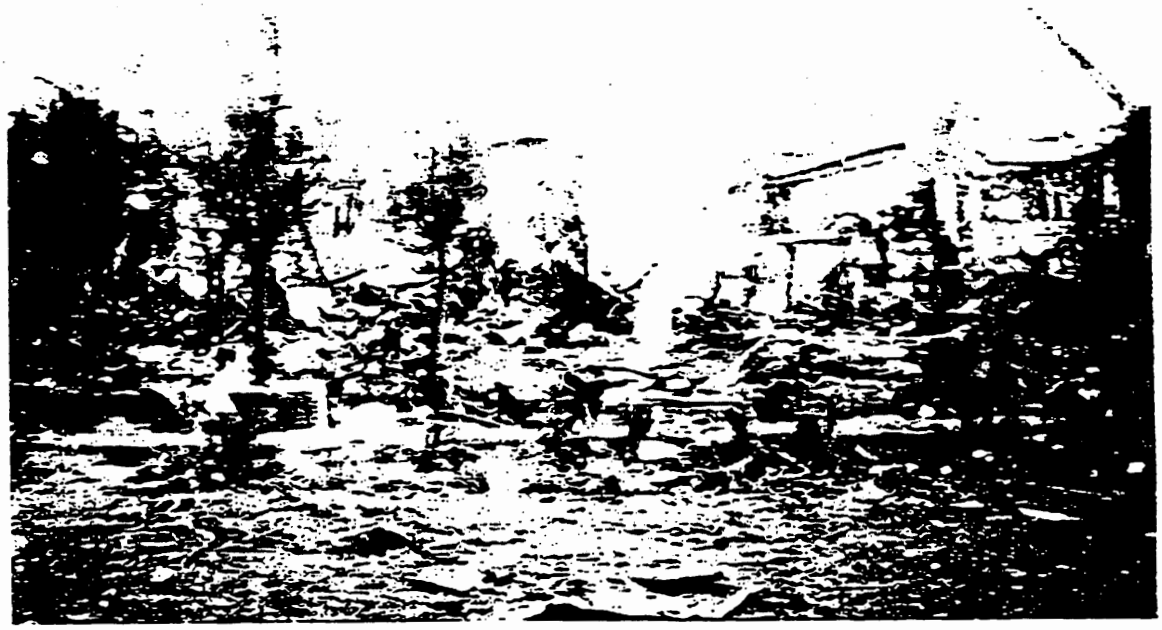
CHAPTER 1

THE DoD ANTITERRORISM HANDBOOK

A. INTRODUCTION

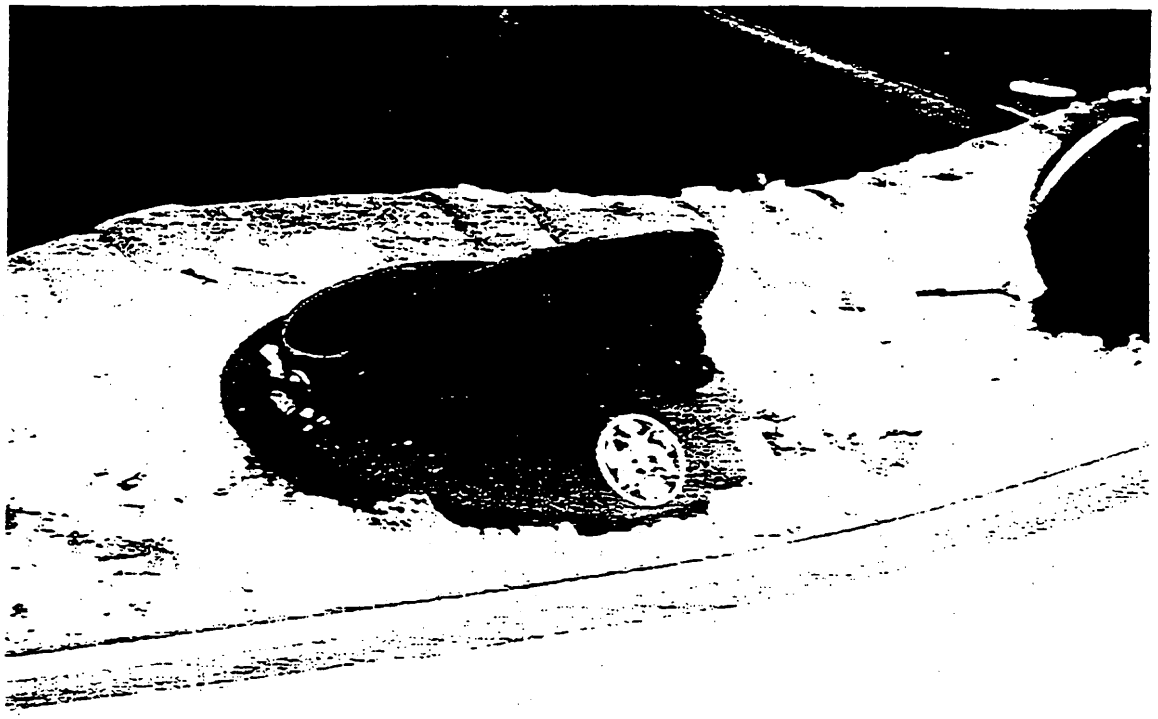
1. DoD personnel, facilities, and materiel have been targeted for attack. Criminal attacks on DoD personnel by individuals and organizations operating outside the formal command and control structure of national governments have claimed nearly 300 DoD-affiliated personnel dead and more than 200 injured in the past twenty years.

2. The destruction of U.S. Marine Headquarters at the Beirut International Airport in October 1983 was the single greatest loss of American military personnel attributed to a single terrorist act. But other attacks could have had caused more casualties and had even more serious consequences for the ability of the DoD to carry out its assigned roles and missions.



U.S. Marine Headquarters in Beirut, Lebanon, was destroyed by a truck bomb in late October 1983

representatives abroad. They are symbols of the U.S. Government. They become terrorist targets as a means of promoting change.



Remains of a private vehicle destroyed in the car bomb attack at Ramstein Air Base, August 1985

8. According to DoD Directive O-2000.12 (reference (a)):

"It is DoD Policy:

1. To protect DoD personnel and their families, facilities, and other material resources from terrorists acts. . . .

2. To facilitate inter-Service coordination and support of U.S. Government antiterrorist activities."

9. This DoD Antiterrorism Handbook is part of a larger set of efforts to implement DoD antiterrorism policy.

B. DoD AT HANDBOOK PURPOSES

1. The DoD Antiterrorism Handbook has been prepared to serve as a reference document for all DoD Components. The Handbook contains material to support the development of antiterrorism awareness, education, and training activities by all DoD components. It contains information that can be used to form the foundation of individual, family, installation, and unit antiterrorism efforts.

2. Used in conjunction with other DoD, Service, Defense Agency, and Joint Publications, this DoD Antiterrorism Handbook can assist in the development of

education and training of personnel in preventive measures; and develop plans and programs to prevent, respond, contain, and resolve terrorist incidents should they occur. There is also a reactive phase in which crisis management plans are implemented and terrorist incidents resolved.

D. ANTITERRORISM AND FORCE PROTECTION

1. The term "antiterrorism" includes those "defensive measures used to reduce the vulnerability of individuals and property to terrorism, . . . to include limited response and containment by local military forces."

2. The term "counterterrorism" involves those "offensive measures taken to prevent, deter, and respond to terrorism." Sensitive and compartmented programs of counter-terrorism are addressed in relevant National Security Decision Directives (NSDDs), National Security Directives (NSDs), contingency plans, and other relevant classified documents.

3. The distinctions between antiterrorism and counterterrorism are approximately analogous to the distinctions between preventive and acute medicine. Preventive medicine including annual physicals, inoculations, and periodic checkups is intended to reduce the likelihood of becoming ill and mitigating the effects of illness should it occur. Acute medicine brings specialized medical resources to a disease, to contain and cure the disease, sometimes to include invasive procedures such as surgery.

4. The DoD Combatting Terrorism Program (antiterrorism) seeks to reduce the likelihood that DoD-affiliated personnel, facilities, and materiel will be attacked, and to mitigate the effects of such attacks should they occur. Antiterrorism, as discussed throughout this Handbook, is an element of a broader concept called force protection. The term "force protection" consists of active and passive measures designed to deter and defeat threats directed toward military service members, their family members, DoD civilians and the facilities and equipment which support them in the execution of operations.

5. The DoD network of people, facilities, and materiel resources span the globe. As a consequence of this far flung distribution of resources, there are an infinite number of circumstances that can occur resulting in some diminution of DoD Components' capability to carry out assigned missions and responsibilities. Natural disasters can degrade DoD capabilities and performance. Common street crime can be equally damaging to the maintenance of readiness and capability.

6. Force protection concepts must take into account all of these potential threats to readiness and capability. Theft and damage to property motivated by greed, acts of espionage, or acts of sabotage, can be equally effective in terms of limiting or reducing DoD capabilities. Self protection measures are an integral part of force protection. People are important "assets," just as are facilities, equipment, and information.

7. Department of Defense antiterrorism efforts build on the foundation of physical security, crime prevention, industrial health, safety, and hygiene programs, and military and civil construction programs. These efforts are designed to reduce a broad range of physical dangers faced by DoD-affiliated personnel. The terrorist threat is a significant danger, and a danger that many DoD force protection initiatives can mitigate.

forces unable to perform because of training accidents, natural disasters, or loss of key assets due to common street crime. DoD efforts to preserve forces are motivated by the need to ensure that the requirements of the combatant commanders can be met at all times.

2. Force protection efforts and antiterrorism programs conducted by all DoD Components are closely related. Each program, including activities undertaken in the defense industrial base, seeks to ensure the ability of DoD Components to carry out all missions and assignments directed by the National Command Authority. Changes in force posture make protection and preservation of existing forces and their supporting industrial infrastructure especially important.

3. This Handbook is intended to be a reference document. Its publication is intended to provide further information that can assist DoD Components in designing, developing, implementing, and evaluating effective programs to reduce the risk of terrorist attack and mitigate its effects should it occur.

CHAPTER 2

CHARACTERISTICS OF TERRORISM

A. DEFINITIONS

1. The term, "terrorism" has yet to be given a universally accepted definition. The Federal Bureau of Investigation (FBI) defines terrorism as:

> . . . the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.[1]

2. The U.S. Department of State (DoS) defines terrorism in a slightly different way:

> . . . "terrorism" [is] premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine state agents, usually intended to influence an audience. "International terrorism" is terrorism involving the citizens or territory of more than one country.[2]

3. The following definition is used by the Department of Defense:

> The calculated use of violence or threat of violence to inculcate fear; intended to coerce or try to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.[3]

4. The definitions of terrorism used by U.S. Government Departments and Agencies are applicable to all forms of political violence.[4] Although this Handbook uses the DoD definition of terrorism throughout, it is important to remember that the DoD definition subsumes both definitions used by the FBI and the DoS. There is no portion of the U.S. Code which makes "terrorism" a crime. However, it is unlawful to use violence or the threat of violence against officers and employees of the United States government, their contractors, or their dependents, as well as U.S. Government property for any purpose. Hence acts of political violence committed against DoD personnel, facilities, and materiel are criminal acts.

---

1 Federal Bureau of Investigation, *Terrorism in the United States* (Washington, D.C.: U.S. Department of Justice, 1990), p. 25.

2 U.S. Department of State, *Patterns of Global Terrorism, 1989* (Washington, D.C.: U.S. Department of State, 1990), p. v.

3 DoD Directive O-2000.12 (reference (a)).

4 David E. Long, *The Anatomy of Terrorism* (New York: Free Press, 1990), pp. 3-5. Mr. Long was, at the time of publication, on loan to the National Defense University from his position as a Foreign Service Officer.

(2) Terrorist groups are by no means invincible. 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 can cause terrorist groups to splinter into new faction(s); e.g., the splintering of the Popular Front for the Liberation of Palestine (PFLP) into the PFLP and the Popular Front for the Liberation of Palestine--General Command (PFLP-GC).

(3) Proliferation of terrorist groups can aid efforts by security forces to apprehend terrorists and bring about the end of a siege of terror[redacted]

c. Terrorist Support Structures

(1) In a broader context, terrorist organizations, especially those with little or no access to government resources, need a support structure. As shown in Figure 2-1, a typical organization consists of operational members who may be functionally organized as outlined below, and several categories of supporters.

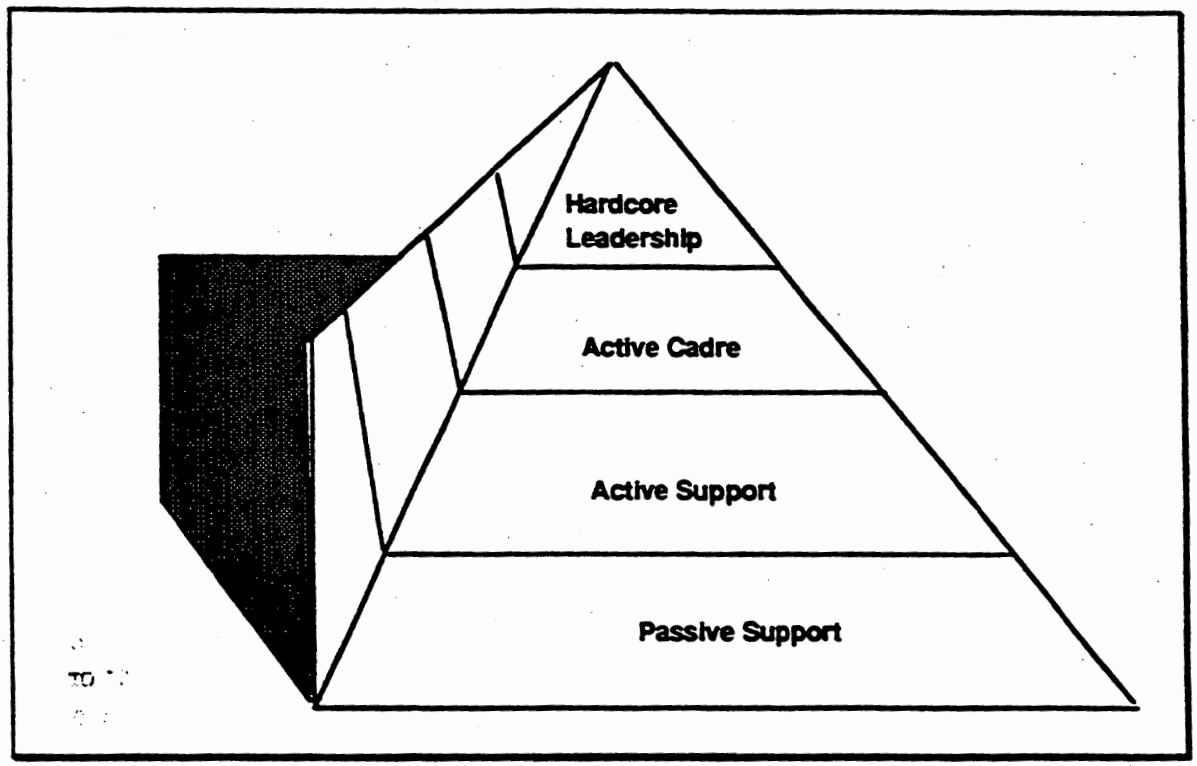


Figure 2-1. Terrorist Group Leadership, Member, and Support Pyramid

(2) At the top of the pyramid is the terrorist group Hardcore Leadership which 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, then the leadership will include one or more members who may have had extensive training or education by the sponsoring state.

(3) Beneath the Hardcore Leadership is the Active Cadre. This membership cadre comprises the "soldiers" of the terrorist group. These are the individuals who build and deliver bombs, commit armed assaults, and take other criminal actions. The active cadre may include individuals who are deranged, sociopaths, or psychopaths. While "crazies" may from time to time achieve notoriety and prominence within a terrorist group, their unstable and idiosyncratic behavior usually prevents them from achieving and sustaining themselves in a leadership role for a long period. It does not, however, prevent them from splintering away from a terrorist group and starting their own group.

(4) Beneath the Active Cadre is a layer of active support. Individuals in this layer may not consider themselves to be members of a terrorist group. They do, however, provide money and other resources to causes which, if not outright fronts for, are closely linked to terrorist groups. They may provide logistical or technical assistance to the terrorist group. They may even play minor, relatively safe roles in terrorist operations, such as acting as a tail or a spotter during a targeting effort.

(5) Finally, the lowest layer of the pyramid includes passive supporters of a terrorist group. This layer includes individuals who acknowledge the presence of terrorist group members or the presence of terrorist group activity in their homes, the neighborhoods, their place of business, or other locations and actively choose to ignore such activities. Passive supporters of terrorist groups "look the other way" so that they do not have to acknowledge their role or complicity in the consequences of a terrorist attack.

(6) As depicted in Figure 2-1 and as observed above, there are many types of individuals who join terrorist groups and organizations or otherwise lend their support to such causes.

C. CHARACTERISTICS OF TERRORIST GROUPS

1. Leadership

Leadership of terrorist organizations is as diverse as the organizations themselves. Although the popular image of terrorists in the media is one of a deranged, almost criminally-psychotic personality, most profiles of terrorists indicate that terrorists and their leaders are generally politically motivated, fairly well-educated, and usually from middle-class backgrounds.[5] Leaders of terrorist organizations are often quite charismatic, and often have extensive background and training in military tactics and planning. Terrorists engage in armed activity, but their leaders are not usually similar to hard-core criminals.

---

5 See Michael Stohl, "Demystifying the Mystery of International Terrorism," published in Charles W. Kegley, Jr., Ed., *International Terrorism: Characteristics, Causes, Controls* (New York: St. Martins Press, 1990), pp. 81-96. See also Charles A. Russell and Bowman H. Miller, "Portrait of a Terrorist," in Lawrence Freedman and Yonah Alexander, Eds., *Perspectives on Terrorism* (Wilmington, Del.: Scholarly Resources, 1983), pp. 45-60.

2. Recruitment

Terrorists are generally recruited at a relatively young age--late teens and early twenties--although those with special skills and training are sought continuously. Those who join terrorist organizations often have highly ambitious goals that they have failed to meet. Or they may be highly idealistic and have been affected by an event that substantiated their political beliefs. This leaves them susceptible to the "pitch" of their recruiter, and increases the chances of their joining the organization.

3. Training

a. Terrorists groups, like other formal organizations, conduct training programs. Although these training programs vary considerably from one terrorist group to another, such programs seem to share some common threads.

b. Terrorists generally learn how to use small arms with minimal if not outstanding proficiency. In some instances, the small arms available to terrorists will be equivalent to or even better than those of many military forces around the world. Some terrorist groups have expanded their training syllabi to include man-portable anti-tank and anti-aircraft weapons. Such weapons are obtained either as the result of thefts, illicit sales, or overt sales diverted to the terrorist organizations by sympathizers.

c. Terrorists have also been given rigorous instruction in the design and use of explosive devices. Depending on the degree of governmental support available, the syllabi have included the use of substances ranging from common grocery store and hardware store chemicals, to military-type explosives including **plastique**.

d. Terrorists are also given instruction in intelligence collection and analysis, including observations, tracking and trailing, cryptography, communications interception, signals interception, and surreptitious entry into and exits from structures, compounds, and vehicles.

e. The quality of training varies significantly from one terrorist group to another. A very large factor in determining the quality of training is the degree to which a terrorist group is operating with the knowledge and support of a foreign government. Those terrorist groups that were supported by the eastern European intelligence services in the 1970s and 1980s appeared to be the best trained.

4. Intelligence Collection and Analysis

a. Terrorist groups frequently establish dedicated intelligence organizations. The mission of these organizations is to collect as much information as possible regarding the activities of potential targets, to aid in the identification of specific targets, to aid terrorist leaders in the assessment of effective and ineffective tactics, and to provide a post attack assessment of actions.

b. Intelligence gathering for terrorist organizations varies in sophistication and quality from group to group. Most well-funded terrorist organizations are able to buy or coerce informants with information regarding law enforcement efforts, airline passenger lists, schedules of events, etc. This is particularly easy in countries with plentiful sources of open information like the United States.

c. Target selection for terrorist incidents results from evaluation of a number of variables. Targets are usually selected for a terrorist event because of the potential for:

(1) Generating large-scale media coverage.

(2) Damaging or destroying an asset of value to an adversary.

(3) Forcing or coercing political negotiations for the group's war or current cause.

(4) Assassinating a key political, military, or other figure.

(5) Enhancing the reputation or credibility of the group.

[redacted]

6. Counterintelligence

a. Terrorists operate very effective counterintelligence organizations on their own behalf. Sometimes, they are able to obtain assistance from government police and intelligence services, either through use of bribes or coercion, or because they find a sympathizer who agrees to provide information about government counterterrorism and law enforcement activities. Terrorists have also demonstrated considerable sophistication in the acquisition and use of communications intelligence equipment. There have been press reports on terrorist incidents in Europe and the Middle East suggesting that terrorists used police and aircraft radio frequency scanners during their attacks.

b. Terrorist groups have demonstrated ruthless behavior towards individuals thought to be informers or police agents. At times, terrorists torture and then murder alleged informers outright. In other instances, however, terrorists manipulate alleged informers, effectively turning them into double agents providing law enforcement services with false, misleading, and deceptive information.

7. Deployment

a. Terrorist groups deploy against targets using any and all means of transportation and documentation. In the 1970s and 1980s, it was quite common for terrorists to travel on genuine passports issued in the pseudonyms of terrorists. During the late 1980s and 1990s, it appears that terrorists relied more frequently on bogus passports or other travel documents.

b. Stolen and forged airline and passenger ship and/or ferry tickets are other examples of travel documents in high terrorist demand. The huge volume of international travel makes the control of such documents difficult at best. Even if ticket blanks are lost or stolen, reporting the loss or theft to law enforcement, insurance companies or other authorities is slow, cumbersome, and expensive. It is not surprising that many thefts of these travel documents are simply ignored.

c. International terrorists operating in Europe appear to have gained substantial freedom of movement as a result of Europe's political integration. European borders are becoming increasingly porous, much as the borders between the individual states in the United States are today. As a result, the requirement for border checks, display of proper identification, and the opportunity to detect the international transport of weapons and/or explosives has diminished.

d. Even though the ability of terrorists to move from one locale to another may be less inhibited by international travel restrictions, terrorists remain very careful and alert. Vehicles used by terrorists often contain hidden compartments in which contraband is concealed. Weapons are often transported in pieces, and improvised explosive devices are oftentimes shipped from the "manufacturer" to the "user" in multiple shipments.

e. Due to the surreptitious nature of terrorist attacks, movement of terrorists from a training or staging area to their target location is often a slow process requiring much support. Safehouses, for last minute communication of plans, intelligence on the target and escape routes, multiple vehicles, and exhaustive trails of false papers are expensive, take much time to assemble, and must be carefully husbanded as scarce resources. The clandestine nature of terrorist activity, especially movement to the attack site, is a potential vulnerability which can be exploited by law enforcement authorities.

8. Types of Terrorist Attacks

a. Common to every definition of terrorism is violent activity. Terrorist organizations resort to various violence to generate publicity, incite fear and achieve political goals. [redacted]

b. Although the world today appears to be more peaceful than in recent years, the threat of terrorism remains real. Therefore, it is important to remain vigilant against the violent acts of terrorism described below.

[redacted]

[redacted]

[redacted]

6 Federal Bureau of Investigation, *Terrorism in the United States, 1989* (Washington, D.C.: U.S. Department of Justice, 1990), p. 21-22.

7 U.S. Department of State, *Significant Incidents of Political Violence Against Americans, 1990* (Washington, D.C.: U.S. Department of State, 1991), p. 3.

[redacted]

D. TERRORIST GROUPS

1. For several years security forces categorized terrorist groups according to their operational traditions--national, transnational, and international.

2. 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 from a foreign government. Ease of international travel and the growing tendency toward cooperative efforts among terrorist groups have rendered these categories of little operational use.

3. Terrorist groups are categorized by government affiliation to help security planners anticipate terrorist targets and their sophistication of intelligence and weaponry. The three general terrorism categories that have gained acceptance are:

a. Non-State Supported

A terrorist group that operates autonomously, receiving no significant support from any government [redacted] While such groups may be difficult to detect, control, and eradicate, they operate without many of the advantages afforded to the other categories of terrorist groups.

b. State-Supported

(1) A terrorist group that generally operates independently but receives support from one or more governments; [redacted] State-supported terrorist groups in the past received a wide range of assistance from their patrons. Such assistance has run the gamut from state-supported training facilities including special warfare instruction by military or intelligence service instructors, sanctuaries approaching resort-like accommodations, logistics and medical

support, intelligence support, and direct financial aid, to as little as sanctuary acknowledged by the state with strict limitations imposed on terrorist group activity while in the sanctuary.

(2) The degree of state-support for terrorist activities emanating from its territory has been used by the Department of State as one of the criteria to determine whether or not a government qualified as a "State Sponsor of Terrorism." States so designated risk loss of trade as well as economic and security assistance from the United States Government, as well as such embarrassment or worse resulting from being labeled a "State Sponsor of Terrorism."

c. State-Directed

(1) In the 1980s and early 1990s, there appears to have been an escalation in the conflict between terrorists on the one hand and governments on the other. In several instances, most notably in the Middle East, certain states were going beyond the provision of support to terrorist groups and were actively engaged in the organization and direction of terrorist activities. Libya, Iraq, and North Korea have been publicly identified as states that have furnished leadership and direction to terrorist groups.

(2) State direction of a terrorist group can change the character of terrorist organizations and activities. It can bring about a much more disciplined, military-like organization, resulting in even better planning and execution of terrorist acts. State direction of terrorist groups often appears to result in an increase in terrorist "fire-power," intelligence collection and analysis capabilities, logistics support, and level of competence in murder, kidnap, hostage taking, and destruction of property.

(3) State direction of terrorist activities can have serious, adverse consequences for both terrorists and their sponsors. Following the bombing of a nightclub in Berlin which was determined to have been the work of state-directed Libyan terrorists, the United States retaliated against Libya. In the subsequent military attack, Libyan government buildings were severely damaged, and the Libyan leader, Muammar Qadhafi suffered the personal loss of a child when his family home was bombed.

(4) State direction of terrorist activity sits on the border between intolerable international criminal activity and initiation of clandestine military activities tantamount to a state of war. International response to the Libyan bombing of the Berlin nightclub and the general lack of opposition to American military retaliation against this terrorist act appears to have been duly noted by other states accused of similar sponsorship and direction of terrorist organizations.

E. SUMMARY

1. Terrorism is characterized as the unlawful use of violence or threat of violence to coerce or intimidate a government or a society. DoD personnel, facilities, and materiel have been victimized by terrorist attacks at home and abroad. They have been selected for criminal attack because they are obvious symbols of the U.S. Government.

2. Terrorist groups are led by rational, calculating leaders. These leaders have well defined goals and objectives. Terrorist tactics are employed as part of their politico-military strategy to achieve these goals and objectives. While active members of terrorist groups

may include individuals who are unbalanced, unstable, or "crazy," it is dangerously incorrect to assume that terrorist groups generally and terrorist leadership cadres in particular are irrational or psychotic. Terrorist attacks can usually be understood as rational so long as the values that define rational in a particular culture are understood.

3. Terrorist groups organize themselves along military lines and develop functional specialists. Many terrorist groups are well disciplined. They carry out their attacks with military-style precision.

4. The U.S. Government has a well articulated policy and implementing strategy to combat terrorism in all of its forms. This is discussed in the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 3

U.S. GOVERNMENT POLICY, STRATEGY, AND ORGANIZATION TO COMBAT TERRORISM

A. GENERAL U.S. GOVERNMENT POLICY

1. The U.S. Government's general policy on terrorism is clear and unambiguous:

a. The U.S. Government is opposed to domestic and international terrorism and is prepared to act in concert with other nations or unilaterally when necessary to prevent or respond to terrorist acts.

b. The U.S. Government considers the practice of terrorism by any person or group a potential threat to its national security and will resist the use of terrorism by all legal means available.

c. States that practice terrorism or actively support it will not do so without consequence. If there is evidence that a state is mounting or intends to conduct an act of terrorism against this country, the United States will take measures to protect its citizens, property and interests.

d. The U.S. Government will make no concessions to terrorists. It will not pay ransoms, release prisoners, change its policies or agree to other acts that might encourage additional terrorism. At the same time, the United States will use every available resource to gain the safe return of American citizens who are held hostage by terrorists.

e. The United States will act in a strong manner against terrorists without surrendering basic freedoms or endangering democratic principles, and will encourage other governments to take similar stands.[1]

2. This clear statement of policy buttressed by statute lays the foundation for an implementation strategy.

B. U.S. GOVERNMENT STRATEGY FOR COMBATTING TERRORISM

1. The basic strategy employed by the U.S. Government to combat terrorism is to encourage all nations to band together and give no sanctuary to terrorists. The strategy has several elements:

a. International exchange of information and intelligence on terrorists;

---

1 *Report of the Vice-President's Task Force on Combatting Terrorism* (Washington, D.C.: U.S. Government Printing Office, February, 1986).

b. Collective efforts to improve law enforcement organizations' effectiveness in the apprehension and prosecution of terrorists;

c. Bilateral and multilateral efforts to improve aviation and maritime security;

d. Bilateral exchanges of terrorist experts and "cross-training" of counterterrorist units;

e. Support of antiterrorism training for law enforcement and internal security forces; and

f. International cooperation in research and development for new equipment to counter existing and potential terrorist capabilities;

2. The U.S. Government has vigorously pursued the arrest and extradition of those individuals alleged to have committed acts of violence against Americans. If extradition has not been forthcoming, the government has lobbied for prosecution in foreign courts for violation of local laws.

3. For example, following the execution of Navy Petty Officer Robert Stethem, the U.S. Government sought to extradite his alleged murderer, Mohammad Hammadi from Germany. Instead, the German government elected to prosecute Hammadi. Upon conviction, he was sentenced to life imprisonment.

4. On November 14, 1991, the Department of Justice returned indictments against two Libyan nationals for their alleged role in the manufacture and insertion of an explosive device into the baggage compartment of Pan American Airways Flight 103. The aircraft was destroyed over Lockerbie, Scotland, on December 21, 1988, with the death of 259 persons on the aircraft and 11 persons on the ground.

5. Throughout the first half of 1992, the governments of the United States and the United Kingdom applied diplomatic pressure to the government of Libya seeking the extradition of two Libyan nationals. Following unsuccessful discussions with the Libyan Government, the United States and the United Kingdom took the matter to the United Nations. The U.N. Security Council adopted a resolution authorizing the application of international economic sanctions against Libya until the two alleged terrorists were extradited either to the United Kingdom or to the United States to stand trial for their roles in the murder of Pan Am Flight 103 passengers and crew and the residents of Lockerbie, Scotland.

6. There are instances, however, when bilateral and multilateral diplomacy is ineffective. In those cases, the United States Government has made clear its intention to act unilaterally to apprehend individuals accused of having attacked or killed American citizens abroad. The clearest, most dramatic example of the U.S. Government's willingness to take extraordinary measures grew out of a 1985 incident.

7. On June 11, 1985, Royal Jordanian Alia Airlines Flight 402 was hijacked en route from Beirut, Lebanon, to Amman, Jordan. Several U.S. nationals were held hostage during this incident. One of the alleged hijackers was Fawaz Younis. Younis was allegedly a member of Amal, a Beirut, Lebanon, based religious-political organization whose members have engaged in acts of terrorism.

8. Based on a Federal warrant issued on June 11, 1985, Younis was arrested by the FBI in international waters in the Mediterranean Sea on September 13, 1987. On March 14, 1989, Fawaz Younis was convicted of conspiracy, hostage taking, and air piracy. Younis' arrest marked the first time an individual has been returned to the United States to face charges for violating an extraterritorial statute, Title 18, United States Code Section 1203 (Hostage Taking).[2]

9. Thus the general strategy by which the U.S. Government implements its opposition to terrorism is the following:

a. Deny sanctuary to terrorists;

b. Encourage the growth and development of international opposition to terrorism;

c. Impose through multilateral, bilateral, or unilateral action appropriate costs on states which support or direct international terrorist activity; and

d. Retain the right and exercise capabilities to seek out and apprehend on a unilateral basis those individuals who commit politically motivated, criminal acts against American citizens if bilateral or multilateral efforts to obtain custody over such individuals is unsuccessful.

10. To carry out U.S. Government policy and implement the broad strategy outlined here, a significant U.S. Government-wide structure has been developed.

C. U.S. GOVERNMENT COMBATTING TERRORISM STRUCTURE

The U.S. Government has developed a formal structure to provide policy guidance and programmatic coordination of efforts to combat terrorism both at home and abroad.

1. Participating Agencies and Departments

[redacted]

2 Federal Bureau of Investigation, *Terrorism in the United States, 1989* (Washington, D.C.: U.S. Department of Justice, 1990), p. 6.

[redacted]

[redacted]

[redacted]

[redacted]

FOR OFFICIAL USE ONLY

[redacted]

[redacted]

F. CHAPTER SUMMARY

1. The U.S. Government has a clear, well-defined policy on terrorism: terrorist acts are criminal acts of violence perpetrated to arouse fear and intimidate persons or governments. They are intolerable, and the U.S. Government will vigorously oppose efforts to cause changes in policy espoused by terrorist means. The U.S. Government will join all other governments in the pursuit of perpetrators of politically motivated violence, and shall employ all lawful means to apprehend, detain, prosecute and punish those convicted of such acts.

2. The U.S. Government has a three pronged strategy to implement this policy. The government works on a multilateral and bilateral basis to deny sanctuary to terrorists. It seeks either to extradite alleged terrorists to the United States for trial on violations of U.S. criminal code or to have foreign governments try alleged terrorists under similar, appropriate laws. It seeks international cooperation to bring informal or formal sanctions against those states which provide support or direction to terrorist groups. Finally, the U.S. Government reserves the right to take direct action against states that support or direct terrorist acts against American citizens and to extradite alleged perpetrators without their cooperation or consent to stand trial in American courts for attacks on American citizens.

3. The U.S. Government has an effective interdepartmental structure involving representatives of all appropriate departments and agencies to coordinate information, promote research and development, and provide technical, logistic, and operational support for domestic and international antiterrorism and counterterrorism efforts.

4. In the following chapter, the legal basis for and boundaries of the DoD Combatting Terrorism Program are outlined.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4

THE DoD COMBATTING TERRORISM PROGRAM: LEGAL AND REGULATORY GUIDELINES

A. REFERENCES

1. DoD Directive 2000.12, DoD Combatting Terrorism Program, August 27, 1990.

2. DoD Directive 5200.8, Security of DoD Installations and Resources, April 25, 1991.

3. DoD Directive 5525.5, DoD Cooperation with Civilian Law Enforcement Officials, January 15, 1986.

4. DoD Directive 3025.12, Employment of Military Resources in the Event of Civil Disturbances, August 19, 1971.

5. 50 U.S. Code Section 797.

6. 18 U.S. Code Section 1382.

B. GENERAL

1. This chapter will briefly outline pertinent DoD authority to combat terrorism. This material is intended only to build a general framework to guide the development of plans, programs, training, and activities to combat terrorism during peacetime to ensure that DoD components comply fully with statutes, directives, and regulations. It is intended only as an introduction. Policy makers and operational commanders should seek additional information and guidance from higher headquarters and servicing legal advisors.

2. A lead agency is designated for coordinating U.S. Government actions to resolve terrorist incidents (ref. 1, para 3-1A). [redacted]

C. DOMESTIC TERRORIST INCIDENTS

1. **On-installation incidents.** [redacted] installation commanders have inherent authority to take reasonably necessary and lawful measures to maintain law and order on installations and to protect military personnel, facilities, and property (ref. 2, para C). This authority also includes the removal from or the denial of access to an installation or site of individuals who threaten the orderly administration of the installation or site.

a. Designated commanders are defined in paragraph E, reference 2. Among other commanders, all military installation commanders are "designated commanders." For installations or activities not headed by a military commander, the "designated commander" is the military commander in the chain of command immediately above such installation or activity.

b. Designated commanders must prepare, conspicuously post, and enforce the security orders and regulation promulgated in accordance with references 2 and 3 in order to ensure the proper safeguarding of facilities, property, documents, and personnel from loss, destruction, or sabotage.

c. Installation commanders are responsible for providing the initial and immediate response to any incident occurring on the installation. Commanders are responsible for containing the damage, protecting property and personnel, and restoring order on the installation. In performing this military purpose, commanders may order searches and seizures and take other reasonably necessary steps to maintain law and order, and to protect Federal facilities and property.

[redacted] Because commanders may never delegate or abrogate ultimate responsibility for protecting Federal property, facilities, and personnel, commanders may not permit the FBI to assume responsibility for these military interests, unless directed to do so by competent authority. Commanders must, however, allow the FBI to perform its lead role in reacting to terrorist incidents when these military interests are not prejudiced.

e. Military personnel will always remain under the command and control of the military chain of command. If military forces are employed during a tactical response to a terrorist incident, the military commander retains operational responsibility. [redacted]

(1) For installations, or portions of installations, under exclusive Federal jurisdiction, the state and local LEA have no jurisdiction or authority, though they may seek or be asked to assist with security precautions and other duties consistent with their respective interests (e.g., off-installation traffic control, sealing the area). Commanders should be cautious in employing state and local LEA in areas of exclusive Federal jurisdiction because such personnel may not be within the scope of their state duties and may also not fall within the protection of Federal status.

(2) If the incident occurs in an area of concurrent or proprietary jurisdiction, the status of state and local LEA is clearer, but their role in responding to the incident remains muddled. The commander exercises broad and ultimate authority to maintain law and order on the installation, notwithstanding concurrent state jurisdiction. The commander also may deny entry to (or remove from) the installation anyone who poses a threat to good order and discipline.

(3) If state and local LEA agree to submit to the commander's authority in reacting to a terrorist incident, those LEA personnel may assume a quasi-Federal status as the commander's agents. Civil liability for their actions or omissions may attach to the U.S.

[redacted] Again, however, if military equipment, [redacted] the commander is ultimately responsible for [redacted] Military personnel and units will always remain under the command and control of military commanders.

D. INTERNATIONAL TERRORIST INCIDENTS

1. DoD activities outside of U.S. territory are bound by international treaties and agreements. Status of Forces Agreements (SOFA) are the most common example, but other bilateral and multilateral stationing agreements impact on U.S. forces preventing and reacting to terrorist incidents. Such agreements provide the authorities and responsibilities of the host country and of U.S. forces based within the host country. Agreements concerning security, safety, use of facilities, sharing of criminal intelligence information, rules for use of force, and other matters of mutual concern bind overseas commanders.

2. Ultimate responsibility for terrorism counteraction overseas lies with the host country. The host country has a legitimate interest in and right to enforce the law and maintain security, even on U.S. installations, within its borders. International agreements allow the U.S. to exercise authority on U.S. installations. Even if the host country refuses to protect U.S. installations, we have the right of self defense to protect U.S. facilities, property, and personnel.

[redacted]

4. The U.S. commander retains the responsibility for the safety and security of personnel and property on U.S. installations outside U.S. territory. Generally, stationing arrangements grant the U.S. the right (permissive) to take necessary lawful measures to ensure the security of U.S. installations and personnel. For example, the NATO SOFA, at Article VII, paragraph 10, states:

> A. Regularly constituted military units of a force shall have the right to police any camps, establishments, or other premises which they occupy as the result of an agreement with the receiving state. The military police of the force may take all appropriate measures to insure the maintenance of order and security on such premises.

a. Applicable directives and regulations for security of U.S. military installations, personnel, and facilities apply outside U.S. territory, except where made inapplicable in whole or in part by international agreements.

b. The U.S. may be obligated by international agreement to cooperate with host country authorities to allow them access to U.S. installations to protect existing host country interests, subject to U.S. security considerations.

c. Generally, U.S. regulations concerning rules for the use of force and rules for carrying firearms must comply with both U.S. and host nation standards (see, e.g., U.S.-Germany Supplementary Agreement to the NATO SOFA Article 12, para 2).

d. The U.S. retains primary criminal jurisdiction over U.S. personnel committing criminal acts while performing official duties, and personnel are generally protected from civil liability while performing official duties. Failing to follow U.S. or host nation rules, such as those for the carrying of firearms, however, may fall outside the scope of "official duties" and subject U.S. personnel to foreign criminal and civil jurisdiction.

E. INTELLIGENCE GATHERING

[redacted] Although the military services also play an important role in this process, there are several restrictions.

2. Commanders and legal advisors must ensure that intelligence personnel, and others, follow the substantive and procedural requirements of these references while conducting intelligence activities:

a. **Public Law 95-511**, Foreign Intelligence Surveillance Act of 1978.

b. **Executive Order 12333**, "United States Intelligence Activities," December 4, 1981.

c. **DoD Directive 5240.1**, DoD Intelligence Activities, April 25, 1988.

d. **DoD Regulation 5240.1-R**, Activities of DoD Intelligence Components That Affect United States Persons, December 1982.

e. Service regulations (e.g., AR 380-13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations, and AR 381-10, U.S. Army Intelligence Activities).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5

TERRORIST THREAT ANALYSIS AND WARNING

A. INTRODUCTION AND OVERVIEW

1. As noted in Chapter 1, the Department of Defense combatting terrorism efforts begin with an assessment of the terrorist threat to DoD personnel, facilities, and materiel. This chapter begins with a brief overview of the organizations that provide threat information and analysis to DoD Components. It then describes the approach that is used by the Department of Defense to analyze terrorist threats posed to DoD assets. Finally, the chapter concludes with a discussion differentiating terrorist threat analysis from terrorist threat warning. An overview of the DoD terrorist threat warning system will be presented as the concluding section of this chapter.

2. Analysis of the terrorist threat is a difficult and challenging task. Many U.S. Government Agencies and Departments contribute information and analytical approaches in attempt to improve understanding of the terrorist threat. The collection and analysis of terrorist threat information and publication of the analytical products is only one step in the combatting terrorism program. Reports of threatening activity, which may or may not be inspired by terrorists, should not immediately propel a DoD military commander or civilian manager into an alert posture. Many additional steps in the combatting terrorism planning process must be completed before informed decisions about appropriate protection postures can be made.

B. THREAT ANALYSIS ORGANIZATIONS

The threat of terrorist activity targeted against U.S. Government personnel, facilities, assets, and interests has resulted in the development of a significant government structure to collect, analyze, and disseminate information about terrorist threats. Since many U.S. Government Agencies and Departments have overseas activities, it is not surprising to find them sharing terrorist threat information among themselves.

1. National Level

[redacted]

[redacted]

2. DoD Level

a. The Secretary of Defense has assigned to the DIA responsibility for establishing and maintaining an all-source terrorism intelligence fusion center. DIA terrorism analysts tailor and focus all-source intelligence in support of U.S. military commanders. DIA represents the Department of Defense in intelligence community forums dealing with terrorism, and provides information and analytical resources to support the Unified and Specified Commands' and the Services' terrorist threat analysis activities.

b. DIA provides a wide range of terrorism intelligence products to DoD components including daily awareness products, longer range assessments and estimates of terrorist activities, as well as indicators and warning information. DIA's role in the dissemination of terrorist threat information is discussed below.

3. Military Services Role

a. The Secretaries of the Military Departments are directed 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." (DoD Directive 0-2000.12 (reference (a)). To accomplish this task, each Service Secretary appoints a Service lead agency (Army: ITAC; Navy and Marine Corps: NISCOM; Air Force: AFOSI and Marine Corps: Headquarters, Marine Corps (CI)) to monitor foreign intelligence and counterintelligence activities focusing on terrorist groups and terrorist acts. To accomplish this mission, the Service lead agency establishes, as needed, field intelligence offices on an area basis to collect and disseminate information to combatant commanders.

b. Each Service:

(1) Coordinates with appropriate U.S. and host-nation agencies.

(2) Provides overall direction and coordination of the Service intelligence and counterintelligence efforts.

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

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

(5) Conducts investigations of terrorist incidents with the FBI or host-nation authorities for intelligence aspects.

(6) Provides terrorist threat information briefings.

(7) Performs as the Service's liaison representative to Federal, state, and local agencies, as well as host-nation agencies to exchange information on terrorists.

(8) Provides periodic international terrorism products and other threat data to supported commanders. On request, provides current intelligence data on terrorist groups and disseminates time sensitive and specific threat warnings to appropriate commands.

4. Field Level Activities

The Department of Defense and each of the Services possess information collection assets in the field that can be directed to collect information bearing on terrorist threats to DoD personnel, facilities, and assets. The following are examples of those field activities that are integrated into the terrorist threat information collection system.

a. Service and/or OSD Investigative Agencies

Service criminal investigative services; e.g., Army CID, Navy NISCOM, Marine Corps CID, and Air Force OSI collect and evaluate criminal information and disseminate terrorist-related information to supported installation and activity commanders. As appropriate, criminal investigative elements also conduct liaison with local military and/or security police and civilian law enforcement agencies.

b. Intelligence and/or Counterintelligence Staff Elements

Intelligence and/or Counterintelligence staff elements of heads of DoD Agencies and commanders at all echelons should execute the following responsibilities in accordance with DoD 5240.1-R (reference (aa)):

(1) Report promptly all actual or suspected terrorist incidents, activities, and early warnings of terrorist attack to supported and supporting units and/or activities, local intelligence field office, Unified and Specified Commands, DIA, and appropriate headquarters.

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

(3) Develop and present terrorist threat awareness briefings to all personnel within their commands in cooperation with the local intelligence field offices.

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

c. Law Enforcement Staff Elements

Law enforcement staff elements of DoD agencies and military commanders should carry out the following responsibilities:

(1) Initiate and maintain liaison with local intelligence field offices and military criminal investigative offices.

(2) Investigate criminal activities committed within their jurisdiction to determine whether or not such activities may constitute a terrorist threat to DoD personnel, facilities, materiel, or other U.S. interests.

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

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

d. Installation, Facility, Activity, or Unit Security Officers

The foundation of the threat reporting function demanded by the DoD Combatting Terrorism Program rests on the shoulders of installation, facility, activity, or unit security officers. These individuals may not be part of the military intelligence community in a formal sense. However, their overall security and force protection responsibilities place them in positions through which quantities of information of potential interest or concern to the intelligence and law enforcement communities pass on a recurring basis. Therefore, these security officers should:

(1) Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting security or military police office, other supported activities, local intelligence field office, and local military criminal investigation office in accordance with applicable Service and DoD instructions, regulations and directives.

(2) Conduct regular liaison visits with the supporting security or military police office, intelligence field office, and local criminal investigation office.

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

C. TERRORIST THREAT ANALYSIS

1. The primary intelligence mission in support of the DoD combatting terrorism program is warning. Specific warning information--time, date, place, and method of attack--is never voluntarily provided by terrorists. Careful threat analysis is required in order to understand and detect preincident indicators of a terrorist attack to issue timely warning messages.

2. Threat analysis is a critical input into the threat assessment process, a process that results in the implementation of force protection plans and the allocation and expenditure of force protection resources. In addition, threat analysis provides the intelligence officer with information upon which to base warnings.

a. Sources

[redacted]

[redacted]

(1) Open Source Information

(a) Open source information is information in all forms or media that is publicly available and can be collected, retained, and stored without special authorization. Examples include the following:

1 News media (print and broadcast).

2 Scholarly publications.

3 Unclassified United States and foreign government documents including congressional or Parliamentary records.

4 Press releases.

5 Political tracts, handbills, posters, flyers, and leaflets, often distributed by organizations committing, supporting, or opposing terrorist actions.

(b) The news media are often excellent open sources of information on terrorism. These organizations report many major terrorist incidents and often include in-depth reports on terrorist individuals or groups. Such reports can provide analysts with insights into terrorist group goals and objectives, the motivation of individual members of terrorist organizations, modes of recruitment, training and training methods, and tactics of attack.

(c) Terrorist groups and their supporters may publish political tracts, pamphlets, and news releases that reveal their objectives, tactics, and possible targets. Such information is often placed into the public domain as part of a campaign of terror.

(d) Some commercial data services offer timely information about international or military affairs. These data bases often include information regarding terrorist incidents. Such data services often rely on foreign news media; some maintain their own network of sources. Information services are provided on subscription or fee-for-service basis.

(2) Criminal Information

Both military and civil law enforcement agencies collect criminal information. Since terrorist acts are criminal acts, criminal information is a lucrative source for terrorist intelligence. Established law enforcement liaison channels must be used to obtain such information because the collection, retention, and dissemination of criminal information are regulated. Local military criminal investigative offices maintain current information in accordance with DoD regulations governing retention of criminal information. Such material may assist managers and military commanders in the assessment of the local terrorist threat.

(3) Government Information

(a) Government information refers to materials collected, analyzed, and disseminated under official auspices. It includes, but is not limited to, scientific and technical reports, political and economic reports, crime and terrorism statistics, policy statements, legislation, and official correspondence.

(b) As noted above, some government information may be open source, available to all persons who either request or purchase it.

(c) Government information may also be restricted or have limited distribution only within government agencies. Such information might include post-conviction court records, export and/or import license applications, immigration records, or financial securities registration information not released to the public.

(d) Government information also includes data and analyses derived from intelligence sources. Intelligence exchanges with local government agencies through, for example, cooperative arrangements can also augment regional information.

(4) Local Information

(a) Another valuable source of information is the individual service member, civil servant, family member, and individuals with regional knowledge such as college faculty, cultural organizations, etc. 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.

(b) Local information is often of critical importance as it is collected and passed through either law enforcement and/or intelligence channels to the national intelligence organizations. It is frequently invaluable to analysts in confirming news media or other open source accounts of terrorist activities; it can provide early warning of potential terrorist activities, allowing law enforcement and combatting terrorism measures to be initiated in a timely manner, thereby thwarting or minimizing the effects of a terrorist attack.

(5) Access to Intelligence

[redacted]

b. Methodology

(1) DoD Threat Analysis

(a) The Department of Defense has developed a methodology to assess terrorist threat to DoD personnel, facilities, materiel and interests. This methodology is used by all DoD Components.

(b) Threat analysis is the process of compiling and examining all available information to develop intelligence indicators of possible terrorist activities. Threat analysis is the essential first step in determining risk of and vulnerability to terrorist attack. Information used in performing terrorist threat analysis is often more difficult and complicated to acquire from all sources than information dealing with less esoteric military threats. Terrorists operate in a clandestine mode. Unlike conventional military forces that acquire deterrent value by being visible and demonstrating at least a small range of their total capabilities, terrorists gain maximum advantage by remaining invisible until they attack. The smallest terrorist groups combine mobility and cellular organization to make it exceptionally difficult to "find" and "fix" members.

(c) The traditional missions of law enforcement and military intelligence organizations have not focused unconventional threats to DoD personnel, facilities, and materiel. Police and law enforcement organizations usually focus their intelligence efforts on identifying, locating, and apprehending individual criminals. Military intelligence organizations focus on conventional threats. Analysis of terrorist threat requires some degree of reorientation for police and intelligence operations.[1]

(2) Threat Analysis Factors

The Department of Defense has identified six factors to be used in shaping the collection and analysis of information from all sources bearing on terrorist threat. These factors are used in making terrorist threat analyses on a country-by-country basis. The methodology described below is used by the Department of Defense only; other U.S. Government Departments and Agencies may apply their own analytical methodology to form their own terrorist threat analyses.

(a) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.[2]

1 Analysis of information regarding the existence of a terrorist group addresses the question: who is hostile to existing organizations and social structures?

2 A terrorist group need not have posed a threat to American or DoD interests in the past to draw notice under this factor. Groups that may not pose a

---

1 *Terrorism Counteraction*, Headquarters, Department of the Army, FM 100-37, Washington, D.C.: U.S. Government Printing Office, 1987, p. 20.

2 DoD Directive O-2000.12 (reference (a)), "Terrorist Threat Condition System, Enclosure 5."

threat to American or DoD interests in one country may elect to target and to strike at these interests elsewhere.

(b) Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.[3]

1 Analysis of terrorist group capabilities addresses the question: what weapons have been used by terrorist groups in carrying out past attacks? What infrastructure necessary to train, equip, target, and execute attacks had to be erected?

2 As suggested by the discussion in Chapter II, terrorists operating without support or direction from foreign governments have access to a wide variety of commercial equipment suitable for intelligence collection, targeting, and striking at American or DoD interests in the United States or abroad. Terrorist groups operating with support or direction from states hostile to the United States can frequently obtain even more sophisticated weapons, intelligence collection and targeting equipment, better financial backing and logistics support, and better access to media to promote their ideological aims than those groups operating without such support.

3 Reports of arms, ammunition, and explosives thefts should be monitored very closely, as should reports of thefts of night vision devices, low-light closed circuit TV equipment, and other equipment used by law enforcement and intelligence agencies worldwide for reconnaissance and surveillance. Large-scale commercial transactions involving explosives for use in mining and mineral exploration, military-style weapons and ammunition should also be monitored. Reports regarding trafficking in lost or stolen government travel documents should also be viewed with concern.

4 The ability of terrorists to move from one country to another is also an important facet of terrorist group capability. Reports of criminal activity regarding thefts, forgeries, or alterations of official identification documents, travel documents, or international tickets may be evidence of future terrorist activity.

5 While none of these information reports is unequivocal evidence of terrorist activity, if such reports are followed with care, such information can quickly become a key indicator of capability meriting further scrutiny. Efforts to analyze terrorist capabilities depend to a very large degree on the ability of analysts to assemble huge quantities of seemingly unrelated information and identify a pattern of disaggregated or distributed transactions. The sum of these transactions translates into evidence of terrorist group capability.

(c) Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity.[4]

1 Analysis of terrorist group intentions seeks to address the questions: Why do groups engage in terrorist acts? What do they hope to achieve?

---

3 *Ibid.*

4 *Ibid.*

2 Terrorist groups sometimes provide the world with information about their long-term goals and objectives. They sometimes provide long treatises that seek to justify the use of terror tactics to achieve stated goals and objectives. They also display behaviors which are clear, unambiguous indicators of intent.

(d) Demonstrated terrorist activity over time.[5]

1 Analysis of terrorist group history addresses the questions: What have terrorists done in the past? What is the terrorist group's method of operations? How did they acquire the capability they demonstrated? Where did they obtain support? What additional attacks did they mount?

2 Terrorism analysts recognize that history is not an especially reliable predictor of future behavior. However, a well-developed history of a terrorist group is important because it helps put into perspective information about current terrorist or terrorist related activities. Maintaining a good history of terrorist groups is essential in order to develop profiles of events that facilitate terrorist threat analysis.

(e) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.[6]

1 Targeting addresses the questions: who is likely to be attacked, why are they likely to be attacked, and what is the basis for accepting reports that such attacks are planned?

2 Translating statements of general intent, supported by historical patterns of hostile, destructive, and even murderous behavior, into predictions about future, time and place specific acts deals with targeting, and is the most challenging aspect of terrorist threat analysis.

(f) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to carry out their intentions.[7]

1 The Security Environment of a country refers to the general ability of national law enforcement, paramilitary, and military institutions to maintain social order. Parameters examined within the Security Environment including training of law enforcement, paramilitary, and military forces to deal with terrorist incidents; quality of equipment available for law enforcement and internal security forces; distribution of internal security forces throughout a country, etc.

(3) Service Level Terrorist Threat Analysis

(a) Each of the Services maintains its own terrorist threat analysis capability. While the DoD methodology is used, the Service threat analysts sometimes view the data from a Service-unique perspective.

---

5 *Ibid.*

6 *Ibid.*

7 *Ibid.*

(b) Differences in the perspectives or the salience of particular terrorist threat factors among DIA, Service, or CINC threat analysts may lead to divergent conclusions about specific terrorist threats.

(c) It is possible, for example, for the DIA terrorist threat analysis to conclude that DoD personnel in a given country are generally at risk. The Service terrorist threat analysis may report that its personnel assigned to the same country are either at greater or lesser risk than the assessment by DIA. The Service threat analysts may form their judgment on the basis that, unlike other DoD components, their Service has no permanent presence in a country. While the threat to all DoD assets in a country may be at one level, a particular Service, having no assets in the country, faces no threat of terrorism in the country in question.

(d) Differences in perspective on and salience of terrorist threat factors assessed by the Unified and Specified Command, Service and DIA terrorism analysts may sometimes account for differences in analyses or judgements about terrorist threats to DoD-affiliated personnel, facilities, and assets.

(4) Combatant Commands

(a) The Commanders in Chief of the Unified and Specified Commands also require terrorist threat analysis from their own intelligence organizations. The purpose of these is twofold:

1 Assist the CINC in providing for the security and protection of forces under his control; and

2 Ensure the flow of information passing through Service lines of communication within the area of CINC responsibility is also brought to the attention of the CINC and his staff and disseminated within the Command as appropriate.

(b) The CINC through his J-2 staff is able to draw upon the information and analysis resources of the DIA, the Services, and through his Political Adviser, all U.S. Embassies in his area of responsibility.

(5) Elements of Information

(a) The Terrorist Assessment Methodology employs an analytical approach that focuses information collection and analysis from all sources in a manner such that data can be aggregated from a wide range of sources over a long period of time to build a mosaic picture of terrorist groups, their capabilities, their modus operandi, and their targets. Information is collected from all sources including resources in the field. Specific requests for information are passed through intelligence channels.

(b) Intelligence tasking may seek very specific bits of information. When combined with information collected from all sources, intelligence information collected in response to specific intelligence tasking becomes the basic data on which analyses and judgments using the six DoD terrorist threat analysis factors--Existence, Capability, History, Intentions, Targeting, and Security Environment--can be built.

D. TERRORIST THREAT LEVEL

1. The DoD terrorist threat analysis community has developed a notation system used to describe the country-specific results of terrorist threat analysis based on the terrorism threat analysis methodology briefly described above. Other departments and agencies may use DoD terrorism information but employ their own terrorist threat analysis methodology. As a result, there may be differences between the Department of Defense and other departments or agencies on gross or simple descriptions of terrorist threat to U.S. Government personnel and facilities in one or more specific countries. The differences among DoD and other views may be less significant than would first appear once the summary description terms used by each are explained.

2. The Department of Defense uses a five-step scale to describe the severity of the threat as judged by intelligence analysts. These five steps from highest to lowest are as follows:

a. CRITICAL.

b. HIGH.

c. MEDIUM.

d. LOW.

e. NEGLIGIBLE.

3. Threat levels are the result of combinations of the threat analysis factors discussed above as reflected in Figure 5-1 below. The factor, Security Environment, is considered separately as a modifying factor and will influence the assigned threat level.

	Threat Analysis Factors				
Threat Level	Existence	Capability	History	Intentions	Targeting
CRITICAL	•	•	¤	¤	•
HIGH	•	•	•	•	
MEDIUM	•	•	•	¤	
LOW	•	•	¤		
NEGLIGIBLE	¤	¤			
• Factor must be present			¤ Factor may or may not be present		

Figure 5-1. DoD-Level Determination of Terrorist Threat Level

4. Threat levels are the result of combinations of the following factors based on analysis. They describe the broad political environment in which terrorist activity might occur.

a. Terrorist Threat Levels may not address the question: "when will a terrorist attack occur?"

b. Terrorist Threat Levels do not allocate protective resources.

c. Issuance of Terrorist Threat Level judgments is not a warning notice.

5. Formal terrorism warning notices are issued separately as described later in this chapter. The follow discussion expands on the data, information, and analysis that underlies each Terrorist Threat Level.

a. Terrorist Threat Level CRITICAL

CRITICAL. Factors of Existence, Capability, and Targeting must be present. History and Intentions may or may not be present.

(1) Analysts declare threat level CRITICAL when as a result of their assessment of all available information they:

(a) Detect the presence of terrorist groups in a region or country.

(b) Identify the level of capability (including specific means) by which terrorist groups can carry out an attack.

(c) Identify the existence of current, credible targeting of U.S. interests, DoD personnel, or DoD facilities or materiel.

(2) This is a short-hand expression, and should be interpreted as the strongest possible analytic judgment to heads of DoD components that further analysis of their immediate situations should be undertaken. Based on information available to the intelligence community from all sources, Threat Level CRITICAL is a judgment that terrorist attack is highly probable.

(3) However, Threat Level CRITICAL may not address the question: when will a terrorist attack occur?

(4) The character of the CRITICAL threat level determination compels local commanders to take appropriate protective measures because current, credible evidence exists pointing to the targeting of DoD personnel, facilities, assets or interests by terrorist groups.

(5) CRITICAL is differentiated from all other Terrorist Threat Levels because it is the only one in which credible information identifying DoD personnel, facilities, assets or interests as potential targets of attack is present.

b. Terrorist Threat Level HIGH

HIGH. Factors of Existence, Capability, History and Intentions must be present.

(1) As in the case of CRITICAL, analysts establish Threat Level HIGH when their assessment of terrorist threat information finds:

(a) Evidence of terrorist individual or group existence.

(b) Evidence of capability to attack.

(c) History of terrorist attacks that may or may not involve American interests, DoD personnel, facilities or materiel.

(d) Credible indications providing evidence of intent to engage in acts harmful to American interests or DoD personnel, facilities, or materiel.

(2) Terrorist Threat Level HIGH is differentiated from CRITICAL because analysts lack targeting information. It is differentiated from MEDIUM because analysts have sufficient credible information to assess threat factor Intentions toward U.S. Government interests.

c. Terrorist Threat Level MEDIUM

MEDIUM. Factors of Existence, Capability, and History must be present. Intentions may or may not be present.

(1) Threat Level MEDIUM and Threat Level HIGH are similar in that data for the factors Evidence, History, and Capability exists.

(2) Terrorist Threat Level MEDIUM is differentiated from HIGH based on the content of information in factors Existence, Capability and History. The presence or absence of information on terrorist group intentions may also permit analysts to differentiate MEDIUM from HIGH terrorist threat.

d. Terrorist Threat Level LOW

LOW. Existence and Capability must be present. History may or may not be present.

(1) Threat Level LOW is assessed when there is evidence of terrorist group existence and capability in a country but no evidence of intentions or targeting. Historical information of terrorist group activity may or may not be present.

(2) Threat Level LOW is differentiated from MEDIUM by the substantive information within the threat analysis factors of Existence and Capability.

e. Terrorist Threat Level NEGLIGIBLE

NEGLIGIBLE. Existence and/or capability may or may not be present.

Threat analysts will report a negligible threat level when little or no credible evidence of terrorist group existence and capability exists for a country subject to analysis and no credible evidence of history, intention, and targeting exists.

E. CHANGES IN TERRORIST THREAT LEVEL DECLARATIONS

1. Analysis of terrorism is an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to DoD-affiliated personnel, facilities, and assets begin anew with each analysis. No formal escalation ladder of Terrorist Threat Level exists; terrorist threat level designations for each country subject to analysis are applied on the basis of current information and analysis.

2. Terrorist threat level designations can go from NEGLIGIBLE to HIGH or from HIGH to NEGLIGIBLE without passing through the intermediate steps of LOW or MEDIUM. While dramatic, extreme changes in judgments about terrorist threat levels in one country are not common, the Terrorist Threat Level system does not preclude analysts from making such dramatic changes in Threat Level Designations.

3. In the former case, a new terrorist group might initiate a series of attacks on DoD personnel or facilities, quickly building evidence of existence, capability, history, intention,

and targeting. In the latter case, law enforcement and security forces might score a big success, apprehending a major terrorist group virtually intact, wiping out its base of support, its capability to attack, its ability to target DoD-affiliated personnel and facilities, and even its entire active cadre membership.

F. THREAT WARNINGS

1. Overview

[redacted]

b. Individual DoD Components also have the right to independently notify their members of impending threats. If a DoD Component intelligence activity receives information that leads to an assessment of an imminent terrorist attack, it may exercise its right to issue a unilateral warning to its units, installations, or personnel identified as targets for the attack.

c. Warnings are issued when specificity of targeting and timing exist or when analysts have determined that sufficient information indicates that U.S. personnel, facilities, or interests, particularly those of the Department of Defense, are being targeted for attack. Warning need not be country specific. A warning can cover an entire region. The key to warning is that the terrorism analyst recognizes that the pre-incident indicators for an attack are present and that a warning must be issued.

d. [redacted]. They are unambiguous--it is clear to the recipients they are [redacted] warned. Warnings are intended for distribution up, down, and laterally through the chain of command--not just downward. Warnings of impending terrorist activity are likely to have national implications and will be provided routinely to decision makers at the policy level of the U.S. Government.

[redacted]

G. TERRORIST THREAT ANALYSIS AND WARNING: SUMMARY OBSERVATIONS

1. The DoD threat analysis methodology described in this chapter is applied by DoD Components to form judgments about terrorist threat.

2. The DoD intelligence activities use the terrorist threat analysis methodology to guide collection and analysis of the best available information on which it forms its assessment and issues warnings of terrorist threats.

3. Terrorist Threat Level assessments are intended to provide a judgment by DoD intelligence activities of the terrorist threat for a country based on all-source information on hand. Terrorist threat analyses summarized in Terrorist Threat Level declarations assist heads of DoD components, the Services, Unified and Specified Commands, and local commands make judgments about the allocation of combatting terrorism and force protection resources. THERE IS NO AUTOMATIC RELATIONSHIP BETWEEN ANY THREAT LEVEL AND ANY SPECIFIC COMBATTING TERRORISM RESPONSE AS ARE DESCRIBED BELOW.

4. IT REMAINS THE RESPONSIBILITY OF COMMANDERS IN THE FIELD, THEIR CHAINS OF COMMAND THROUGH THE UNIFIED AND SPECIFIED COMMANDS, THE MILITARY SERVICES, AND THE HEADS OF DEFENSE AGENCIES, TO ALLOCATE PROTECTIVE RESOURCES. Judgments about use of personnel, special security equipment, and changes in organizational behavior should be influenced by but not automatically driven by Threat Level declarations.

5. In the chapters that follow, additional criteria and analytical techniques to be used by civilian managers and military commanders to inform further judgments about the allocation of protective resources will be discussed. As noted in Chapter 1, decisions to alter the force protection posture of DoD personnel and facilities in response to terrorist threats must consider the risk posed by terrorists, the vulnerability of DoD assets to such

attacks, and the importance or criticality of such assets to the accomplishment of DoD missions. Chapter 6 examines these important considerations.

CHAPTER 6

ASSESSMENT OF RISK, VULNERABILITY, AND CRITICALITY

A. INTEGRATED TERRORIST THREAT ESTIMATES

1. Several elements of the DoD Combatting Terrorism Program were identified in Chapter I of this Handbook. The initial step in the development of a combatting terrorism program is an analysis of the threat of terrorism as it affects each DoD activity, installation, or organization in all DoD Components. The process by which terrorist threats can be analyzed was described in Chapter V. In this chapter, the second step in the development of a combatting terrorism program will be explored.

2. The development of an Integrated Terrorist Threat Estimate is executed by civilian managers and military commanders at all levels within the DoD Components. They and their staffs assess the risk of terrorist attack. Questions such as the following are considered:

a. Are there individuals or organizations in the vicinity of DoD personnel, facilities, or materiel that represent a threat to those personnel, facilities, or materiel?

b. Is there a risk that the threat will materialize?

3. Assessments of terrorist attack risk seek to understand the circumstances under which a terrorist attack is more or less likely, and how civilian managers, military commanders, and their staffs can exert influence before the fact to reduce the likelihood of terrorist attack and mitigate its effects should it occur.

4. After answering these questions, the following questions are examined:

If DoD assets are attacked, how likely is it that they will be rendered unable to perform assigned missions?

5. This question goes to the element of vulnerability, the probability that DoD assets if attacked will not be usable to perform assigned missions and responsibilities:

If DoD assets are inoperable or unable to perform, can assigned missions be accomplished?

6. This question goes to the issue of mission criticality and the potential ability of terrorist attacks in peacetime, crisis, or war to disrupt the ability of DoD Components to carry out missions and functions assigned by the National Command Authorities.

7. This chapter examines assessments of terrorist attack risk, vulnerability to terrorist attack, and the mission criticality of DoD assets including personnel, facilities, and materiel subject to terrorist attack.

B. RISK OF TERRORIST ATTACK

As noted in Chapter 5, DoD-level terrorist threat analysts prepare tailored and focused products for DoD Components generally and the Unified and Specified Commands with territorial responsibilities specifically. [redacted] Assessing the risk of becoming the victim of a terrorist attack is the responsibility of management and command at every echelon. It is a responsibility that cannot be delegated or waived. The risk of becoming the victim of a terrorist attack appears to be influenced by several factors.

1. Terrorist Group Goals and Objectives

a. Many terrorist groups around the world have developed clear goals and objectives. Violence and threats of violence are employed in pursuit of these goals and objectives.

b. In some countries, DoD personnel and facilities may not be at great risk from such groups because attacks on other targets directly related to terrorist groups objectives are available. In other countries, multiple terrorist groups may be operating. In such cases, some groups may represent a lesser threat to DoD personnel and facilities than other groups because DoD personnel and facilities are not their priority target. For example, during the mid to late 1980s, the Provisional Irish Republican Army (PIRA) launched a series of armed attacks including bombings and shootings of British military forces stationed in the Netherlands and Germany. Although DoD personnel, facilities, and materiel in Germany were at considerable risk of becoming victims of terrorist attack, the probability of PIRA attacks on DoD assets was less than the probability of other terrorist group attacks such as the Red Army Faction or Revolutionary Cells.[1]

2. Proximity to Other Terrorist Group Targets

Even if a terrorist group has well-defined goals and objectives, a strategy to achieve such goals, and attempts to execute a carefully planned attack aimed at other targets, DoD personnel and facilities can become the victims of terrorist violence. Whenever DoD personnel and facilities are collocated with facilities of host governments overseas, there is an increased risk that attacks by terrorists against the host-government facilities will also include DoD personnel, facilities, and materiel.

---

1 See Appendix A for a list of selected attacks on DoD-affiliated personnel and facilities during the period 1972-1991. For additional information on terrorist attacks against U.S. and NATO forces stationed in Germany during the 1980s, see Department of Defense, *Terrorist Group Profiles* (Washington, D.C.: U.S. Government Printing Office, 1989).

3. Prominence or Wealth

a. Terrorist groups often conduct attacks as a means of publicizing their group, of spreading word of their cause, and of intimidating the public. Attacks on prominent individuals, organizations, or institutions are often newsworthy. Attacks on wealthy individuals also garner press coverage.

b. [redacted]

[redacted]

b. Americans are generally proud of their heritage. We find much within our nation of which to be proud. Sometimes, however, discretion is the better part of valor, and some consideration should be given to the various ways in which our nationality is revealed when so doing places us at risk.

(1) Vehicle Identification

In many overseas countries, Americans are issued vehicle identification including special license plates (color, design, special characters) or decals identifying the vehicle as one registered to an American national.

(2) Personal Dress

The way Americans dress sets us apart from others, particularly overseas. Loud clothes and T-shirts with civilian and military slogans written on them provide identification of the wearer's nationality.

(3) Speech

The way Americans talk can give others an opportunity to identify us as potential targets, even if we speak the language. The louder the volume of speech, the more military terms and American slang used in conversation, the easier it is to determine the nationality of the speaker.

(4) Customs and Habits

Even if Americans physically blend in with the locals, our customs and habits give us away. Simple customs such as the manner in which we use a knife and fork at dinner to more sophisticated social practices such as greeting business or social acquaintances can give observers excellent clues as to our nationality, even if we "fit in" with the appearance of the local population.

(5) Personal Behavior

(a) Some social behavior acceptable in America is not socially acceptable in foreign lands. Many Americans when overseas do not dress, speak, or behave in appropriate manner. Some of the inappropriate behaviors observed that help identify the nationality of American's overseas are the following:

1 Loud and obnoxious speech.

2 Inappropriate attire for churches, national shrines and memorials.

3 Public displays of affection.

4 Smoking in inappropriate places.

5 Smoking American brands of cigarettes, not local brands.

6 Inappropriate use of alcohol.

7 Heckling or verbally accosting other persons.

8 Inappropriate operation of motor vehicles.

(b) Even if there is nothing uniquely American about these behaviors, the fact we behave in a different, remarkable fashion from others draws attention to us. Having aroused curiosity in outside observers, it usually does not require exhaustive observation to determine our nationality from other indicators discussed here.

(6) Currency

Use of American currency or travellers checks with unambiguously American banks or financial institutional identification on them is another means by which terrorists can identify the nationality of Americans overseas.

5. American Government Representatives

Some terrorist groups have developed rather sophisticated understandings of the American political system. The leadership of some terrorist groups recognizes that there are often strongly held views in the American populace that are different from the official views of the U.S. Government. Sometimes, American government officials are at risk of terrorist attack even though American tourists or businesspersons are not. [redacted]

[redacted]

6. Military Affiliation

Once in a while, terrorist groups discriminate against specific groups of U.S. Government employees. It is not surprising that when such discrimination by terrorist groups take place, State Department employees and DoD personnel appear to be singled out for special treatment. There are many indicators associated with U.S. military affiliation that have been used to identify and target DoD personnel in the past. Among these are the following:

a. Uniforms

Many terrorist groups have generally been able to identify American military uniforms and differentiate them from those worn by foreign military organizations. Some appear able to identify differences among U.S. military uniforms including Service, season, and uniform purpose (fatigues, Service dress, formal dress uniforms, etc.). In such circumstances, appearing in uniform identifies the wearer as American and military.

b. Tattoos

Tattoos have been quite popular among American military personnel for years. Aside from the risk of infection and disease that accompanies use of improperly sterilized tattooing instruments, tattoos are often uniquely American works of art. Tattoos of specific military unit logos, unit nicknames, American landmarks, or slogans popularized by American movies can be significant identifying marks that give clues as to the nationality and affiliation of the owner.

c. Grooming Standards

DoD personnel are expected to adhere to a well-defined set of grooming standards. Not only are such standards helpful in establishing espirit de corps, in many instances they serve to improve and maintain personal hygiene and in case of combat ensure proper fit of protective equipment. In some circumstances, however, rigid

adherence to personal grooming standards can be an important aid in identifying DoD military personnel.

7. Specific Identity

Some terrorist groups have developed especially sophisticated tactics to terrorize and intimidate their target audiences. A tactic that has been used from time to time with effect has been to target specific, named American officers or officials. [redacted]

[redacted]

g. Name Plates and Luggage Tags

Name plates on residences, offices, vehicles, and mail boxes help identify potential targets of terrorist actions. Luggage tags with names and addresses readily visible are also good sources of information for use by terrorists.

8. Mistaken Identity

Terrorists are human, and even they make mistakes in identifying and targeting from time to time. Certain circumstances seem to increase the risk of mistaken identity.

a. Housing

It is useful to know the rental history of a residence before committing to a lease. If, for example, the previous tenants were affiliated with certain governments known to be high priority terrorist targets, it may be prudent to look further for housing.

b. Uniforms

Some terrorist organizations have demonstrated excellent uniform and grade recognition skills; other groups have not. Depending on the existence and capability of terrorist groups operating in each country, wearing American military uniforms may

increase risk of attack because of an inability of terrorists to differentiate DoD personnel from host government personnel on the basis of uniform.

c. Symbols of Power and Prestige

As in other instances of mistaken identity, if one looks the part of a powerful or prestigious person, there is always the possibility that one will be mistaken for a powerful or prestigious person. In those instances where terrorists are seeking a specific individual, it may be useful to avoid appearing much like the presumed target.

9. Detectability

Even if terrorists develop detailed information on potential victims of kidnapping or hostage-taking, they must still be able to detect the presence of their target. Terrorists use visual surveillance; they may have used electronic surveillance in some instances as well.

10. Accessibility

Even if terrorists can identify DoD personnel as American nationals, as symbols of American power and prestige, as symbols of military oppression, and even if they can single out specific individuals, the risk of becoming a terrorist victim may still be controllable. Not only must terrorists identify, detect and track targets, they must get within range of their weapons if they are to have any chance of a successful attack. [redacted]

C. VULNERABILITY ASSESSMENTS

1. General

a. Vulnerability assessments address the consequences of terrorist attacks in terms of the ability of units, installations, commands, or activities to accomplish their assignments successfully, even if terrorists have inflicted casualties or destroyed or damaged DoD assets. Put slightly differently, vulnerability analysis seeks to understand the compound probability of (1) being hit by a terrorist attack and (2) whether or not assigned responsibilities can be fulfilled as required if attacked.

b. In assessing vulnerability, some excursions from the range of attacks described in terrorist threat analysis products for relevant terrorist groups should also be made. Not only are such excursions helpful in planning for the "greater than expected" threat, such excursions help managers and military commanders identify the sensitivity of their combatting terrorism plans, programs, and protective measures to changes in analytical assumptions, threat, role or mission.

2. Vulnerability Assessment Functions

a. The minimum purpose of vulnerability assessments is to aid installation civilian managers and military commanders identify the following:

(1) Weaknesses in the physical security plans, programs, and structures.

(2) Inefficiencies and diminution of effectiveness in personnel practices and procedures relating to security, incident control, incident response, and incident resolution

including but not limited to law enforcement and security, intelligence, command, communications, medical, and public affairs.

(3) Enhancements in operational procedures during times of peace, mobilization, crisis, and war.

(4) Resource requirements necessary to meet DoD, Service, combatant command, and local security requirements.

b. Installation civilian managers and military commanders may use vulnerability assessments for other management, training, and oversight purposes as well.

3. Vulnerability Assessment Process

a. "Terrorist Thinking"

It is imperative that members of the installation staff participating in the vulnerability assessment step outside their usual roles and "think like a terrorist." They need to ponder several questions.

(1) What assets would terrorists target? Why?

(2) What capabilities are they reported to have? Which would be effective against targets assessed as likely? Why?

(3) How might those capabilities be employed?

(4) What might early signs of attack be? How might such attacks be detected by the authorities?

(5) What are the avenues of approach terrorists would take to reach targeted assets?

(6) How well-protected are the assets likely to be targeted?

b. Elements of Vulnerability

(1) After identifying several approaches terrorists might employ to gain access to DoD personnel and facilities, the facility should be examined from physical, personnel, and operations security perspectives.

(2) The following enumerated list of vulnerability elements is intended to be descriptive and thought provoking; it is not intended to be comprehensive or definitive. Vulnerability elements include steps criminals or terrorists might take to gain access to protected DoD assets and the resulting adverse consequences for the Department of Defense in terms of diminution of capability to carry out assigned missions. Vulnerability elements also include actions taken by DoD personnel during the course of execution of assignments that may increase the risk of terrorist attack and exacerbate the consequences of attack should it occur.

(3) Terrorists can cut perimeter fences, gain access to a facility, inflict casualties, and degrade DoD capabilities to execute assigned missions. Undetected intrusions or detected intrusions that generate no alarm or response suggest a potential vulnerability to terrorist attack.

(4) Removal of vehicles from secure storage facilities to an open field in preparation for unit transit from a main operating base to a training area increases the exposure of vehicles to potential terrorist attack. Conduct of training exercises is, however, part of the normal peacetime training and exercise routine.

(5) Military commanders and civilian managers as appropriate have responsibility for balancing exposure of DoD assets to terrorist attack risk and vulnerability with continued preparation, training, and execution of DoD missions. Assessments of vulnerability are continuous, based on the operational tempo of each DoD component's specific activities.

[redacted] personnel who may be at risk because of their prominence or positions. Appendix D, Enclosure 1, provides a survey instrument tailored to port security considerations; this survey instrument can also be used to assess waterside security at DoD installations bordering rivers, lakes, or bodies of salt water. Topics that should be addressed in a physical security survey include, but are not necessarily limited to, those illustrated by Figure 6-1.

(7) Physical Security Surveys together with terrorist threat analyses provide the data necessary to determine Physical Security Threats as defined in DoD 5200.8-R, Security of DoD Facilities, May 1991.[3] Physical Security Assessments provide key inputs necessary to make judgments with respect to terrorist attack risk (can the targets be hit?) and vulnerability (can DoD units continue to accomplish assigned missions if attacked by terrorists?).

4. Application of Physical Security and Assessments

a. Visible, fixed, land-based DoD facilities should have vulnerability assessments performed on a regular basis if terrorist threat analyses establish the existence of terrorist threat groups in the country housing the facility. However, vulnerability assessments should not be limited to fixed, land-based DoD facilities. Some DoD assets that require protection are senior military officers or senior DoD civilian officials. The specific assignments of these individuals may place them at risk of becoming the victim of a terrorist attack. In some cases, loss of an individual is tantamount to the termination or failure of a DoD mission.

b. Vulnerability assessments can also be applied to residences of DoD-affiliated personnel, travel plans, and life styles.

c. Vulnerability assessments should explicitly consider the possibility of indirect attacks or attacks from unusual approaches. Terrorists have attempted to use hot air balloons, ultra-light aircraft, powered hang-gliders, swimmer delivery vehicles and other unusual means to breach perimeter security devices.

---

2 See Chapter 13 for discussion of High Risk Personnel and High Risk Billets.

3 This subject is addressed in Chapter 7.

DELETED

Figure 6-1. Physical Security Survey Topics

d. Three-dimensional vulnerability assessments are imperative when assessing the vulnerability of DoD personnel, facilities, or material located within installations or buildings not owned or completely controlled by the Department of Defense.

e. Vulnerability assessments are an ongoing process. Vulnerability of DoD assets changes daily, if not hourly, depending upon the nature of the terrorist threat on the one hand, and the nature of the tasks being performed on the other. A detailed, static vulnerability assessment provides a baseline assessment from which decreases or increases in vulnerability can be assessed.

f. The process of constructing an Integrated Terrorist Threat Estimate requires another building block. The overall importance of each DoD asset must be examined in light of assigned missions, protection requirements, and identified threats.

D. CRITICALITY ASSESSMENTS

1. General Observations

a. The criticality assessment identifies key assets and infrastructures that support DoD missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation's and/or unit's ability to perform its mission. It examines costs of recovery and reconstitution including time, dollars, capability and infrastructure support.

b. Analysts performing criticality assessments should consider the possibility of collateral damage sufficient to disable or destroy a DoD critical asset in the event that a nearby target is attacked by terrorists.

c. Criticality assessments should be performed within the acquisition and logistics communities as well as in operational units and reserve forces. Application of criticality assessment elements to research, development, test, and evaluation (RDT&E), procurement, maintenance, and logistics life-cycle events will facilitate continued Service and DoD Agency support of combatant commanders and their subordinate commands in the field during times of crisis or combat, even if the United States and our allies defense industrial bases should become targets of terrorist attack.

d. The Service Acquisition Executive and Acquisition Program Executive Officers should direct preparation of a Key Assets list required under DoD Directive 5160.54 (reference (bb)) for each acquisition program. Contracting Officers and Contracting Officer's Technical Representatives should survey contractors performing contracts for DoD to identify key assets as defined by reference (bb).

2. Criticality Assessment Functions

a. In military units deployed under the command of the Services or a Unified and Specified Command, the staff at each echelon of command determines and prioritizes critical assets. The commander approves the prioritized list.

b. The criticality assessment:

(1) Identifies installation's and/or unit's key assets.

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

(3) Determines time required to duplicate key assets or infrastructures 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.

3. Elements of Criticality

[redacted]

E. USE OF INTEGRATED TERRORIST THREAT ESTIMATES

1. In Chapter 1, it was observed that the DoD Combatting Terrorism Program has two phases: a proactive or preventive phase and a reactive phase. In Chapter 5, Terrorist Threat Analysis, the first building block in the proactive phase, was discussed. In this chapter, the assessment of terrorist attack risk, DoD asset vulnerability to such attacks, and DoD asset criticality to DoD mission accomplishment have been addressed.

2. The DoD Combatting Terrorism Program mandates that civilian managers and military commanders at all echelons assume responsibility for assembling an integrated Terrorist Threat Estimate. This estimate is constructed from four basic building blocks provided by organizations indicated:

a. Terrorist Threat Analyses (intelligence community).

b. Terrorist Attack Risk Assessments (civilian management/military commanders).

c. Terrorist Attack Vulnerability Assessments (civilian management and/or military commanders).

d. DoD Asset Criticality Assessments (civilian management and/or military commanders).

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7

PHYSICAL SECURITY SYSTEM CONCEPT

A. INTRODUCTION

1. This chapter considers the plight of civilian managers and military commanders, depicted in Figure 7-1. They are frequently confronted with Terrorist Threat Analyses prepared by DoD-level intelligence agencies. They receive supplementary terrorist threat information and analyses through Service and CINC channels. Their own intelligence, counterintelligence, and law enforcement staffs add to the general storehouse of terrorist threat information.

2. In addition to terrorist threat information and analyses, they receive--on a continuing basis--judgments on terrorist attack risk, the vulnerability of their missions to the consequences of attacks on their assets, and the criticality of key assets that may require protection. Since civilian managers and military commanders have other tasks to perform as well as to protect DoD-affiliated personnel, facilities, and assets from terrorist attack, they can easily become overloaded with security-related information and demands for response in the absence of guidance on establishment of priorities for DoD asset protection.

3. Figure 7-1 illustrates this situation. It shows the aggregate potential for security enhancements as a result of the development of an Integrated Terrorist Threat Estimate in the upper left of the figure; the lower right shows a broad range of daily activities that must be managed and overseen, each embedded in a security or force protection environment. As suggested by the Plan of the Day in the lower right-hand corner of the figure, life within DoD components goes on, with or without a terrorist threat. [redacted] The challenge is to find the proper balance of Force Protection and Antiterrorism on the one hand, and carrying out other elements in the Plan of the Day that contribute to DoD mission accomplishment.

4. The upper-right hand corner introduces a new block of information, analytical tools, and guidance on security and security resource allocation priorities: DoD Physical Security Policy.

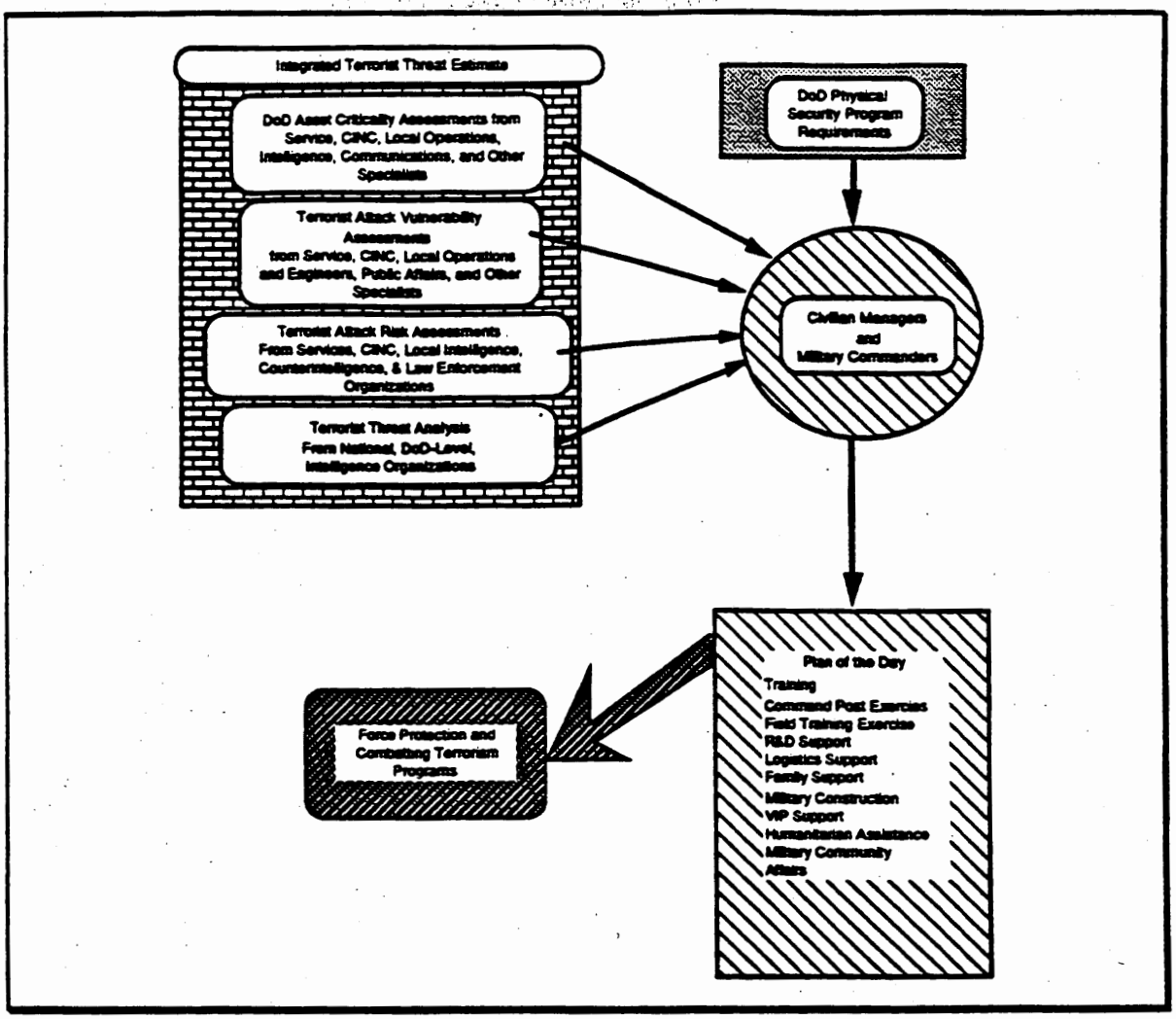


Figure 7-1. Processing Integrated Terrorist Threat Estimates Into Antiterrorism and Force Protection Programs

[redacted] As will be shown in greater detail below, this regulation facilitates integration of physical security programs, personnel security activities, and operations security into a mutually reinforcing set of antiterrorism preventive measures.

B. DoD PHYSICAL SECURITY POLICY

1. Policy Objectives

a. DoD has promulgated a general policy dictating physical security measures applicable to all DoD installations, facilities, and activities. The objectives of reference (cc) are to:

(1) Establish general policy for the security of personnel and installations, military operations, and certain assets.

(2) Provide realistic guidance, general procedures, and the necessary flexibility for commanders to protect personnel, installations, operations, and assets from typical threats.

(3) Reduce the loss, theft, or diversion of, and damage to, DoD assets, thereby ensuring that warfighting capability is maintained.

b. To implement this policy, OSD has established some nominal design threats used to help planners address physical security requirements. The design threats include peacetime, crisis, and wartime conditions, identify broad classes of perpetrators of physical attacks against DoD facilities and materiel, and postulate nominal ranges of capability defined by types of weapons or tools used on the one hand, or the ability to penetrate DoD facilities protected by standard protection systems.

2. Physical Security Threats

a. [redacted]

c. The DoD Regulation describes a broad range of physical security threats based on the types of tools or weapons incorporated in the physical security threats and the capability of perpetrators to penetrate physical security protective devices. Figure 7-2 illustrates the range of threats and capabilities against which protection must be designed and implemented. Emphasis on terrorist threats has been added.

d. [redacted] Physical Security Threat Level as used by the DoD Regulation addresses the tools and weapons used by perpetrators of attacks on DoD facilities. The capabilities and characteristics of weapons and tools dictate protection requirements. Protection requirements, in turn, drive architectural plans, drawings, and construction.

---

1 Individuals who resort to violent attacks against DoD assets motivated by personal anger, not politics.

DELETED

Figure 7-2. Physical Security Threat Matrix

e. Civil engineers have a very narrow perspective on the design and construction of facilities to withstand assault. [redacted] terrorist threat analysts are also interested in the capabilities employed by terrorists as they execute attacks against targets. These analysts are concerned about the technical capability of weapons and tools and the method of operations employed in terrorist attacks.

3. Systems Approach to Physical Security

[redacted] standards used to define acceptable or unacceptable security are not based on rigid, fixed construction standards. They reflect instead the variable nature of physical security threats to DoD assets, the dynamic character of DoD force structure, the distribution of forces and assets among widely distributed DoD installations, and the different activities of the DoD components.

b. The Regulation establishes the following physical security system PERFORMANCE GOAL:

The goal of the security system for an asset or facility is to deploy security resources so as to preclude or reduce the potential for sabotage, theft, trespass, terrorism, espionage or other criminal activity. To achieve this goal a security system provides the capability to DETECT, ASSESS, COMMUNICATE, DELAY AND RESPOND TO AN UNAUTHORIZED ATTEMPT AT ENTRY.

c. To meet the functional requirements of the physical security system specified above, several system components are identified, including the following:

(1) Integrated electronic security systems.

(2) Entry and circulation control.

(3) Barrier systems.

(4) Access delay and denial systems.

(5) Dedicated security forces.

(6) Designated immediate response forces.

By combining these physical security system components into an integrated protection system, appropriate levels of protection for United States defense resources can be achieved. It is also clear that such systems can be prohibitively expensive if applied to each and every DoD installation or facility within a DoD installation. Physical Security Protection priorities are therefore established.

4. DoD Asset Types and Protection Priorities

a. The DoD Regulation provides clear guidance on the priority for protection of installations, facilities, activities, organizations, or individuals based on the functions supported or carried out by each. The Regulation also prescribes the combination of physical security system components that can and should be used to achieve appropriate levels of protection. [redacted]

b. Figure 7-3 illustrates how physical security protection resources should be used to achieve the desired degree of protection for DoD's assets.

5. Specific Physical Security Policy Direction

a. Combining the concepts of a physical security threat, a physical security system that contains multiple components, and assets requiring protection, the DoD Regulation elaborates the following policy:

DELETED

Figure 7-3. Resource and Asset Priorities

It is DoD policy that DoD Components shall develop, establish, and maintain policies and procedures to control access to installations, including the following:

1. Using a defense-in-depth concept to provide graduated levels of protection from the installation perimeter to critical assets.
2. Determining the degree of control required over personnel and equipment entering or leaving the installation.

b. The Regulation also prescribes the development of plans, programs, and specific measures to enhance security to be implemented under the following situations: (emphasis added):

(1) National emergency.

(2) Disaster.

(3) TERRORIST THREAT CONDITIONS.[2]

(4) Significant criminal activity.

(5) Civil disturbance.

(6) Other contingencies that would SERIOUSLY AFFECT THE ABILITY OF INSTALLATION PERSONNEL TO PERFORM THEIR MISSION.

C. SUMMARY OF PHYSICAL SECURITY SYSTEM FUNCTIONS

1. The physical security system emplaced around DoD installations, facilities, activities, organizations, and even individuals must perform the following functions:

a. Detect threats;

b. Assess and classify threats;

c. Communicate warning and threat assessment information;

d. Delay penetration by the threat to the protected asset as long as necessary; and

e. Provide for timely, effective response to the threat.

2. In the discussion that follows in Chapters 8, 9, and 10, various approaches to enhancing physical security of DoD assets will be addressed. While many of the specific measures identified will be illustrated with examples based on DoD installations, the principles apply equally to all DoD activities regardless of their location.

---

2 See Chapter 17 and Appendix DD below for further discussion.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8

PHYSICAL SECURITY SYSTEM COMPONENTS

A. OVERVIEW

1. The physical security systems installed in and around DoD installations and facilities form the physical backbone of DoD combatting terrorism efforts. The facilities, equipment, and personnel comprising the installation security force are the first lines of defense against terrorist attack. DoD installation civilian managers and military commanders should develop an integrated physical security system as described in Chapter 7, consistent with the threat, in order to achieve the necessary levels of protection of DoD assets.

2. DoD 5200.8-R (reference (cc)) encourages the use of technology and people to achieve a cost-effective, security system level of performance. In this chapter, the basic components of a physical security system will be described. Security managers should bear in mind that cost-effective security systems designs use the minimum essential components to achieve the desired level of security; resource limitations and constraints mean that trade-offs will be required.

3. This chapter will consider the basic approach to the design and implementation of installation physical security systems. Each major component will be discussed. The chapter will conclude with a discussion of physical security system integration with other installation site selection and design issues.

B. LAYERED SECURITY CONCEPT

1. The DoD Physical Security Program Regulation emphasizes the need to think of physical security as a system providing protection-in-depth. In some cases defense-in-depth can be obtained by constructing "islands" of extreme or high security with a "sea" of moderate security.

2. The object of the physical security system no matter how it is described is the same:

a. Retain operational capability and mission functionality by providing the greatest level of protection to those resources necessary and sufficient to meet specified operational and/or mission requirements.

[redacted]

3. As noted in Chapter 7, protection of DoD assets is provided by a Physical Security System consisting of the following major components:

a. Integrated electronic systems.

b. Entry and circulation control.

c. Barrier systems.

d. Access delay and denial security systems.

e. Dedicated security forces.

f. Designated immediate response forces.

4. Figure 8-1 illustrates the general, layered defense approach to the implementation of a physical security system. The DoD asset(s) to be protected are located within an innermost ring of security. Additional layers of security are provided at increasing distances from the asset to be protected. The number of layers, the components that comprise them, and their resistance to penetration depend on the threat and the importance of the asset to be protected.

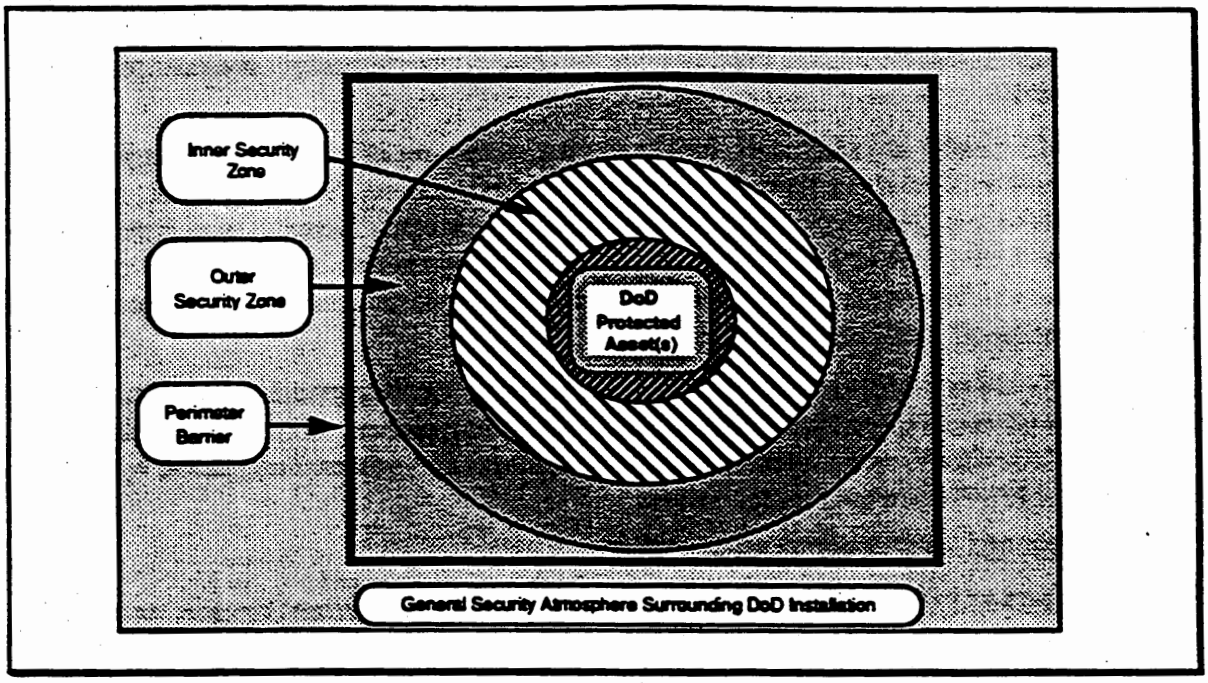


Figure 8-1. Layered Approach to Protection of DoD Assets

5. Figure 8-2 illustrates the concept of layered, integrated physical security system components contributing to the security of a DoD asset. An outer perimeter is established and clearly marked. Just inside the outer perimeter is an outer security zone. Within this zone are surveillance systems to monitor activities within the zone and beyond the perimeter. Access control points have been constructed to control access from outside the perimeter to the outer security zone. [redacted]

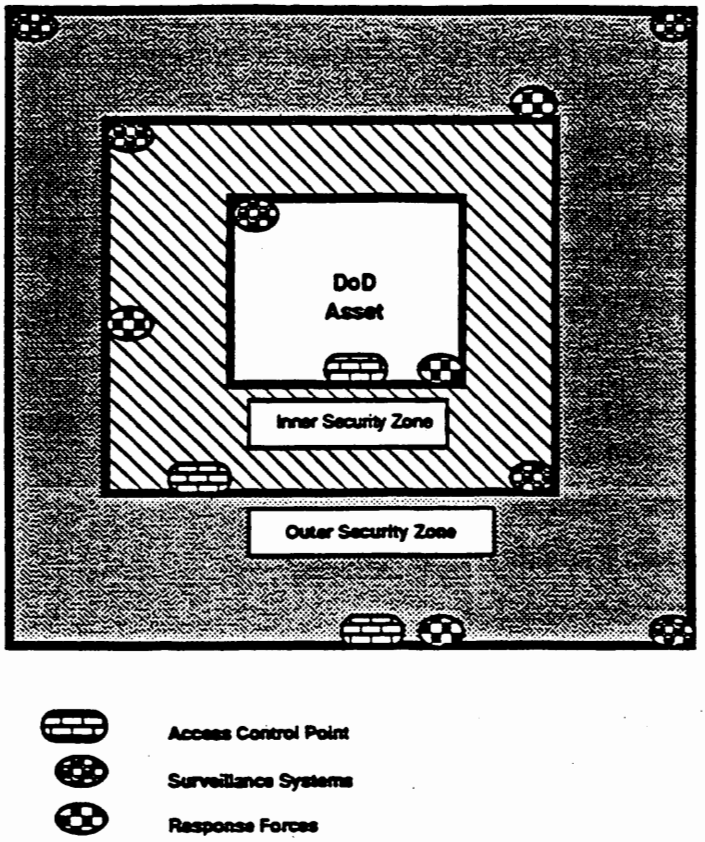


Figure 8-2. High Security Illustration of the Layered Security Concept

[redacted] It illustrates integration of multiple technical and human physical security system components into a physical security system that can provide high resistance to penetration, prolong an attack against protected DoD assets, and delay attackers long enough to permit a response force to arrive in time to apprehend and/or detain the perpetrators, recover assets, and restore them to their secured status.

7. Figure 8-2 depicts key physical security system components and an approach to the integration of these elements into a physical security system that can detect threats; identify, classify, and assess intrusions; delay intrusions long enough to permit response forces to arrive and complete containment and apprehension; and if all else fails, delay intruders still longer until overwhelming force arrives to rescue and/or recover the asset.

8. The concept of a layered defense also includes protection from threats launched against DoD assets from any direction. Threats could come from below or above, as well as through perimeter fences, walls, or other barriers. Underground parking garages in office buildings, high-rise apartments, and hotels can harbor terrorists, as can large utility

service structures such as tunnels, culverts, canals, or spillways. Ceilings or roofs can be penetrated and must also be protected. Even wide open spaces on a large installation can represent potential danger for terrorists equipped with hang-gliders, ultralight aircraft, parachutes, or even helicopters.

9. Most DoD assets do not require and should not be protected to the level depicted in Figure 8-2; if circumstances require such protection, use of the physical security systems concept allows for identification of temporary or expedient measures that can be used to increase protection afforded to DoD assets for the duration of a transient threat.

C. PHYSICAL SECURITY SYSTEM FUNCTIONAL REQUIREMENTS

1. General

a. For a physical security system to protect DoD assets, certain security functions must be performed. Among these functions are the following:

(1) Threat Detection.

(2) Threat Classification and Assessment.

(3) Threat Annunciation.

(4) Threat Delay.

(5) Threat Response.

b. Each of these functions is critical to the overall performance of the Physical Security system. Each is considered in turn.

2. Threat Detection

a. The first challenge to the physical security system is its ability to detect the presence of hostile intruders. As a general rule, the earlier the detection of threats and the longer the range at which they are detected, the greater the opportunities are to protect DoD assets and minimize the impact of terrorist acts against DoD personnel, materiel, and facilities. A wide variety of systems can be used to detect the presence of activity at a distance from the facility. The ability of surveillance systems to detect activity can vary widely. Several factors can influence surveillance system performance.

[redacted]

[redacted]

e. The number and variety of surveillance sensors can be affected by the location of initial threat detection. If a threat can be detected at the outer perimeter, then additional sensors can be used between the outer perimeter and the inner perimeter to aid in the classification and assessment of the intruder before the response force is dispatched. If the installation or facility is compact and little distance separates the outer perimeter from an inner security zone, then the response force must be dispatched almost immediately upon detection of an intrusion so that it can complete assessment and make an initial response.

f. Barriers such as fences, walls, ditches, or roads become platforms on which intrusion detection system sensors are mounted. Such systems can detect the passage of an object, animal, or person through a line. They can be used to detect the presence of intruders within a restricted zone such as sand strip encircling the perimeter of a facility. They can detect the presence of intruders in a restricted volume of space such as an office, a garage, or a hangar. Intrusion detection systems are especially useful within an installation, and oftentimes can be used in conjunction with perimeter barriers, security zones, and interior barriers to provide detailed information about the location of a potential threat.

g. If the geography and siting of an installation do not permit detection of threat at its periphery as is the case when DoD facilities occupy only a portion of a commercial office building, then threat detection must occur at close quarters to the protected DoD asset. Under such circumstances, multiple intrusion detection systems, based on different detection principles, can be employed to provide threat detection and additional information needed for classification and assessment as discussed below.

h. Detection systems have varying strengths and weaknesses depending upon the physical climate and environment in which they are expected to operate, the nature of targets to be detected, the training and skill of their operators and interpreters of data, and the topography and geography of the installation or facility from which surveillance is being mounted. Careful planning is necessary to install a surveillance system at the installation or facility perimeter with capability of providing both outward and inward surveillance. Planners should consult with Service and OSD experts with respect to their site-specific needs.

3. Threat Annunciation

a. It is, of course, not sufficient to detect the presence of potential threats. The physical security system must take additional steps to mitigate the threat.

b. A critical component of the physical security system is threat annunciation.

(1) Threat annunciation must occur in some type of watch center from which initial attempts to classify and assess the threat will be made.

(2) In some DoD facilities where most stringent security requirements must be met, threat annunciation may also be needed in a response force ready-room, where members of the response force remain in an alert state, prepared to respond to identified threats.

(3) Threat annunciation in the immediate quarters or offices of key personnel who are considered protected DoD assets, or other DoD assets may also be necessary to permit transitioning them into a highly protected physical structure (sending key personnel to a safehaven, pulling aircraft into hardened shelters and revetments, etc.)

c. While the annunciation of threat need not occur simultaneously in these locations, the physical security system must have a way of communicating the need for action to personnel assigned to assess or respond to threats. Annunciators can be **auditory** (alarm bells, whistles, horns, etc.), **visual** (flashing lights, blinking and/or color marks appearing on computer screens), or even **tactile** (vibrating units worn as pocket pagers).

d. It is recommended that at least two different types of annunciators be used throughout an installation where resources permit and a requirement for rapid security response exits.

e. Annunciators should be scattered throughout an installation to enable assessment personnel to summon response forces and to alert protected assets to an imminent attack. Intercom systems, portable radios, telephones, and radio paging devices can be used to alert specific personnel or specific facilities. Bells, whistles, sirens, and flashing lights can be used for general alarms.

f. Where the threat environment and resources warrant, installations should be fitted with general annunciators that allow personnel to discriminate among different types of emergencies. One set of alarms should be used for emergencies requiring the evacuation of facilities (fire or bomb threats). Another set of alarms should be used to warn of emergencies that require taking shelter in interior building spaces away from windows and exterior walls as in the event of civil disturbances or tornadoes.

4. Threat Classification and Assessment

a. Once the presence of a threat has been detected and threat assessment personnel notified, the physical security system must classify and assess the threat. The presence of a threat is usually detected as a result of some sort of alarm. Surveillance systems, including but not limited to visual surveillance systems and intrusion detection systems, transmit data to an information processing center, where detection data are assessed.

b. Assessment of and response to alarms must be swift and as practiced as possible. An intruder running can cover considerable distance in a matter of seconds. Guards and other security personnel are relied upon primarily to assess intrusion alarms. They must respond immediately when alerted. Often, security personnel use CCTV to assist them in their assessment role. CCTVs can also be slaved to the Intrusion Detection System (IDS) system. When a sensor alarms on a slaved system, a CCTV camera is immediately focused onto the alarmed area and the picture focused for the security guard monitoring the IDS system for assessment.

c. The purpose of such assessments is to determine the following:

(1) Is the alarm real or false?

(2) If the alarm was real, is the intrusion hostile or benign?

[redacted]

5. Threat Delay

a. Delay is provided by perimeter, exterior, and interior physical barriers erected or installed to protect the structure, such as fences, gates, walls, windows, doors, locking systems, ceilings, and floors. These physical barriers are evaluated as a system. The effectiveness of a barrier system is measured by the minimum total delay time it provides on any path into the protected area. Delay time is measured from the time the intruder is detected until he has penetrated all of the barriers, including the time it takes to travel from barrier to barrier, and the protected area.

b. Delay has three purposes:

(1) Facilitate definitive threat classification and assessment.

(2) Facilitate response by physical security response forces.

(3) Facilitate evacuation of protected DoD assets if evacuation is the most appropriate, cost-effective force protection remedy.

c. Delay of potential threats at the greatest distance possible from the protected DoD assets can be essential in making definitive threat classifications and assessments. Being able to delay intruders at the installation perimeter long enough to classify the threat (human) and assess it (not carrying firearms) may prevent unnecessary injury or loss of life.

d. Delay allows the response force an opportunity to take up defensive positions to protect DoD assets, to defend facilities and personnel, to counterattack, and to conclude an incident with arrest and apprehension of the perpetrators. The greater the amount of time intruders can be kept away from major DoD assets requiring protection, the greater the opportunity for DoD personnel to terminate the threat without loss or compromise of mission capability.

e. Delay can be critical in facilitating the successful evacuation of DoD assets from facilities under attack. Delay to facilitate evacuation is especially important to DoD personnel serving in isolated posts.

6. Threat Response

a. Response to threats begins immediately upon detection; response activity increases concurrently with threat classification and assessment. The purposes of the physical security system response to threats are as follows:

(1) Stop further intrusion by the threat at the greatest distance possible from protected assets;

(2) Slow the rate of advance towards the protected asset as much as possible;

(3) Facilitate the evacuation of the protected asset to safe areas;

(4) Secure the protected asset and contain the threat;

(5) Contain the threat, prevent additional hostile resources from arriving, and prepare to apprehend the threat and relieve the protected asset.

b. Specific methods to accomplish these response goals are discussed in Chapter 15. In general, physical security design elements included in DoD installations and facilities can aid response forces in accomplishing these objectives. [redacted]

D. BARRIERS

1. Barriers are an integral part of all physical security systems. They are used at the perimeter of DoD installations to perform several functions. Barriers establish boundaries. They deter and intimidate individuals from attempting unlawful or unauthorized entry. Barriers become platforms on which more sophisticated sensors can be placed to aid in threat detection and classification. Some barriers at the perimeter of a DoD installation help shield activities within the installation from immediate, direct observation.

2. Barriers are also used at the perimeter of DoD installations to facilitate pedestrian and vehicle entrance and exit control. Use of barriers channels traffic through designated access control points, where pedestrians and vehicles can be monitored and searched for contraband, explosives, or other threats as circumstances warrant.

3. Barriers are used within individual buildings on DoD installations for similar purposes. In addition, use of high security doors, window glazings, and walls can provide building occupants with protection against ballistic penetrations--small arms fire, bomb fragments, broken glass, etc.

4. Figure 8-3 presents an illustrative list of both natural and man-made barriers of potential interest to security program planners.

5. Specific permanent, temporary, and expedient barrier materials are discussed in Chapters 9 and 10.

BARRIER FUNCTION	Natural Obstacle Naturally Occurring	Man-made or Result of Human Endeavor
Establish Boundary	River, valley, forest line	Wall, fence, hedge
Isolate Activity, Discourage Visitors	Mountains or hills, jungle, dense growth, desert	Walls, fences Berms, canals, moats
Aid Detection of Unauthorized Entry, Intrusion		Electronic detection devices mounted on boundary Sand strips at boundary of areas to be isolated Electronic Devices
Impede Pedestrian Passage	Rivers, swamps, natural terrain features	Fences and walls with or without doors or gates
Impede Vehicle Passage	Rivers, swamps, natural terrain features	Fences, walls, Jersey Bounce barriers, Specially designed vehicle barriers Aircraft arresting cable
Prevent External Visual Observation	Forests, natural terrain features	Berms, earthworks Walls, solid fences Masonry block screens Translucent glass block, polycarbonate sheet Shutters, awnings, draperies
Minimize Ballistic Material Penetration		High berms, earthworks Steel reinforced concrete or masonry walls Blast shields fabricated from steel-ply materials Ballistic resistant glazings

Figure 8-3. Security Barrier Functions and Illustrative Examples

E. INTRUSION DETECTION SYSTEMS (IDS)

1. IDS Overview

a. Intrusion Detection Systems (IDS) are used to accomplish the following:

(1) [redacted]

(2) Provide additional controls at critical areas or points.

(3) Substitute for other physical security measures which cannot be used because of safety regulations, operational requirements, building layout, cost or similar reasons.

(4) Provide insurance against human error.

(5) Enhance the security force capability to detect and defeat intruders.

(6) Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

(7) There are four types of IDS:

(a) Local Alarm

In this system, the protective circuits and alarm devices actuate a visible or audible signal in the immediate vicinity of the detected intrusion, usually on the exterior of the building. The alarm transmission and/or communication lines do not leave the building. Response is by local security forces that may be in the area when the alarm is sounded. [redacted] This system should be used only when guards can respond in a timely manner.

(b) Central Station

In this type of system, the operation of alarm devices and electrical circuits are automatically signalled to, recorded in, maintained, and supervised from a central station owned and managed by a commercial firm with guards and operators in attendance at all times. These personnel monitor the signals and provide the response force to any unauthorized entry into the protected area. [redacted]

(c) Police Connection

In this type of system, the alarm devices and electrical circuits are connected via leased telephone company lines to a monitoring unit located in nearby civilian police stations. An agreement with the local police department must be arranged prior to establishment of this type of system.

(d) Proprietary IDS Station

1 This system is quite similar to a Central Station operation, except that the IDS monitoring and/or recording equipment for all IDS at the installation is located within a constantly manned DoD civilian or military police, or security force communications center maintained and owned by the Government installation. The installation police or security force responds to all IDS activations. [redacted] If a computerized IDS is used, it must be safeguarded against tampering.

2 DoD facilities equipped with IDS should utilize Proprietary IDS Station systems where DoD personnel monitor and respond to all alarms.

2. IDS Sensors

Intrusion Detection Systems have several components including sensors, data transmission subsystems, displays and assessment subsystems, power subsystems, communications subsystems, and maintenance systems. Intrusion detection system (IDS) sensors are divided primarily into two groups, exterior sensors and interior sensors, depending upon their environmental capability.

a. Exterior Sensors

(1) Exterior sensors are those that function in an outside environment. These sensors, and their associated processing equipment, are weatherproofed and less sensitive to changes in climatic conditions. Exterior sensors are used for early detection of intruders before they reach a protected structure. They are designed to provide fairly uniform protection coverage over outdoor areas. Exterior sensors are used to establish an intrusion detection line along fences, walls, and water or other land boundaries surrounding a protected structure.

(a) Perimeter Sensors

Perimeter sensors are exterior sensors normally installed on fences, walls, or gates. They detect different types of fence movement resulting from an intruder climbing, cutting, lifting up, or otherwise violating the fence. They can also be used within structures to establish inner security zones or to monitor movement within a large, open structure.

(b) Line Sensors

These exterior sensors form an extended boundary through which intrusion can be detected upon breaking or interfering with the sensor line, passing through a magnetic field, or changing the pattern in a electronic field.

(2) Figure 8-4 lists various types of exterior sensors.

[redacted]

Figure 8-4. Exterior IDS Sensor Types

b. Interior Sensors

(1) [redacted]

(2) Sensors use various methods of detection. Among the most common, exterior sensors use seismic, magnetic, microwave, infrared, electric field, electromagnetic,

and vibration detection methods. Interior sensors primarily use capacitance, magnetic, ultrasonic, shock and/or vibration, and infrared techniques. Combinations of these methods may also be designed into individual sensors. They can be configured in electronic tiers, requiring an intruder to pass through each tier in progressive succession, thereby increasing the likelihood that the intruder will be detected.

(a) Penetration Sensors

These interior sensors are designed to react to mechanical or acoustical vibration, sensor movement, or sensor destruction.

(b) Volumetric Sensors

Volumetric sensors are interior interior type sensors are designed to react to the motion of an intruder. They may based on infrared, seismic, acoustic, or sensing technologies.

(c) Duress Switches

Duress switches, like those used in banks, set off an alarm at the touch of a button. They allow individuals to communicate situations of duress to forces that can render assistance. Both fixed and portable switches can be used in this application. Fixed duress switches are normally wired to the IDS duress circuit and are permanently mounted for activation of the duress alarm when needed. Portable hand duress switches electronically transmit to a receiver that is wired to the IDS duress circuit. Upon activation of a switch button, the small, wireless transmitter sends a radio signal to the receiver, triggering a duress alarm. Transmitters are designed either to be carried or mounted in suitable locations.

(3) Figure 8-5 provides a listing of several different types of interior intrusion detection sensors, the purposes for which such sensors are appropriate, the principles by which each sensor operates, common false alarm causes, and appropriate applications.

3. Data and/or Signal Transmission

This subsystem links sensors with control and monitoring consoles. The transmission medium is used to send control signals and data to and from all sensors, control points, and annunciator panels. This subsystem may be hardwired land lines, radio frequency links, fiber optic cables, or any combination thereof. Most recently, transmission of data-encrypted alarm signals via satellite has been developed and is now available commercially.

4. Annunciator, Control, and Display

Annunciator, control, and display subsystems provide equipment for central operational control and monitoring of the IDS. Through this equipment, security force personnel are instantly alerted to the status of any protected area. This subsystem should be located in a restricted area and closed off from public view. Alarmed spaces should be designated by zones to facilitate identification of penetrated areas, assessments of vulnerability resulting from intrusions, and dispatch of response forces in a timely manner.

DELETED

Figure 8-5. Selected Interior Intrusion Detection Sensors

DELETED

Figure 8-5. Selected Interior Intrusion Detection Sensors (continued)

5. Primary Power

a. In the selection process, a planner must ensure that an IDS is capable of operation on the power (frequency and voltage) that is available. Within the United States 60 Hz (cycles) and 110 volts alternating current (ac) is the standard. Outside CONUS, frequencies may be 50 Hz or 60 Hz and voltages can range from 110V to 440V, in any combination.

b. In many overseas areas, line voltages can fluctuate widely and voltages for a 240-volt system can drop to 180V then surge to near 300V. Where this occurs, surge arrestors and line conditioners will be required to protect the IDS equipment. If the system selected is not capable of operating on available power, then some means of converting the power to a usable form must be provided. Sufficient power must be available to operate the equipment in each area to be protected as well as the control monitoring station. The power required by each item of equipment must be included in determining the total system load.

c. Many sensors and display units operate on direct current (dc). When these are used, it is necessary to provide sufficient dc power rectifiers at each location to convert

locally available ac power to the dc power required by the sensors and display units. Many of today's control units and sensors use microprocessors to accomplish their function. Although powerful in performance, they are susceptible to damage from electrical transients such as surges or spikes that result from interference or noise on the power line. This vulnerability can be reduced through the incorporation of surge protectors and/or lighting arrestors in the design.

6. Emergency Backup Power

a. The IDS must be capable of providing protection even when the primary power fails or is cut off. To ensure this, an alternative power source must be provided. If there is an uninterruptable power supply (UPS) available, then connecting the IDS to the UPS should be a prime consideration. Most systems contain a back-up battery that is continuously trickle-charged by the primary power system. An 8-hour battery backup is mandatory. However, if the primary power is subject to being out for longer periods, a 16- or 24-hour backup should be procured or arrangements made to provide a guard force as additional protection.

b. Use of an emergency backup generator can provide the necessary power when the primary power fails. Battery backup is still required to keep the system up until the generator is started. Expected power outages, system load requirements, and fuel availability will determine the capacity and type of generator required.

7. Tamper Protection

Protection from tampering with the IDS, the access system, and the assessment system should be designed into components of these systems so their effectiveness cannot be compromised. In typical applications, a switch is located within equipment covers or doors that are vulnerable to unauthorized entry. A tamper alarm is registered at the annunciator panel when a cover or door is pried off or removed.

8. Alarm Assessment

a. Alarm assessment is an essential function of a physical security system relying on intrusion detection systems. IT IS IMPERATIVE THAT THE CAUSE OF THE ALARM BE INVESTIGATED. Accurate and rapid assessment is essential to prevent the commitment of response forces as a result of false or nuisance alarms.

b. When an intrusion alarm is received, security personnel must assess the validity, severity, and nature of the event causing the alarm. Visual methods are commonly used, either by direct sighting or by the use of Closed Circuit Television (CCTV).

[redacted]

[redacted]

10. IDS Maintenance

a. Requirements

Proper maintenance of an IDS is essential. Systems not properly maintained may fail to detect intrusion or yield a high number of false and/or nuisance alarms, thereby losing credibility and demoralizing the security force to the point where alarm activations are often ignored. As a result, security may be less than that obtained without an IDS. The more complex an IDS, the more highly skilled and trained the maintenance technicians must be. The number of technicians required to maintain and IDS depends upon the system's complexity and reliability. [redacted]

b. IDS Testing Frequency

[redacted] All individual [redacted] should be tested to determine the continued adequacy of their intended application. All transmission devices will be validated to ensure proper operations. Testing should be conducted in concert with the security officer. Tests should include temporary interruption of AC power to ensure AC/DC transfer and that batteries or other alternate power sources are functional. Test result records should be retained consistent with Service, Agency, or Inspector General requirements.

F. LIGHTING SYSTEMS

Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. Adequate lighting for all approaches to an installation not only discourages attempted unauthorized entry, but also reveals persons within the area. However, lighting should not be used alone. It should supplement other measures such as fixed security posts or patrols, fences, and alarms.

1. Protective Lighting Approaches

a. Good protective lighting is achieved by adequate, even light upon bordering areas, glaring lights in the eyes of the intruder, and relatively little light on security patrol routes. In addition to seeing long distances, security forces must be able to see low contrasts, such as indistinct outlines of silhouettes, and must be able to spot an intruder who may be exposed to view for only a few seconds. All of these abilities are improved by higher levels of brightness.

b. In planning protective lighting, high brightness contrast between intruder and background should be the first consideration. The volume and intensity of lighting will vary based on the surfaces to be illuminated. Dark, dirty surfaces, or surfaces painted with camouflage paint require more illumination than installations and buildings with clean concrete, light brick, or glass surfaces. Rough, uneven terrain with dense underbrush requires more illumination to achieve a constant level of brightness than manicured lawns.

2. Types of Lighting

a. Continuous Lighting (Stationary Luminary)

[redacted] It consists of a series of fixed lights arranged to flood a given area continuously during the hours of darkness with overlapping cones of light. Two primary methods of employing continuous lighting are glare protection and controlled lighting:

(1) Glare Projection Lighting

Glare projection lighting is useful where the glare of lights directed across surrounding territory will not be annoying to neighbors or residents and not interfere with adjacent operations. It is a strong deterrent to potential intruders because it makes it difficult for them to see the inside of the area. It also protects guards by keeping them in comparative darkness. Such lighting allows guards to observe intruders at considerable distance beyond the perimeter.

(2) Controlled Lighting

Controlled lighting is best used where it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railroads, navigable waters, or airports. In controlled lighting, the width of the lighted strip can be controlled and adjusted to fit the particular need, such as illumination of a wide strip inside a fence and a narrow strip outside; or floodlighting a wall or roof. This method of lighting often illuminates or silhouettes security personnel as they patrol their route.

b. Standby Lighting (Stationary Luminary)

The layout of this system is similar to continuous lighting. However, the luminaries are not continuously lighted, but are either automatically or manually turned on only when suspicious activity is detected or suspected by the security force or alarm systems.

(1) Building Face Perimeters

Building face perimeter lighting illuminates the faces of buildings on or within 20 feet of the property line, or the area line to be protected, and where the public may approach the buildings. Guards may be stationed inside or outside of the buildings. Doorways or other insets in the building's face should receive special attention for lighting to eliminate shadows.

(2) Active Entrances

Active entrance lighting for pedestrians and vehicles should have two or more lighting units with adequate illumination for recognition of persons and examination of credentials. All vehicle entrances should have two lighting units located to facilitate complete inspection of passenger cars, trucks, and freight cars as well as their contents and passengers.

(3) Semiactive or Inactive Entrances

Semiactive or inactive entrances should have the same degree of continuous lighting as the remainder of the perimeter, with standby lighting of sufficient illumination to be used when the entrance becomes active. Gatehouses at entrances should have a low level of interior illumination to enable guards to see better, increase their night vision adaptability, and avoid making them targets.

c. Movable Lighting

A movable lighting system (stationary or portable) consisting of manually operated searchlights that may be lighted during hours of darkness or as needed. This system is normally used to supplement continuous or standby lighting.

d. Emergency Lighting

Emergency light may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on alternative power sources, such as installed or portable generators or batteries.

3. Wiring Systems

Both multiple and series circuits may be used to advantage in protective lighting systems, depending on the type of luminary used and other design features of the system. The circuit should be arranged so that failure of any one lamp will not leave a large portion of the perimeter line or a major segment of a critical or vulnerable position in darkness. Connection should be such that normal interruptions caused by overloads, industrial accidents, and building or brush fires will not interrupt the protective system. In addition, feeder lines should be located underground (or sufficiently inside the perimeter in the case of overhead wiring) to minimize the possibility of sabotage or vandalism from outside the perimeter. The design should provide for simplicity and economy in system maintenance and should require a minimum of shutdowns for route repairs, cleaning, and lamp replacement. It is necessary in some instances to install a duplicate wiring system.

4. Power Sources

a. Power sources should meet the following criteria:

(1) Primary - usually a local public utility.

(2) Alternate - the following should be provided:

(a) Standby batteries or gasoline-driven generators may be used.

1 If cost-effective, a system should start automatically upon failure of outside power.

2 Must ensure continuous lighting.

3 May be inadequate for sustained operations; therefore, additional security precautions must be considered.

4 Tested to ensure efficiency and effectiveness. The frequency and duration of test depend on:

a Mission and operational factors.

b Location, type, and condition of equipment.

c Weather (temperature affects batteries very strongly).

(b) Located within a controlled area for additional security.

(c) Generator or battery-powered portable and/or stationary lights:

1 For use in a complete power failure.

2 Includes alternate power supply.

3 Available at designated control points for security personnel.

b. Under ideal circumstances, power supplies related to physical security systems should be routed to the installation along separate routes from other utility service. In addition, power supplies for physical security systems should enter each protected facility as well as each protected enclave or restricted area within a facility separately from other power and utility service.

5. **Control Systems**

Controls and switches for protective lighting systems should be inside the protected area and locked or guarded at all times. An alternative is to locate controls in a central station similar to or as a part of the system used in intrusion detection alarm central monitoring stations. High impact plastic shields may be installed over lights to prevent destruction by stones, air rifles, etc.

G. THREAT DELAY

1. Several specific barriers can be employed to delay specific types of threats. [redacted]

2. A number of techniques can be used to harden perimeter barriers with modest resistance to penetration. For example, erecting a ballistic barrier on the interior side of unreinforced masonry building walls can increase the wall's resistance to penetration by bullets, grenade fragments, and hand tools. While this type of structure would be likely to fail were explosives detonated immediately at its face or within a few feet to tens of feet, a ballistic liner can be used to increase resistance to penetration.

3. Doors and windows can also be hardened to increase their resistance to penetration. Techniques for hardening are discussed in Chapter 10.

4. Ceilings, floors, and roofs, particularly in residential structures, may require hardening in order to enhance the protective value of such structures. Techniques to accomplish such hardening are discussed in Chapter 10.

5. Other entrances, openings, or penetrations into installations, facilities, and structures can be hardened to make them more resistant to penetration. The effect of such hardening is three-fold.

6. Increasing the resistance of facilities and structures to resistance forces terrorists to change their mode of operation. It requires terrorists to spend more time conducting surveillance of their target. Hardening targets may force terrorists to acquire new tools, postpone their attacks, and increase their risk of exposure.

H. ASSESSMENT AND INCIDENT RESPONSE FORCES

1. [redacted] guards and other security personnel have three interrelated but very different functions to perform as part of their role in the physical security system.

2. First, they function as **barriers**. Their presence is a visible and often tangible reminder of harm that could befall an intruder who ventures on to a DoD military installation without proper authorization.

3. Second, guards are an **essential element** in the intrusion detection system. Typically, they are responsible for making an on-the-spot assessment of initial alarms. Their judgement will figure prominently in installation responses. The ability to assess an intrusion alarm as real or false is an important skill. The ability to determine that a real intrusion is benign or hostile is a life-threatening decision. Either the intruder or the guard force, or both are at risk if a miscalculation occurs.

4. Third, guards are usually the **initial response force** and are therefore responsible for initial incident control and containment in the event of a terrorist incident. The desire of terrorists to generate as much publicity as possible can be fulfilled or minimized depending upon the knowledge and skills of those guards who make the initial on-scene determinations surrounding a terrorist incident.

5. Guards are an essential element of the physical security system. Therefore, consider implementing the following measures when employing military personnel, civilian personnel, and civilian contractor personnel as part of a physical security system.

a. EXAMINE GUARD DUTIES AND RESPONSIBILITIES CAREFULLY; COMMUNICATE THE REQUIREMENTS OF THE JOB CLEARLY.

[redacted] Keeping the guard force informed, focused, and aware of job requirements and expectations will help the force do a better job and keep morale high. Identify surveillance, intruder detection, classification, and assessment problems and conduct regular as well as unscheduled exercises to keep the guard force sensitive to events and aware of their own environment.

b. PROVIDE GUARDS WITH TRANSPORT AND COMMUNICATION APPROPRIATE TO THE SIZE AND TERRAIN OF THE AREA TO BE KEPT UNDER SURVEILLANCE.

Consider supplying bicycles, mopeds, and motor scooters where foot patrols are especially long, difficult, or tedious because of local environmental conditions. [redacted]

c. USE PERSONNEL DRAWN FROM MIDDLE ENLISTED RANKS AND CIVILIAN GRADES AS WELL AS JUNIOR ENLISTED AND CIVILIAN PERSONNEL AS PART OF THE GUARD FORCE.

[redacted] Consider development of a rotating schedule in which all security and security related personnel are required to stand at least some period of guard duty each month.

d. KEEP GUARD PERSONNEL INFORMED OF THE THREAT.

One of the most frustrating aspects of being a guard is not knowing what one should be looking for. Consider arranging for special briefings for guard personnel on local threat matters. Even if the material is the same material available to others, brief guard personnel separately. Build **esprit de corps** wherever possible.

e. PROVIDE FREQUENT TRAINING OPPORTUNITIES FOR THE GUARD FORCE AND ENCOURAGE THEIR PARTICIPATION IN EXERCISE PLANNING, IMPLEMENTATION, AND EVALUATION.

(1) [redacted] ertheless, it can mean the difference between the satisfactory protection of DoD assets or the loss of assets, capability, and innocent lives. Guard force training, accompanied by other security forces who would operate jointly with the guard force during an incident, should be a recurring part of physical security system exercises.

(2) Guard personnel and other security personnel frequently bear much of the burden in standing inspections and participating in exercises. They often have insights based on their experiences that can improve physical security system response to stress and to specific threats. They also have concerns about command and control viewed from the perspective of those who receive orders. Including guard personnel in exercise planning and evaluation reinforces the value and importance attached to guard responsibilities by management and command. It also affords security planners additional perspectives that can result in improvements in the performance of guard and security forces.

I. SUMMARY

1. This chapter has described the basic components of the physical security system that protects DoD assets in accordance with DoD policy. The system must correctly detect, classify, and identify threats; it must issue warnings to protected assets to take additional measures, while meeting, containing, and resolving the threat. The physical security system relies on a combination of sensor technology, civil engineering techniques, barriers, and humans to perform these functions.

2. The purpose of a physical security system is to protect assets; it should be proportionate in acquisition and operating and maintenance costs to the value of the assets that it is protecting. High value assets--assets that are critical, make accomplishment of DoD missions vulnerable if they are successfully attacked by terrorists, and at risk--need greater levels of protection than low value assets. Physical security systems must be designed with specific threats in mind; excursions from anticipated threats to assess system level sensitivities and capabilities should and must be made to design a cost-effective physical security system. The existence of multiple technical and human physical security system components creates options to mix and match components against security needs. All components need not be used in all circumstances to create an effective physical security system.

3. [redacted]

CHAPTER 9

PHYSICAL SECURITY MEASURES FOR AN INSTALLATION

A. INTRODUCTION

1. The DoD Combatting Terrorism Program concept introduced in Chapter 1 emphasized preventive measures designed to reduce the likelihood of terrorist attack and mitigate its effects should it occur. [redacted]

2. This chapter will integrate the DoD combatting terrorism program concept with DoD physical security policy requirements to illustrate the application of a generic physical security system to common aspects of DoD installations and facilities to protect DoD assets against terrorist attack. Physical security planning should consider physical security threat as well as the integrated terrorist threat estimate. Care should be given to ensure plans are drawn broadly enough to be responsive to radical changes in the physical security threats.

3. Again, prudence must be exercised in the implementation of a physical security system design. While systems can be designed to meet the most stressful, conceivable physical security threats terrorist might attempt, the actual measures implemented should be selected on the basis of threat, risk, vulnerability, and criticality of assets to be protected. Sensitivity analysis should be performed to verify that the elements of the design to be implemented can respond to some growth in either the terrorist threat, the criticality of assets to be protected, or both. Planning for future growth and investing in facility infrastructure to support future growth at low incremental cost is prudent.

B. INSTALLATION AND FACILITY DESIGN

1. General Physical Security Considerations

a. The effectiveness of a physical security system depends on at least three factors. It depends upon the careful planning, development, and installation of physical security hardware and security procedures to:

(1) Provide early detection of an intrusion.

(2) A layered system of barriers that delay the intruder.

(3) An effective, timely, and practiced response force.

b. Major considerations for tailoring a security system to an individual installation or building include:

(1) Location of the installation and/or building

(a) On or Off Government property.

(b) Near perimeter or near center of installation and/or property.

(2) Availability and capability of local military and/or police and fire department personnel.

(a) Maximum response time.

(b) Firepower capability.

(c) Dependability.

(3) Availability and proximity of U.S. Government response force personnel.

(4) Reliability of utilities service for the protected location.

(5) Access routes in the vicinity of the protected building.

(a) Response force requirements.

(b) Escape routes for attackers.

(6) Cost of security system components.

(7) Status of Forces agreements, host-nation restrictions, lease restrictions, and legal considerations related to the safeguarding of DoD facilities overseas.

c. Questionnaires and survey instruments identified in Appendix C for use in facility vulnerability assessments are also useful in identifying physical security strengths and weaknesses for each installation. Portions of the survey instrument can be repeated as often as necessary to cover each building or special facility within each building as necessary.

d. The purpose of a physical security survey is to pinpoint the ability of an existing structure to support current or future DoD activities, given the range of threats that might be foreseen on the one hand, and type of assets to be installed in the facility on the other.

2. Functional Physical Security Objectives

a. In general, however, facilities and structures, whether built new for use by the Department of Defense, modified to meet new requirements, or simply occupied "as is," should meet the following functional security objectives:

(1) Physical and psychological boundaries (signs, closed doors, etc.) should establish four areas with increasing security controls beginning at the property boundaries. The areas are defined as: (a) perimeter--property boundaries; (b) exterior security zone (which may include building lobbies and loading docks or other work areas); (c) interior security zone (which may include general workspace for DoD personnel and contractors);

and (d) Category III or High Security (restricted and/or exclusion) areas (which may include executive offices, armories, communications facilities, computer rooms, etc.)

(2) Vehicular traffic signs should clearly designate the separate entrances for trucks and/or deliveries and visitors and employee vehicles. Control points should be provided near the site boundaries where feasible. Sidewalks should channel pedestrians toward controlled lobbies and entrances.

(3) All areas of the site should be either supervised or secured so unobserved access is not possible.

b. The physical security surveys should draw attention to specific, pragmatic issues which can affect the utility and cost of providing physical security to DoD personnel and DoD contractors.

c. The following are specific issues that can arise during the course of a physical security survey that can have tremendous impact on the dollar and operational cost of providing security:

[redacted]

3. Industrial Safety and Hygiene Considerations

a. There is a close interaction between installation physical security design and installation industrial safety and hygiene considerations. As a general rule, activities involving the utilization of hazardous, toxic, or explosive materials should be isolated from all other activities; they should be separated from each other as well. Fuel depots, storage sites for ammunition, medical waste, agricultural and industrial chemicals, and toxic and hazardous waste processing activities should be isolated from unrelated activities and from each other wherever possible. Utility service to hazardous, toxic, or explosive materials handling facilities should be redundant and isolated from other utility service to the installation or facility if at all feasible. This will ensure uninterrupted operation of systems

essential to the maintenance of health and safety and for the annunciation of emergency conditions.

b. Installation design and operations should be reviewed to ensure that day-to-day activities do not create situations in which the effects of a terrorist attack cannot be multiplied because of the industrial safety or hygiene implications of such an attack. For example, special antiterrorist protection may be necessary for facilities storing toxic or hazardous materials while awaiting removal or destruction.

4. Security Considerations For New Construction at New DoD Sites

Consolidation of DoD activities at home and abroad creates new opportunities to build some new facilities at entirely new DoD installations. Under such circumstances, the following general security considerations should be born in mind:

a. Topography

[redacted]

b. Siting

[redacted]

(6) Sufficient space for construction of an outer perimeter barrier or wall.

c. Future and Alternative Use Considerations

Although the type of assets to be installed in a new facility and the perceived physical security threat may not require all of the security measures identified above, it is important to remember that the Department of Defense typically erects structures which must stand for 25 to 100 years. During the life-cycle of such structures, their use may change radically. Accordingly, site selection should bear in mind the possibility that

stringent physical security measures which are land and/or structure intense may be required in the future. Land acquisition, soil tests, foundation plans, and major structural member plans should be examined from the perspective of potential, physical security equipment intense use to ensure that acquisitions and initial designs contain sufficient expansion capacity to adjust to changing uses and/or changing physical security threats and countermeasures.

d. Environmental Considerations

(1) New DoD facilities should be selected from sites that are located in areas where local vehicular traffic flow patterns do not impede access to or from the site. In seeking overseas sites, it is suggested that DoD activities be housed in a semi-residential, semi-commercial area where traffic is only moderate in volume and can be monitored without highly visible surveillance systems which might be offensive to the host-country neighbors.

(2) New DoD facilities should be located away from known natural hazards such as active geological faults, flood plains, steep hillsides known for mud slides and/or brushfires. Similarly, care should be taken to avoid sites suspected of severe environmental contamination, directly beneath usual takeoff and/or approach paths to civilian airports, adjacent to rail yards, locks, dams, large fossil fuel or nuclear power plants, or other structures that could endanger the facility were there to be a major accident or terrorist incident at the neighboring facility.

5. Security Considerations for Existing Structures

a. Consolidation of DoD assets has also created a situation in which several [redacted] Some of these facilities may have previously served DoD organizations. Other facilities may previously have been used by other U.S. Government agencies and departments. Still others may have hosted commercial activities unrelated to the U.S. Government. The following issues should be addressed as plans are made to relocate a DoD facility, activity, or organization to an existing structure.

[redacted]

2. Permanent Structures

Several permanent structures can be used as perimeters around an entire DoD installation, around enclaves within a DoD installation, or around an isolated building used solely to house DoD activities. Among the favored approaches are the following:

a. Walls

(1) [redacted] Perimeter walls and fences can serve many other functions. They are primarily used to accomplish one or more of the following:

(a) Provide a legal boundary by defining the outermost limit of a protected area.

(b) Assist in controlling and screening authorized entries into a protected area.

(c) Support detection, assessment, and other security functions.

(d) Cause an intruder to make an overt action that will demonstrate intent to penetrate the protected area.

(e) Serve as a ballistic shield against small arms fire, deny visual observation of activities being conducted within the enclosed area, and add an increased deterrence to scaling.

(f) Serve as a "stand-off" barrier to protect the structure from vehicle bomb blast effects.

(g) Channel visitors through an opening providing better access control.

(2) [redacted]

(3) Walls [redacted] may be worthwhile physical security system additions to DoD or U.S. Government installations at home or abroad.

(4) In using exterior walls to enhance security, several considerations must be addressed:

[redacted]

c. While each of the arrangements described above can be made reasonably secure, those at the top of the list can be made more secure (better surveillance and detection of intrusion, longer delay times, better protection of DoD personnel) at comparable or lower cost than those at the bottom of the list.

C. INSTALLATION PERIMETER BARRIERS

The first line of defense in any physical security system is usually some form of perimeter protection system. The perimeter of a facility is the outermost area over which the facility has control. In many cases, a simple sign defining an intangible boundary is sufficient to delimit the boundary of a DoD installation. This approach is often used where the expanse of the facility makes physical demarcation impossible or economically infeasible. In other cases, elaborate structures, such as fences or walls, are used to mark the outer boundary of a DoD installation. The following discussion is intended to introduce readers to the range of options available.

1. General Guidelines

a. An unobstructed area or clear zone should be maintained on both sides of and between permanent physical barriers. [redacted]

b. Perimeter protection systems can assume a wide range of forms, in addition to fences and walls. Waterways, forestation, ditches, berms, barricades, vehicle barriers (active and passive), difficult approach and/or exit routes, and lighting systems, are often used effectively in perimeter barrier systems. An IDS should be considered for the exterior perimeter to provide the earliest possible notification and identification of an intrusion.

(a) Walls should be at least several feet away from other structures [redacted]

(b) Walls should be built in a manner such that vehicles cannot park immediately adjacent to them, thereby affording potential intruders a platform from which to mount an attack.

CONSIDER THE USE OF ADDITIONAL TOPPINGS ON WALLS SUCH AS CONCERTINA WIRE, PICKET FENCES, MULTIPLE STRAND RAZOR OR BARBED WIRE, OTHER DEVICES TO INHIBIT EFFORTS TO VAULT OR GO OVER THE TOP OF THE WALL.

CONSIDER INSTALLATION OF BOLLARDS OR OTHER BARRICADES LESS THAN THREE FEET IN HEIGHT AT THE BASE OF THE WALL TO INCREASE STAND-OFF DISTANCE BETWEEN PARKED VEHICLES AND THE WALL TO AT LEAST 10 FEET.

b. Fences

(1) Fences are frequently used to establish boundaries between a perimeter of an installation and its surrounding area. Fences, particularly at military facilities, are typically standard metal chain link fences. Barbed wire and field fencing are often found at major installations and overseas, as well as wood fences.

(2) Chain link or woven metal mesh fences can be used to establish an outer perimeter. While SUCH FENCES GENERALLY PROVIDE LITTLE DELAY TIME FOR TRAINED, WELL-MOTIVATED INTRUDERS, they are important psychological barriers for many individuals who might seek to penetrate a facility "just for fun." CHAIN LINK FENCES ARE EXCELLENT PLATFORMS ON WHICH TO MOUNT SURVEILLANCE SYSTEMS AND INTRUSION DETECTION DEVICES.

(3) Chain link or woven metal mesh fences can be stiffened and made somewhat more resident to penetration by vehicles through use of several techniques. [redacted] These techniques can increase the resistance to vehicle penetration offered by such fences, thereby adding to the delay in penetration.

(4) Chain link fences can be topped with concertina wire, razor wire, or multiple strands of barbed wire. SUCH TOPPINGS can be useful in adding to the psychological barrier effect of a fen[redacted]

(5) PICKET FENCES are also economical and aesthetic. They may be constructed of wood, iron, or steel. While they are not usually a physical deterrent, they will keep a watchdog or other watch animals secured on the grounds while not providing a hiding place for an intruder. They PRIMARILY SERVE TO DELINEATE THE PROPERTY LINE to intruders and observers alike. Heavy steel picket fences installed with reinforced and well anchored concrete piers can provide an attractive barrier against light- to moderate-weight vehicle penetration. Such fences must have properly designed gates to be effective.

(6) Picket fences are also more suitable for residences than office buildings but in some cases picket fences may be installed along approaches to the office building to channel traffic along selected routes. Like other fences, picket fences provide excellent platforms on which to mount surveillance systems.

3. Temporary Barriers

a. Vegetation

Hedges and natural vegetation are both economical and aesthetic and blend into their surroundings. They provide a symbolic but practical delineation of the property line. Unless hedges are thick and covered with thorns or pointed leaves, they can be easily breached. Once breached, they can provide some degree of cover from exterior observation. The main disadvantage of hedges is the time required to grow to sufficient size, especially if a portion dies, and a continuing requirement for periodic maintenance. They are more suitable for residences than office buildings; however, hedges can be used in either situation when appropriate.

b. Portable Fencing

(1) Portable fencing can be used as a temporary perimeter to establish psychological barriers and to channel pedestrian and vehicle movement.

(2) Several portable fencing materials are available. Among the materials available on the commercial market are the following:

(a) Plastic netting.

(b) Rolled wooden slat and/or support wire fencing (snow fencing).

(c) Fixed panels of chain-link fencing materials supported by temporary posts anchored with cinder blocks or other stabilizing materials.

(d) Fixed panels of board-on-board wooden plank fencing or wooden stockade fencing supported by temporary posts anchored with cinder blocks or other stabilizing materials.

(3) Other materials available within DoD that can be used as portable fences include the following:

(a) Coils of concertina wire.

(b) Canvas panels supported by tent-posts.

(c) Plastic sheeting materials supported by tent posts, athletic equipment supports, etc.

c. Temporary Walls/Rigid Barriers

(1) Several temporary devices can be employed to establish barriers to high speed vehicle approaches to DoD installations and facilities. Among the devices available are the following:

(a) Concrete vehicle barriers (Jersey wall segments).

(b) Concrete or sand filled oil drums.

(c) Concrete bollards and/or planters.

(d) Steel or steel-reinforced concrete posts.

(2) These structures can be installed along approaches to DoD installations or facilities within an installation's boundaries in a manner as to force vehicles to make tight, slow turns before approaching gates or building entrances. These structures can also be used as temporary barriers to deny access provided that additional barriers are placed in front of areas to deny high speed vehicle penetrations.

4. Expedient Perimeter Devices

a. Under certain circumstances, it may be necessary to establish a perimeter for psychological purposes. Several commercially available materials can be used as well as other materials often found on DoD installations to accomplish the expedient erection of a perimeter and/or perimeter barrier.

b. To mark a perimeter, the following materials can be used:

(1) Painted line.

(2) Rope (cloth rope, steel cable, chain, etc.).

(3) Colored plastic tape (commercially available products come in multiple colors and are without lettering or contain warnings such as "caution," "construction area," "danger," "police line - do not cross," etc.).

(4) A line of sandbags, one or two bags high.

(5) Barricades, saw horses, empty oil drums, construction barricades, etc.

(6) Jersey walls or concrete vehicle barrier segments.

c. The purpose of establishing such perimeters is usually to channel movement by pedestrians and vehicles as an aid to threat detection. Use of expedient perimeters can establish security zones within an installation or facility, thereby facilitating threat identification, classification, and assessment. Use of some expedient perimeter devices can add delay to movement within an installation or facility, channeling vehicles and pedestrians through choke points, slowing movement, and giving security personnel additional time to survey and assess pedestrians and vehicles as they approach and proceed through check points.

d. Under some circumstances, use of expedient perimeters can add delay to pedestrian threats by changing the configuration of an approach to a building. Erecting "trip wire" barriers in front of doors to be secured after hours, or installing water-filled oil drums in a random pattern along a vehicle or pedestrian approach to a building can disorient or impede an intruder who has been unable to make last moment observations on changes to the approaches to the targeted DoD asset.

e. Vehicles in all sizes and configurations can also be used as expedient barriers. Parked bumper-to-bumper, vehicles provide an effective barrier to personnel engaged in routine activity. Most people will not attempt to vault a line of vehicles parked such that

their bumpers touch, nor will they usually attempt to pass underneath such a line. Large construction-type vehicles or armored vehicles can be very effective as supplemental barriers behind gates to installations or facilities. Vehicles parked randomly on open, straight expanses of road, aircraft taxiways, or runways can interfere with unauthorized use of those facilities.

D. VEHICLE BARRIERS

1. In recent years, all agencies and departments of the United States Government have taken active measures to restrict the ability of vehicles carrying explosives to reach buildings housing government personnel. The destruction of the American embassies in Kuwait City and Lebanon in 1982 and 1983, as well as the bombing of the Marine Barracks at Beirut International Airport in October, 1983, effectively sensitized DoD to the need for vehicle barriers to hold potential threats away from critical structures or outside critical installations.

a. Vehicle Barrier Types

Several types of vehicle barriers are available. These include the following:

(1) Active Barrier Systems

A barrier is considered active if it requires action by personnel or equipment to permit entry. Systems that move solid masses, impalers, beams, gates, tire shredders, and fences, and those that create pits or ramps, are active barriers. Vehicles (trucks, bulldozers, etc.) are active barriers if used in that mode in the access control system.

(2) Passive Barrier Systems

A barrier is passive if its effectiveness relies on its bulk or mass and it has no moving parts. Such systems typically rely on weight to prevent entry into a restricted area. Sandbags, highway medians (Jersey Bounce), angled posts, tires, and guardrails are examples of passive barrier systems.

(3) Fixed Barrier System

A barrier system is fixed if it is permanently installed or if heavy equipment is required to move or dismantle the barrier. Hydraulically operated rotation or retracting systems, pits, and concrete or steel barriers are examples. Fixed barrier systems can be either active or passive.

(4) Movable Barrier System

A movable barrier system can be transferred from place to place. It may require heavy equipment or personnel to assist in the transfer. Highway medians, sandbags (large numbers), 55-gallon drums (filled), or vehicles are typical examples.

(5) Portable Barrier Systems

A portable barrier system is used as a temporary barrier. A movable system can be used, but may take more time, money and effort than desired. Examples of portable barriers are ropes, chains, cables, vehicles, or tire-puncture systems.

(6) Expedient Barrier Systems

An expedient barrier system is comprised of one or more articles or vehicles normally used for other purposes that have been pressed into use on a temporary or interim basis. Use of heavy earth-moving or engineering equipment, armored personnel carriers, or tanks as perimeter gates or perimeter gate barriers are examples of expedient barrier systems.

b. Vehicle Barrier Design Considerations

(1) Location

Vehicle barriers can be located in different areas: facility entrances, enclave entry points (gates), or selected interior locations (i.e., entrances to restricted areas). Exact locations vary among installations; however, in each case locate the barrier as far from the critical resource as practical. When possible, position gates and perimeter boundary fences outside the blast vulnerability envelope or reposition the resource within the installation to a more secure area. It is more cost effective to secure a specific critical resource than an entire facility. However, consolidating critical resources into one central area may heighten security, but is also reduces the number of target areas for the aggressor to attack.

(2) Aesthetics

The overall appearance of a vehicle barrier plays an important role in its selection and acceptance. Many barriers are now made with aesthetics in mind so that a "fortress effect" can be avoided. [redacted]

(3) Safety

A vehicle barrier system should be respected as a tool capable of wielding deadly force. Even when properly installed to perform its intended purpose, it can kill or seriously injure individuals as a result of accidental or inadvertent activation caused by either operator error or equipment malfunction. Provide proper warning signs, lights, bells, and adequate colors to identify the barrier to ensure personnel safety. Questions such as the following should be addressed to manufacturers and current users to identify potential safety considerations affecting the selection of a barrier system. What happens when power is lost? Is there an emergency stop switch? Is lighting adequate? What safety options are available from the manufacturer? Once installed, vehicle barriers should be well marked and pedestrian traffic channeled away from unsafe areas.

(4) Reliability

[redacted] others have developed problems not anticipated by either the manufacturer or user. Many manufacturers indicate a remarkable willingness to resolve problems and work effectively with users. Backup generators or manual operating

provisions are available. Spare parts and supplies also should be maintained on hand to facilitate rapid return of the barriers to full operation.

(5) Maintainability

Many manufacturers provide aesthetics, diagrams, maintenance schedules, and procedures for their systems. They should also have spare parts available to keep barriers in nearly continuous operation. Manufacturers should be asked for maintainability requirements in the form of training, operation, and maintenance manuals. If these requirements are not available, the agency that purchases the vehicle barrier must develop maintenance instructions for the user. In addition, for periods of vehicle barrier maintenance, the user should consider providing alternate traffic routes.

(6) Cost

Traffic in restricted or sensitive areas should be minimized and the number of entryways limited. Reducing traffic flow and the number of entryways may provide increased security and lowered costs for the vehicle barrier system. Installation costs, which may be excessive, and the cost of operating the system should be addressed during the barrier selection process. Complexity and lack of standardized components can incur higher costs for maintenance and create long, costly downtime periods. Reliability, availability, and maintainability (RAM) data on the system also affect costs.

(7) Active Barrier Operations

A barrier is active if it requires action by personnel or equipment to operate. It should allow for continuous operation with minimal maintenance and downtime, so that it may be employed during normal and emergency conditions. Emergency procedures must be available to operate the barrier in case of system breakdown or power failure. Selecting a normally open or closed option should be evaluated in light of experienced or expected traffic. Evaluate system failure modes to ensure that the barrier fails in either the open or closed position, as dictated by security and operation considerations.

(8) Clear Zones

Barriers installed in clear zones must be designed so that they will not provide terrorists with a protective hiding place or shield.

(9) Operating Environment

The environment of the facility must be considered when selecting an appropriate vehicle barrier or barrier options. Hinges, hydraulics, or surfaces with critical tolerances may require heaters to resist freezing temperatures and ice buildup, or they may require protection from dirt and debris. If options that protect against environmental conditions are not available, the system may become inoperative.

(10) Installation Requirements

The vehicle barrier selected must be compatible with the location in which it is installed, the available power source and its reliability, and other security equipment.

PROTECTION OF PRIMARY AND ALTERNATE POWER SOURCES AND HYDRAULICS MUST BE CONSIDERED.

(11) Operator Training

Most users recommend operator training regardless of the simplicity of the system. Operator training prevents serious injury and legal liability as well as preventing equipment damage caused by improper system operation. Manufacturers do not always provide information on possible operator problems. The user may have to develop individual checklists for normal and emergency operating procedures to avoid experiencing serious problems.

(12) Manufacturers Options

Manufacturers offer additional features with their systems in the form of options or optional equipment. Some options enhance system performance while other facilitate maintenance or safety. Options increase system cost and may increase maintenance requirements. Because options vary among manufacturers, consulting with each company is advised to determine which options are offered and their cost.

2. In addition to the foregoing considerations, the following should also be considered when assessing vehicle barrier requirements and options:

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

f. [redacted]

g. [redacted]

E. PERIMETER BARRIER PENETRATIONS AND ACCESS CONTROL

1. Vehicle Entrance and/or Exit Barrier Penetrations

As a general rule, vehicle barriers described above should be placed outside the installation perimeter or outside an installation interior perimeter. The following discussion addresses vehicle access to an installation or facility once past the vehicle barrier(s) described above:

a. Installation Vehicle Access Control Measures

(1) RESTRICT VEHICLE ENTRY POINTS TO A MINIMUM.

Vehicular entry-exit points should be kept to a minimum. Ideally, to maximize traffic flow and security, only two regularly used vehicular entry-exit points are necessary. Both should be similarly constructed and monitored. The use of one should be limited to employees' cars. The second should be used by visitors and delivery vehicles. Depending on the size and nature of the facility, a gate for emergency vehicular and pedestrian exit should be installed outside the perimeter to increase the setback of the buildings. In either case, design and placement of bollards or other anti-vehicular devices should be considered in the early planning stages. [redacted]

(2) PROTECT ALL VEHICLE ACCESS POINTS AGAINST REVERSE ENTRY AND RAMMING ATTACKS.

(a) All entry-exit points should be secured with a heavy duty sliding steel, iron, or heavily braced chain link gate equipped with a heavy locking device. Approaches to all vehicle exit points should be aligned such that high speed approach from outside the perimeter is not possible. The goal of such realignment is to ensure to the maximum degree possible that intruders could not simply enter the facility by going the wrong way against the flow of exiting vehicle traffic. Passive vehicle barriers described above can be incorporated into the road and pedestrian access designs to accomplish this goal.

(b) All entry-exit points should be constructed with protection against a ramming vehicle attack. Passive vehicle barriers described above can be incorporated in ingress-egress designs to make ramming attacks difficult. Vehicle perimeter penetration gates can also be designed to be highly resistant to ramming attack. Additional vehicle barriers can be installed behind the gates to provide defense-in-depth against such attack.

(3) LOCK ALL GATES NOT IN USE AND UNDER DIRECT SUPERVISION; VERIFY THAT LOCKS IN PLACE BELONG TO AND CAN BE OPERATED ONLY BY SECURITY PERSONNEL.

Emergency gates should be securely locked and periodically checked. Security personnel should physically lock and relock all gates or other penetrations secured with locks to verify that the lock in use belongs to the security department and not some other activity on the installation or would-be intruders. Any lock found inoperable by the security personnel should be removed immediately and a security department lock substituted in its place. Control over keys is essential.

(4) INCLUDE STORAGE LANES, PROTECTED GUARD POSITIONS, AND HARDPOINTS FOR SECURITY GUARD BOOTHS TO PERMIT MULTIPLE VEHICLE INSPECTIONS FOR EXPLOSIVES, WEAPONS, OR CONTRABAND OUTSIDE THE INSTALLATION PERIMETER WHEN PREPARING PLANS FOR REVISED VEHICLE ACCESS.

(a) Some of the measures implemented at DoD facilities in response to terrorist threat may result in significant traffic congestion at vehicle entry gates. Such

congestion can be reduced if storage lanes can be included in installation access alignments. During periods of rigorous vehicle inspection, security personnel can inspect vehicles and their occupants in groups. Vehicles waiting their turn for inspection can be held in storage lanes adjacent to the installation. This approach to vehicle inspection and installation access will ease traffic congestion for those not seeking access to the DoD installation. It will also place vehicles and their operators waiting inspection in an area where they can be monitored for indications of potentially threatening behavior.

(b) Be sure that vehicle barriers, storage lanes, security booth tie down points, and protected positions for backup security forces are considered as an integrated security package. Doing so will ensure that vehicle barriers do not obstruct fields of vision and/or fields of fire for the backup security forces responsible for protecting guards conducting vehicle inspections.

b. Vehicle Access Control Systems

(1) Primary entrances to a facility should have a booth for security personnel during peak traffic periods and automated systems for remote operations during other periods.

(2) THE FOLLOWING CAPABILITIES ARE RECOMMENDED FOR VEHICLE ACCESS CONTROL SYSTEMS:

(a) Electrically-operated gates to be activated by security personnel at either the booth or security control center or by a badge reader located in a convenient location for a driver;

(b) CCTV with the capability of displaying full-facial features of a driver and vehicle characteristics on the monitor at security control center;

(c) An intercom system located in a convenient location for a driver to communicate with the gatehouse and security control center;

(d) Bollards or other elements to protect the security booth and gates against car crash;

(e) Sensors to activate the gate, detect vehicles approaching and departing the gate, activate a CCTV monitor displaying the gate, sound an audio alert in the security control center;

(f) Lighting to illuminate the gate area and approaches to a higher level than surrounding areas;

(g) Signs to instruct visitors and employees;

(h) Road surfaces to enable queuing, turnaround, and parking;

(i) Vehicle bypass control (i.e., gate extensions), low and dense shrubbery, fences, and walls.

(3) Vehicle perimeter access control barriers and gates should be controlled by key card or remote operation by the central security office when the gatehouse is not manned. An intercom and CCTV camera with low-light and area scan capability should be

provided to facilitate communication between the central security office and personnel in vehicles seeking entry when the access point is closed. The access point should be sufficiently illuminated such that all vehicle occupants can be seen via CCTV systems.

c. Perimeter Security Office Booth

(1) At the vehicular entry-exit, a security officer booth should be constructed to control access. At facilities not having perimeter walls, the security officer booth should be installed immediately inside the facility foyer.

(2) If justified by the threat the security officer booth should be completely protected with reinforced concrete, walls, ballistic doors, and windows. The booth should be equipped with a security officer duress alarm and intercom system, both annunciating at the facility receptionist and security officer's office. This security officer would also be responsible for complete operation of the vehicle gate. If necessary, package inspection and visitor screening may be conducted just outside of the perimeter security officer booth by an unarmed security officer equipped with walk-through and hand-held metal detectors. Provisions for environmental and personal comfort should be considered when designing the booth.

2. Parking

a. As a general rule, parking should be restricted to the areas that provide the least security risks to DoD personnel.

b. If possible, establish a visitor parking facility outside the installation perimeter. If space does not permit this, try to restrict visitor parking to an area as close to the main installation gate as possible. Conduct pedestrian screening between the visitor parking area and other sections of the installation if possible.

c. All parking within the perimeter walls should be restricted to employees, with spaces limited to an area as far from the building as possible. Parking for patrons and visitors, except for predesignated VIP visitors, should be restricted to outside of the perimeter wall. If possible, parking on streets directly adjacent to buildings, especially those housing highly valued assets, should be forbidden. [redacted]

d. When establishing parking areas, security of visitors as well as DoD personnel should be considered.

(1) AVOID EXTREMELY REMOTE PARKING FOR VISITORS.

(2) INSTALL AN EMERGENCY COMMUNICATION SYSTEM (INTERCOM, TELEPHONES, ETC.) INSTALLED AT READILY IDENTIFIED, WELL LIGHTED, CCTV MONITORED LOCATIONS TO PERMIT DIRECT CONTACT WITH THE SECURITY DEPARTMENT.

(3) PROVIDE PARKING LOTS WITH CCTV CAMERAS CAPABLE OF DISPLAYING AND VIDEOTAPING LOT ACTIVITY ON A MONITOR IN THE SECURITY CONTROL CENTER.

Lighting must be of adequate level and direction to support cameras while, at the same time, giving consideration to energy efficiency and local environmental concerns.

(4) CHANNEL PEDESTRIANS TOWARDS A PEDESTRIAN ACCESS CONTROL CHECKPOINT AND/OR INSTALLATION, FACILITY AND/OR BUILDING ACCESS CONTROL POINT.

(a) Fences, Jersey wall segments, low, thorny hedges, and other barriers may be used to guide pedestrians and maintain control over their movements.

(b) Although in-building or underground parking is to be strongly discouraged, there are circumstances in which there is no alternative. The following recommendations are made to enhance the security of building occupants.

(5) PROVIDE A COMPLETE VEHICLE CONTROL SYSTEM FOR THOSE BUILDINGS IN WHICH THE PARKING GARAGE IS INTEGRAL TO THE BUILDING ITSELF.

Provide nondescript vehicle ID that must be displayed before entering the garage; CCTV surveillance should be provided for employee safety and building security.

(6) ACCESS FROM THE GARAGE OR PARKING STRUCTURE INTO THE BUILDING SHOULD BE LIMITED, SECURE, WELL LIGHTED, AND HAVE NO PLACES OF CONCEALMENT.

Elevators, stairs, and connecting bridges serving the garage or parking structure should discharge into a staffed or fully monitored area. Convex mirrors should be mounted outside the garage elevators to reflect the area adjacent to the door openings.

3. Pedestrian Access Controls

a. Access control is primarily directed at decreasing exposure to criminal activity. Criminal opportunity can be reduced through design of a facility that restricts persons from areas where they do not belong. Access to an installation, a group of buildings, or a single building can be designed so that surveillance, control, and segregation of traffic by function are facilitated. Depending on the functions to be accomplished by the occupants, access points can be designed either to be closed during non-duty hours, or to be subject to surveillance and control for all-hours entry.

b. [redacted]

c. [redacted]

[redacted]

DELETED

Figure 9-1. Generic Pedestrian Access Control Point

4. Utility Penetrations and Security

a. The installation physical security survey should identify all utility service to the DoD installation, as well as all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities that may cross the installation perimeter. Detailed knowledge of such service is important for public health and safety considerations as well as installation security concerns.

b. All penetrations of the installation's perimeter should be clearly marked. All penetrations in fences, walls, or other perimeter structures should be screened, sealed, or secured to prevent their use as access points for unlawful entry into the installation. If access is required for maintenance of utilities, secure all penetrations with screening, grating, lattice work, or other similar devices such that no opening is greater than ten inches in diameter. Attach intrusion detection sensors and consider overt or covert visual surveillance systems if warranted by the sensitivity of DoD assets requiring protection.

c. Under some circumstances, it may be necessary to insert a large sleeve composed of multiple sections of pipe each no more than 10 inches in diameter into large storm sewer culverts or tunnels. This approach is illustrated in Figure 9-2.

DELETED

Figure 9-2. Installation of a Sewer Pipe Plug

d. This approach should be employed to block all other penetrations through the perimeter barrier that are large enough for a person to crawl through (i.e., more than 10 inches in diameter), but cannot be sealed closed for any reason. All such penetrations should be equipped with intrusion detection sensors or placed under surveillance.

F. EXTERIOR SURVEILLANCE AND/OR INTRUSION DETECTION SYSTEMS

1. As noted in Chapter 8, the physical security system's initial task is to detect the presence of threats to DoD personnel and materiel protected within the facility. A wide range of surveillance options should be considered, based upon the following:

a. Identified threats to the facility;

b. The types, function, operating characteristics, and missions of DoD assets to be protected;

c. Legal and diplomatic limitations on surveillance activities; and

d. Overall resource constraints.

2. Technology offers physical security system planners a wide range of sensors and phenomenology from which external surveillance systems can be assembled. Figure 9-3 indicates that surveillance systems readily available to local military installation

commanders capable of providing detailed visual images are somewhat less abundant than systems that detect the presence of a target but may not be able to report back the full particulars on the detected target. As the target of surveillance moves closer to the facility, it becomes possible to use guards with binoculars, CCTV or other electrooptical systems, or imaging infrared systems to detect the presence of terrorist threats.

DELETED

Figure 9-3. External Installation Surveillance Technologies

3. Electromagnetic energy sensor systems use radar to detect aircraft, sonar to detect water vehicles and swimmers, and laser radar to detect humans or vehicles. These systems can report surveillance targets in digital or analog formats. Such reports usually require additional interpretation by operators. Visual surveillance systems report data in image or photographic form, requiring less interpretation by surveillance system operators before surveillance information is assessed as threatening or benign. Visual surveillance systems are usually more limited in detection range than electromagnetic sensors. Many visual surveillance systems are passive devices. Their use does not require the emission of energy which could alert an intruder to the presence of surveillance systems. Visual surveillance systems have performance limitations due in part to ambient weather conditions that may require use of additional passive sensors. Such systems report information in a form that may necessitate more complex analysis before the detection of an intrusion can be classified as a threat.

4. SURVEILLANCE SYSTEM MONITORS NEED TO BE PROVIDED INFORMATION OR DECISION RULES THAT THEY CAN USE TO INTERPRET DATA PROVIDED BY ALL SURVEILLANCE SYSTEMS IN USE.

5. Figure 9-4 indicates some of the surveillance problems that installation guards and security officials routinely confront. External surveillance may detect the presence of general activity hostile to DoD assets; it may also detect the presence of activity or targets

at, near or beyond the perimeter barrier which behave in a peculiar manner. [redacted]

DELETED

Figure 9-4. External Installation Combatting Terrorism Surveillance Functions

6. [redacted]

7. On the other hand, it is clear that if external surveillance detects the presence of the threat at the perimeter barrier and is able to maintain contact with the threat, then classification of the threat and preparing an immediate response if the perimeter is penetrated is both easier and quicker.

8. Surveillance systems that combine detection systems registering the presence of a threat as well as detection systems that permit direct visual monitoring of the threat provide considerable information to installation threat assessment personnel. Multiple sensors arrayed in a grid patter from the perimeter barrier stretching in toward the center of the facility can provide the security force with much information necessary to classify and characterize the threat without forcing the guard force to leave secure positions. Surveillance systems often have a lower life-cycle cost. They can be hardened against the

elements to a substantial degree. It is not surprising to see more DoD components placing greater emphasis in IDS and other technical surveillance systems to meet their physical security system protection requirements. The advantages of technical surveillance are lost, however, unless IDS and other systems remain in top notch repair.

G. INSPECTION AND MAINTENANCE OF BARRIERS AND SECURITY SYSTEM COMPONENTS

1. Security force personnel should check security barriers at least weekly for defects that would facilitate unauthorized entry and report such defects to supervisory personnel. Inspections should look for the following maintenance problems which can have adverse implications for security:

a. Damaged areas (cuts in fabric, broken posts).

b. Deterioration (corrosion).

c. Erosion of soil beneath the barrier.

d. Loose fittings (barbed wire, outriggers, fabric fasteners).

e. Growth in the clear zones that would afford cover for possible intruders.

f. Obstructions which would afford concealment or aid entry and/or exit for an intruder.

g. Evidence of illegal or improper intrusion or attempted intrusion.

2. Locks should be opened and closed to verify that they are in working order and that the locks can be opened and closed by the guard or security force. Locks that cannot be opened by the guard or security force should be removed immediately and replaced with a DoD lock. An investigation should be undertaken to determine if apparent substitution of the security department lock was an error, an attempt to maintain security following loss or compromise of a lock, or an attempt to create a "trap door" through which terrorists could ingress or egress from a DoD facility.

H. RESPONSE FORCES

1. Another element of the physical security system that is easy to overlook is the response force. As is discussed in greater detail in Chapter 15, the response force consists of three elements:

a. Initial response force.

b. Locally available augmentation force (with or without reserves).

c. Regional and/or national special capability response forces.

2. It is imperative that response forces be assigned to tasks and otherwise housed in facilities that are in close proximity to but not necessarily within or immediately contiguous to targets of terrorist attack. While some elements of the response force can be assigned responsibilities for day-to-day protection of DoD assets, most members of the initial response force should be dispersed within a facility so that a terrorist attack cannot

eliminate the response force necessary to contain, regain control, and terminate an incident with the rescue and release of DoD personnel.

3. Consider taking the following specific measures:

a. PROVIDE SECURITY PERSONNEL AND OTHER RESPONSE FORCE MEMBERS WITH SECURE WORKPLACES.

Structures in which security personnel work should be hardened to increase the likelihood that personnel can survive if attacked, and at a minimum survive long enough to provid etailed information describing the nature of the attack on their posts.

b. PROVIDE SECURITY PERSONNEL AND OTHER RESPONSE FORCE MEMBERS WITH SECURE COMMUNICATIONS.

The ability for security personnel to communicate with the central security office and other security units in the field without interception and/or interference is critical to the detection, classification and assessment, and response to penetrations of facilities and further criminal acts.

c. PROVIDE SECURITY PERSONNEL WITH PROTECTED QUARTERS AND/OR REST AREAS.

It makes little sense for security personnel to work in a secure environment and then return to quarters that leave them vulnerable to attack and unable to respond if called. While providing secure quarters to a level of protection comparable to those provided to high risk personnel may not be feasible, a relatively secure area or facility should be established so that response forces can remain reasonably protected during off-duty hours during periods of extreme threat.

I. AIRFIELD COMBATTING TERRORISM SECURITY CONSIDERATIONS

1. Airfields represent special security challenges because of the unique character of the facilities and the DoD assets they support. All of the foregoing discussion applies to airfields. Airfield security planners may also wish to consider the establishment of multiple internal security perimeters, hardening of selected buildings against terrorist attack, hardening of petroleum storage, aircrew facilities, maintenance facilities, and other facilities collocated on the installation. Security planners are, of course, fully aware of DoD Regulations and Instructions, Service regulations and instructions, and CINC requirements for enhanced physical security protection for many types of munitions stored at DoD airfields.

[redacted]

stretches of pavement often requires substantial reconfiguration of the local topography, creating the need for extensive drainage and stormwater management systems.

3. [redacted]

4. Airfields are often adjacent to areas with substantial wildlife activity. Exterior intrusion alarm systems are prone to provide much data on movement that is regarded as false; i.e., non-human. [redacted]

5. Use of multiple phenomenology intrusion sensors is essential to the effective management of limited security personnel resources at airfields. Use of line detectors, motion detectors mounted on fences, seismic and/or acoustic sensors sown in patterns is critical. Multiple phenomenology IDS systems can permit alert center personnel to classify and identify an intrusion looking at reports from each type of sensor. Subtle differences are reported between human and animal interactions among different types of sensors. By laying out multiple sensors across a wide area, the differences between human and animal activity can be magnified allowing alert center personnel to determine if the intrusion is human or animal as well as the direction and rate of advance of the intruder. This information can be used to determine whether or not the security force must be dispatched, to what point they should go, and how quickly they must arrive at the designated interception point.

6. Another unique aspect of airfield security is the nature of the activity and the type of assets to be found there. [redacted]

a. CONSIDER ESTABLISHING OBSERVATION POSTS IN OFF-BASE AREAS BENEATH OR ADJACENT TO FLIGHT PATHS FOR LANDINGS AND TAKEOFFS.

Use of DoD personnel for law enforcement and security operations outside the perimeter of a DoD installation is tightly constrained by Federal statute within the United States, its territories, and its possessions and by SOFAs overseas. However, in many instances, it may be permissible to establish observation posts manned jointly by DoD

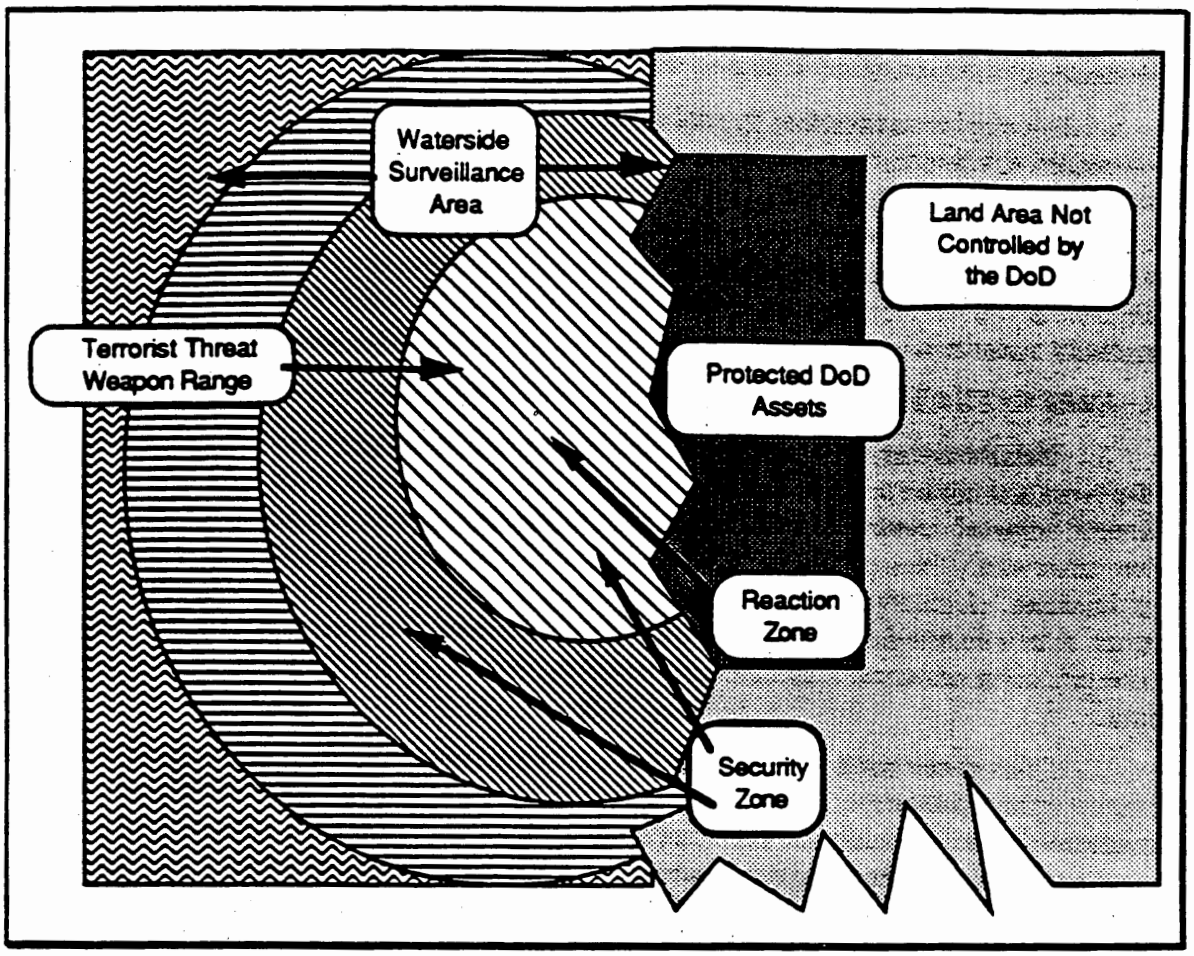


Figure 9-5. Waterside Terrorist Surveillance and Engagement Zones

8. It should be emphasized that DoD facilities bordering bodies of water should include waterside protective measures as part of the facility physical security plan, even if there are no active waterside commercial, military, or recreational facilities at the facility or installation.

K. EVACUATION FACILITIES

1. The purpose of a physical security system is to prevent the loss, destruction or compromise of DoD assets. Under some circumstances, this purpose can be best achieved by withdrawing the asset from locales where terrorist threats cannot be mitigated, or can only be mitigated at unacceptable costs. Under such circumstances, removal of assets may be warranted.

2. Security personnel should survey the area adjacent to DoD installations or facilities to identify potential sites for helicopter landing zones. If no appropriate site is available near DoD installations for facilities, appropriate alternatives should be identified.

3. In preparing plans for evacuation of DoD assets requiring maximum protection, the security personnel should consider construction of one or more safehavens in the vicinity

personnel and local law enforcement officers. The purpose of such observation posts is merely to detect the presence of potential dangers to flight operations and report such threats to appropriate local authorities so that they can respond.

J. WATERSIDE SECURITY

1. Securing DoD facilities located astride waterways is also an especially challenging task. [redacted]

2. [redacted]

3. [redacted] The security perimeter must be extended into the water if terrorists are assessed as having the capability to launch attacks using stand-off weapons from boats or other craft.

5. External surveillance must monitor traffic on the surface of the water adjacent to the facility, extending from the barrier to range exceeding the range of identified terrorist threats. [redacted] In some port areas, the security zone will be constrained; in other areas the security zone may be extended further, especially if the terrorist threat includes longer-range standoff weapons such as man-portable antitank missiles. Within the security zone exists a reaction zone. It is within this zone that aggressive actions may be undertaken to isolate, delay, and resolve potential threats to DoD assets from waterside terrorist action.

[redacted] However, the principle can be extended to one or more warships at anchor; security zones may also be declared around navigation aids mounted on structures in shallow water, as is the case for airfield navigation aids in bays or rivers.

[redacted]

of the emergency evacuation site. Such structures should be well camouflaged and knowledge of their existence kept on a strict "need-to-know" basis.

4. Erecting or constructing special safehavens near emergency evacuation sites should be considered when circumstances are such that helicopter evacuation might require several hours to execute after requested. Plans should be prepared that would permit dispersal of DoD personnel to several safehavens including those adjacent to emergency evacuation sites before local travel became too dangerous. Relocation of DoD personnel to remote safehavens to await evacuation may be an effective alternative in some circumstances, especially those in which the number of DoD personnel and dependents is small.

L. DoD INSTALLATION SECURITY SUMMARY

1. In this chapter, the components of a physical security system outlined in Chapter 8 have been assembled to form the outer layer of security at the level of a DoD installation. General physical security considerations and functional physical security objectives have been discussed. Incorporation of good industrial safety and hygiene practices has been emphasized. Security planners and facilities planners must coordinate their efforts to ensure that all activities involving the handling of hazardous materials, POL, ammunition and explosives, and toxic waste are well separated from other installation activities and each other.

2. The chapter has also examined the use of perimeter barriers and methods to ensure their continued integrity. Application of surveillance systems to provide early warning of attempted intrusion detection has been discussed. This chapter has also emphasized the importance of continuous physical security system maintenance and training activities. The importance of the guard and security forces to the effective operation of the entire physical security system has been addressed. The chapter also addressed three areas of special security considerations: airfields, ports, and evacuation sites.

3. As in foregoing discussions, the design and implementation of a physical security system for an installation must look outward at the threat and inward at the types of assets, the risks of attacks against those assets, the importance of those assets to successful DoD mission accomplishment, and the criticality of those assets to the Department of Defense. Protection systems combining components of physical security systems outlined here should be constructed in relationship to requirements. The existence of physical security system components does not mandate their use in each and every case; the wide range of physical security components allows security planners to mix and match them to achieve an optimum level of security within the available financial, materiel, and human resources.

[redacted]

CHAPTER 10

PHYSICAL SECURITY FOR A FACILITY

A. INTRODUCTION

1. In Chapter 8, components of a physical security system for each DoD installation or facility were discussed. In Chapter 9, these components were integrated into an installation-level physical security system. The installation-level physical security system provides a basic level of physical protection for all DoD-affiliated personnel, individual facilities or activities, and materiel on the installation.

2. In this chapter, the application of the physical security system concept will be extended to individual DoD facilities. For purposes of this discussion, a DoD facility can be one or more of the following:

a. An entire building.

b. One or more floors of a building.

c. One or more contiguous suites within a building.

d. A residence belonging to a DoD High-Risk Person or provided to a person occupying a DoD High-Risk Billet.

3. The balance of this chapter considers physical security system application to DoD facilities other than residences. Chapter 11 will consider residential security as a special case of facility protection.

4. The basic concepts of the physical security system remain valid. The security functions of threat detection, threat classification and identification, threat annunciation, threat delay, and threat response must be performed. The principal differences between the performance of these security functions between an installation and a facility is the distance and speed with which they are performed. An installation perimeter is usually well removed from assets to be protected. A facility perimeter may be only a matter of inches away from the assets to be protected. Under these circumstances, the security system functions must be performed precisely, accurately, and very quickly.

5. [redacted] Careful management of scarce resources is necessary. Physical security can be a force multiplier. If forces are not protected when not actually in use, they, and the nominal reserve, replacement, or reconstituted forces that are supposed to be

available may never materialize. As a result, the Department of Defense might be unable to perform. Force protection takes on new importance from this perspective, but not at the expense of protecting assets of greater importance faced by larger, more menacing threats.

B. BUILDING PERIMETER BARRIER SELECTION AND HARDENING

1. Building Perimeters

a. Perimeters surrounding buildings located off Government property vary from those with industrial-type perimeter fences to those composed of little more than aesthetically attractive landscaping.

b. Exterior IDS sensors are not recommended for the Perimeter Protection System of most office buildings unless either personnel and vehicle access is to be controlled at the perimeter entrance gate, or the building is required to be secured during non-duty hours to protect sensitive assets. Where access control is to be administered at the entrance gate, exterior sensors should be activated around the remainder of the perimeter during working hours.

[redacted]

CCTV should be provided to allow security personnel to evaluate alarms around the perimeter of the residence. Even residences without Perimeter Barrier System IDS sensors should be provided with CCTV that will provide coverage of all of the residence's doors, windows, and other openings that could allow penetration of the Building Protection System. These cameras should be slaved to the sensor system to immediately position themselves to view the area protected by the violated sensor and force this view to the security guard's monitor for rapid evaluation. With today's solid-state CCTV technology, cameras are considerably smaller than the older tube-type cameras and thus can be mounted in a myriad of covert locations.

2. Exterior Doors

a. LIMIT NUMBER OF DOORS TO BARE MINIMUM NECESSARY FOR EMERGENCY EVACUATION; PERMIT NORMAL ENTRY AND EXIT THROUGH ONLY ONE DOOR.

Because of their functional requirements, construction, and methods of attachment, doors are less attack-resistant than adjacent walls and frequently provide a "soft spot" in an otherwise attack-resistant structure. For this reason, the number of doors to a facility or residence should be reduced to an absolute minimum and, in cases where more than one door exists, only one should be provided with outside mounted locks and entry hardware. All others should, where practicable, present blank, flush surfaces to the outside to reduce their vulnerability to attack.

b. STRENGTHEN AND HARDEN DOOR JAMB.

The strength of the door jamb must be considered when planning the secure door system. Hardening of the upright surfaces into which the door is fitted will resist jamb attack.

c. USE HIGH SECURITY LOCKING SYSTEMS ON ALL DOORS.

(1) The weakest part of a door system is the latching component of the lock or locking device. Typical delay times for defeat of locking devices range from 9 seconds to 3 minutes. Because of this, priority must be given to protection of the locking system when selecting components for a door system.

(2) Locking systems can be divided into two basic groups: surface-mounted or mortise systems. Externally mounted locks and hasps are used for securing utilities openings, etc. These should be replaced with internally locking devices. Internal locking systems are always preferred for applications where high security is desired.

[redacted]

d. LOCATE HINGES TO REDUCE THEIR VULNERABILITY TO ATTACK; HARDEN HINGES IF EXPOSED.

Hinges should be on the inside of the door where possible. If exposed, hinges become vulnerable to attack by removal of the hinge pin or by cutting or sawing the hinge barrel from the hinge. A number of measures involving positive interlocking hardware for coupling the hinge sides to the door and the door frame are available to increase their penetration resistance.

3. Windows

a. Windows of various sizes and configurations are required in the walls of most structures for the passage of light, ventilation, and observation. Windows are always a significant weak point in the Building Protection System because of their low penetration resistance. Standard construction window assemblies provide penetration resistance of less than 10 seconds.

b. Several steps can be taken to harden windows in offices and residences. Among these are the following:

(1) STRENGTHEN WINDOW FRAMES AND SASHES.

For maximum penetration resistance, window frames should be constructed of steel and securely fastened or cement grouted to the surrounding structure to prevent easy removal, separation, or penetration at the point where the window frame and building meet. [redacted] This not only slows an intruder, but prevents the glazing from being blown from the sash in the event of a bomb blast.

(2) INSTALL HEAVY DUTY WINDOW LOCKS ON ANY WINDOWS WHICH CAN BE OPENED.

(a) Wherever possible, windows should be stationary (non-opening). Common latching devices found on both residential and commercial window systems are

susceptible to manipulation from the outside. Several techniques can be used to enhance the security of movable windows.

[redacted]

(c) Sliding glass doors and windows should be constructed with the movable section on the inside of the fixed section. As a minimum, sliding glass doors should be glazed with laminated safety glass and equipped with a key lock having a sturdy hook-type bolt that binds the door and frame together when secured. [redacted]

(d) French doors and any double doors opening out should be equipped with protective hinges and a mortise-type lock that is key operated from both sides. The inactive half of the double door should be equipped with flush throw bolts [redacted]

(3) CONSIDER SUBSTITUTING BURGLARY-AND BALLISTIC-RESISTANT GLAZING, ACRYLIC GLAZING, OR POLYCARBONATE GLAZING FOR CONVENTIONAL GLASS OR SAFETY GLASS GLAZING MATERIALS.

(a) Burglary- and ballistic-resistant glass is similar to laminated safety glass but has a thicker inner laye[redacted] between two panes of glass. [redacted] Use of ballistic-resistant glass increases the safety of building occupants because this material has multiple layers of polyvinyl butyl and [redacted]

(b) Acrylic glazing is lightweight, heat treated or "tempered" plastic. It is 17 times more impact resistant than a comparable thickness piece of conventional glass. [redacted] It is recommended that glass-clad polycarbonate materials be used for [redacted] where maximum resistance to penetration and attack are desired. These compound glazing materials withstand environmental effects of ultraviolet light, cleaners, and normal wear and tear better than simply polycarbonate glazing alone. [redacted]

(c) The following observations are important if selecting use of polycarbonate materials for window glazings:

[redacted]

2 [redacted]

3 [redacted] Tests [redacted]ve proven this to be an effective countermeasure to spall.

4 [redacted]

(4) INSTALL SHATTER RESISTANT SECURITY WINDOWS.

[redacted] An alternative approach is to install a safety film on the inside of windows. [redacted] can substantially increase penetration time for cutting or smashing attacks, and will reduce spalling and flying glass injuries resulting from explosive attacks.

(5) INSTALL HIGH SECURITY GRILLS, SCREENS, OR MESHWORK OVER WINDOWS AND SKYLIGHTS.

(a) All skylights should be screened to prevent access to buildings via these routes. Other windows that might be used to gain access to a structure including all windows on the ground floor and other windows accessible from nearby buildings, walls, parked vehicles, trees, or utility poles should be screened or grated in some manner. Windows of a size sufficient to permit entry or removal of arms should be either screened or barred.

(b) [redacted]

(c) [redacted]

(d) Care should be given to the manner in which grillwork, screens, or bars are affixed to a structure. Attackers often attack the screens, bars, or grillwork by prying the treatments away from the window rather than by trying to saw, cut, or burn their way through them. All bolts used to connect grillwork, screens or bars to the structure or

to other parts of the window treatment should be welded so that they cannot be manipulated by an intruder to gain access.

(e) When grillwork is installed in buildings or residences where windows are designed as emergency escapes, be sure to hinge the grillwork and equip it with a proper release. Ensure the emergency release does not become a weakpoint in the window security system.

4. Utility Access

a. A careful inspection of the structure exterior must be made to locate any utility openings. In conventional building designs, utility openings, manholes, tunnels, air conditioning ducts, filters, or equipment access panels can provide a vulnerable entrance route with no significant delay. If such openings cannot be eliminated, their delay times must be increased.

b. [redacted] Such penetration resistance can be achieved in several ways.

(1) INSTALL SECURITY SCREENS OR GRATES OVER UTILITY ACCESS OPENINGS.

The techniques described above to secure a window or skylight using bars, grates, or mesh can be used to restrict access to a structure via utility penetrations. [redacted]

(2) ATTACH IDS SENSORS TO UTILITY OPENINGS.

All utility openings greater than 10 inches in diameter should be equipped with IDS sensors incorporated into the facility's IDS system.

5. Duress Alarms

a. Duress alarms are devices that can be activated manually in the event of an unauthorized penetration attempt. An audible alarm can be sounded locally in an attempt to frighten off the intruder. Alternatively, a silent alarm can also be sent to the organization's security center, or other location where the alarm would summon immediate assistance.

b. Duress alarms can be placed in inconspicuous locations, and can even be disguised as common office objects or home decorator items. Duress alarms can also be incorporated into home or office furnishings.

6. Communication Systems

Telephones are needed at all times and secure means of communication are essential between a secured area and its dedicated response force. Telephones in many parts of the world are unavailable, unreliable, and, as in many CONUS locations, exposed and vulnerable to terrorist attack. The security planner often has little knowledge and no control over where or how the telephone lines are routed or if they are even minimally secured. Telephone systems required for security and safety of executive personnel must

be over secure dedicated lines. Where this is not possible, a secure radio communication link must be established. Portable, hand-held radios can assure backup communication when other communication links are severed.

C. INTERIOR BARRIERS

Barriers may be used within the interior of facilities to accomplish the same functions as are performed by barriers to access to installations. They establish boundaries or lines of demarcation of different activities (and differing levels of security) within a facility. They deter and intimidate individuals from attempting unauthorized entry. As in the case of installation-level barriers, they are platforms on which intrusion detection sensors or surveillance systems can be mounted. Barriers may be used within a facility to channel pedestrian and service vehicle traffic. Barriers are used within individual buildings on DoD installations for similar purposes. In addition, use of high security doors, window glazings, and walls can provide building occupants with protection against ballistic penetrations--small arms fire, bomb fragments, broken glass, etc.

1. General Constraints on Facility Barrier Selection

a. A wide range of materials and construction techniques can be used within a facility to erect a barrier. The selection of materials and construction technique is constrained by the strength and load-bearing capacity of the facility itself. The specific construction site conditions may also constrain or limit barrier construction within a facility. The requirement to access utility lines, fire protection systems, or specific emergency entry/exit routes may dictate use of movable barriers as opposed to fixed, anchored barriers. Perceived terrorist threat capabilities, construction costs, local building codes, and limitations on tenant construction for leased facilities also constrain or limit the selection of materials and types of barrier construction undertaken. The following discussion identifies a selection of materials and techniques that may be appropriate for enhancing the security and protection of DoD assets.

b. Further information is available from Service security engineering branch within each Service's civil engineering organization. [redacted]

2. Barrier Materials

a. An infinite range of materials and construction techniques is available to help security planners meet specific needs. Materials and techniques used to enhance the building exterior's resistance to penetration can also be applied within a building. [redacted]

b. Use of multiple barrier materials and construction techniques can sometimes accomplish one barrier purpose with less expensive and less disruptive construction techniques. For example, use of ballistic-resistant, glass-clad polycarbonate panels accompanied by overt surveillance cameras, warning signs, annunciator devices (flashing lights, buzzers, etc.) can create an intimidating picture of a high security barrier adjacent to

a high security passageway at equal or less cost than the construction of a reinforced masonry wall to accomplish the same purpose.

Table 10-1. Selected Facility Barrier Materials

DELETED

of protection and security resources, access control points as illustrated can be established in series. The greater the value of the protected asset, the larger the number of checkpoints that must be passed before access is granted.

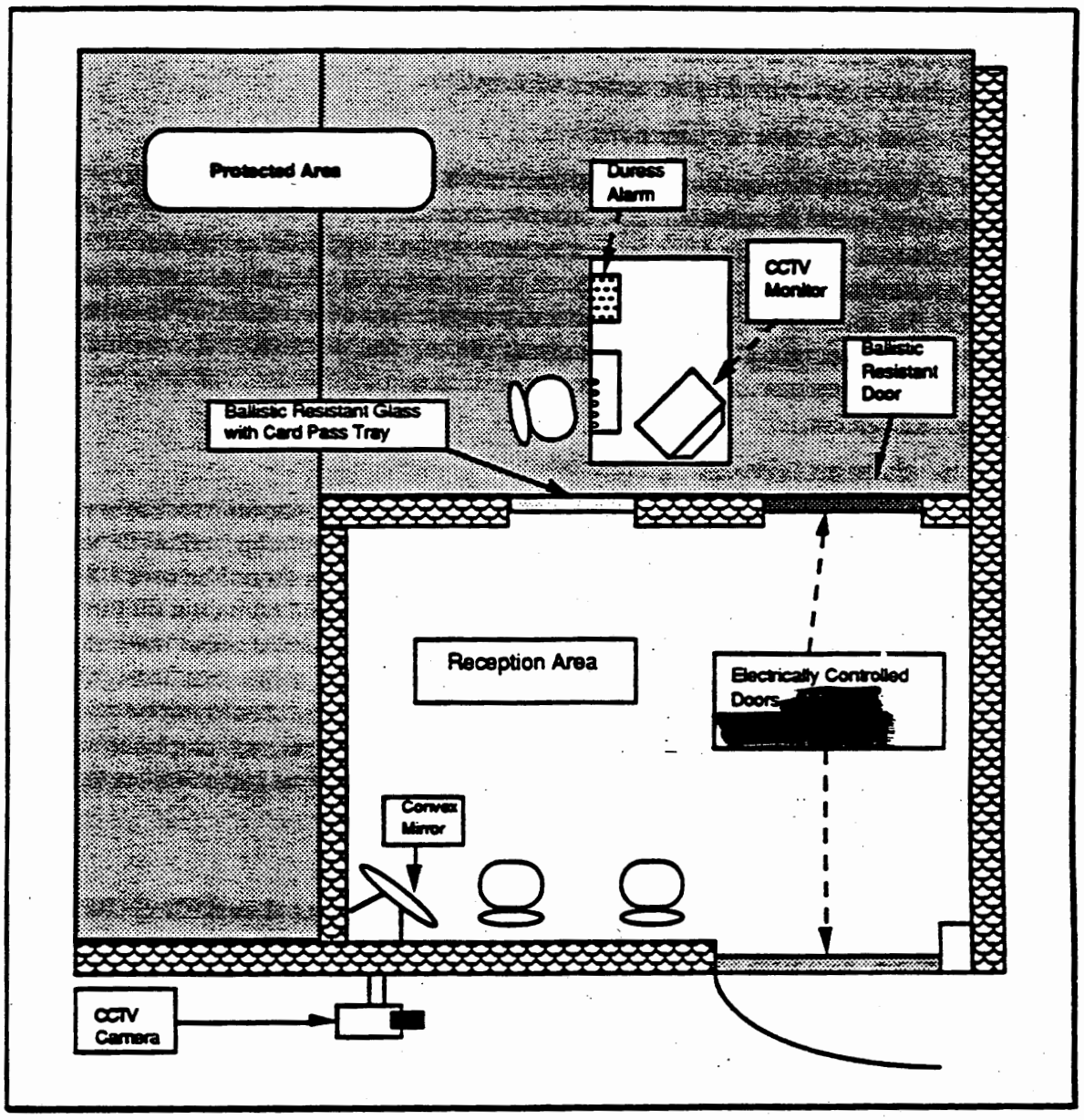


Figure 10-1. Reception Area to Access Controlled Facility

c. This figure illustrates several important features of a secure area access control point. [redacted] The door to the entryway is hardened [redacted] The waiting area is hardened, and is subject to surveillance by a guard. The guard is protected from the waiting area by ballistic resistant glass and an electrically controlled ballistic resistant door. The guard also has a hidden duress alarm.

d. The access control checkpoint can screen employees and visitors. [redacted]

2. Access Control Procedures

The systems approach to physical security includes an assessment of day-to-day operations within the secured area. In order to maintain adequate security throughout a DoD installation, within a facility, within an activity, and within an organization without unduly interfering with day-to-day work, it is necessary to permit personnel to move about. On the other hand, the physical security system has a responsibility to ensure that protected assets remain protected throughout the regular workday. Accordingly, the following measures can be implemented to maintain positive control over access to protected DoD assets.

a. Pass and Badge System

Where the area is large or where the number of personnel exceeds a number that can be recognized personally by the guard or persons charged with security responsibility of the area, a pass and badge identification system should be used. Security badges will be used primarily for access control. Badges should contain a picture of the individual authorized access, and may contain additional information about the individual. Such information should be communicated through badge borders, badge color, identification photograph background color, etc. Information that should not be printed on the badge includes home address, specific work location address and telephone number, security information, and in some areas, information identifying the badge holder as a DoD or U.S. Government employee.

b. Access List System

Admission of personnel to very high security areas (Level Three Restricted Access Areas, formerly termed exclusion areas) should be granted only to those persons who are positively identified. One approach is to prepare access lists containing the names of those individuals specifically authorized access to a facility. Access lists should be maintained under stringent control of an individual who is formally designated by the commanding officer or manager of the facility. That person should be responsible for updating and confirming the need for access on a regular, frequent basis. Admission of persons other than those on the authorized access list should be approved by the commanding officer, manager, or designated representative. Access lists should always be controlled carefully and never displayed to public view. If a computerized access list system is used, the computer files used to generate such a list must be safeguarded against tampering.

c. Exchange Pass System

The exchange pass system is an identification system that may be employed in highly sensitive areas to ensure stringent access control. It involves exchanging one or

more identification media (badges, passes, etc.) for another separate type of identifier (badges, passes, etc.). This system is particularly useful where visitors must gain access to a high security facility. The process of exchanging passes is an intimate one, permitting security personnel an opportunity to examine all personnel both upon entering and upon existing the secured facility.

d. Escort System

Escorting is a method to control visitor personnel within secured facility. The escort must remain with the visitor at all times while within the restricted areas. If local written policy determines that an individual does not require an escort within the area, the individual must meet all the entry requirements for unescorted access. Escort personnel may be civilian or military employed by or attached to the visited activity, and will normally be from the office of the person being visited. A major objective in escorting visitors around a facility is to ensure that all material brought into the facility by the visitor is left with someone who can open and examine the contents, and that visitors leave no packages or other materials behind upon their departure.

E. SAFEHAVENS

1. The innermost layer of protection within a physical security system is the safehaven. Safehavens are not intended to withstand a disciplined, paramilitary attack featuring explosives and heavy weapons. [redacted] The safehaven should be designed such that it requires more time to penetrate by attackers than it takes for the response force to reach the protected area. [redacted]

2. [redacted]

3. [redacted]

4. [redacted] When engaged, bolts secure the door to the jamb in all four directions--up, down, left, and right. Electrically operated deadbolts are acceptable provided that in the event of power failure, the bolts slide into their locked condition *and* a backup power source with automatic switchover is available. [redacted]

5. Safehavens should have only one door and no windows. [redacted]

6. [redacted]

7. Consider installing a main power switch in the safehaven that would allow occupants in an emergency to interrupt power to the entire office building or residence with the exception of emergency services circuits (emergency lighting, emergency communications, emergency computer power supplies, etc.) Interruption of electrical service in the building can interfere with the use of power tools to gain access to individuals taking refuge in the safehaven. Furthermore, darkness can make it more difficult for the intruders to press their attack.

8. Safehavens can be installed in office buildings and private residences. [redacted]

10. Safehavens can remain functional areas of an office building. Eliminating use of the space is not necessary. It is necessary, however, to regulate use of the space so that those individuals whose protection is essential can be inserted into the safehaven in a timely manner in the event of warning of a terrorist attack.

11. The following listed equipment should be provided inside the safehaven. [redacted]

c. [redacted]

d. [redacted]

DELETED

Figure 10-2. Safehaven Concept Implemented in a High-Rise Office Building

[redacted]

12. Even though a safehaven is not intended or designed to provide penetration protection over an extended period of time, it may be necessary for occupants to remain in the safehaven for several hours while response forces converge on the site, contain and resolve the terrorist incident, and verify that no threats to the safehaven occupants remain in the area. Under such circumstances, occupants of the safehaven may be more secure and

less likely to be injured or to compromise crisis management by remaining in the safehaven until the on-scene commander directs them to evacuate or leave the facility.

F. FACILITY PHYSICAL SECURITY SYSTEM SUMMARY

1. DoD facilities draw their basic security infrastructure from the installation physical security system. Threats to a particular facility on an installation will usually originate outside the installation. Detection and warning will come in most instances as a result of an attempt to penetrate the installation.

2. Facility security enhancements are intended to augment the basic physical security posture of an installation. These enhancements take into account real limitations on security resources. [redacted] Assets must be protected because of their criticality to specified missions, their criticality to the support of specified forces, or in some instances, because of the grave harm and danger to personnel, facilities, and materiel as a consequence of improper use or misuse of the asset.

3. The basic tenets of good security planning at the installation level extend to individual facilities. To wit:

a. Utilities providing power, communications, and cooling to security systems should be isolated from other utility service to the facility; utility connections should be protected and alarmed;

b. Good industrial safety and hygiene practices should be followed without exception; toxic, hazardous, and explosive materials should be isolated from all other facilities as [redacted]

c. Safety equipment including fire extinguishers, first aid kits, emergency communications, and emergency lighting equipment should be installed and kept in properly working condition at all times.

d. Facility vulnerability assessments and protective measures implemented in response thereto should consider terrorist threat from all dimensions where terrorist group history and capability demonstrate such threat or installation and facility vulnerability assessment reveal security weaknesses in basement level and/or roof level perimeter barriers, ballistic penetration barriers, or structural weakpoints.

4. The concepts of a physical security system can be expanded to include facilities that are not located on DoD installations but house DoD assets that must be protected. Such assets might include distributed DoD offices, or the residences of military officers or DoD civilians serving in High Risk Billets or who have been designated High-Risk Persons. Chapter 11 illustrates how the concepts outlined and described in Chapters 8, 9, and 10 can be applied to these circumstances.

CHAPTER 11

RESIDENTIAL PHYSICAL SECURITY CONSIDERATIONS

A. INTRODUCTION

1. The DoD Physical Security Regulation (reference (cc)) mandates the protection of all DoD assets to the degree necessary to preserve mission capability. DoD personnel are valuable assets, just as are weapon systems, facilities, and bases. Many of the concepts and specific techniques used to make DoD installations and facilities more secure can be applied to residences as well.

2. This chapter highlights security matters to be considered when selecting a residence. It describes techniques used to enhance the basic level of physical security provided by personal residences.

3. Many senior military officers and DoD officials (referred to below as "executives") are assigned to overseas posts. Because of their specific assignments or positions of visibility and terrorist threat conditions, they are designated High-Risk Persons.[1] [redacted] This chapter presents security measures appropriate for use in private residences.

4. Residential security should be examined just like the security of a DoD installation. A layered defense or defense in depth should be prepared. This chapter outlines specific steps that can be taken by all DoD-affiliated personnel. The chapter concludes a discussion of supplemental security measures for High-Risk Persons.

B. SELECTION OF RESIDENCES

1. General Considerations

a. There are a number of factors that are often considered when a family residence is being selected. Among these factors are the following:

(1) Employment locations for DoD personnel and any working dependents accompanying them.

(2) Recreational facilities.

(3) Schools for dependents.

(4) Shopping.

---

1 See Chapter 13 below for further discussion of these designations.

(5) Inter-urban, regional, and international transportation facilities.

(6) Religious institutions.

(7) Medical facilities.

b. It is strongly suggested that some security considerations be added to this list of residential site selection factors including the following:

2. General Security Atmosphere Indicators

a. A number of observable characteristics can provide clues about the general security atmosphere.

(1) When selecting a neighborhood in which to consider residing, OBSERVE THE GENERAL SECURITY ATMOSPHERE as indicated by the following typical indicators:

(2) The general character of streets, sidewalks, lighting, pedestrian and vehicular traffic patterns;

(3) The presence and condition of parks, playgrounds, recreation areas;

(4) The existence of public or commercial enterprises intermingled with residential dwellings; and

(5) The existence and condition of fire hydrants and police call boxes.

b. Where the streets are paved, well lit, broad enough for at least two cars to pass one another, and lined with sidewalks filled with a variety of people, there is a strong possibility that the neighborhood is fairly secure. Where these favorable impressions can be reinforced by a walk through clean, well utilized parks, playgrounds, an recreational areas, a walk through clean, attractive mixed use neighborhoods, and a walk through areas with visible presence of police and fire services, the initial impression is likely to hold up to further scrutiny.

c. In general, the overall appearance of the area may often serve as an indicator of crime levels. Where property lines are well defined, homes appear well maintained, and the landscaping shows an obvious pride in the property, crime rates are likely to be low. While that may not eliminate the threat of terrorist attack, it does suggest an attractive general security atmosphere.

3. Specific Indicators of General Security Levels

a. Several observable security measures taken by residents of a neighborhood can provide specific indications about local security conditions:

(1) Look for specific indicators of security precautions taken by local residents.

(2) Presence of barred windows, security grills on doors;

(3) Security walls and fences;

(4) Security lighting;

(5) Large dogs or other watch animals; and

(6) Presence of private security guards, especially during the day.

b. Observe or make inquiries about the frequency and type of police patrols in a given neighborhood. Find out what type of police or which police jurisdiction responds to calls for assistance. Observe the general appearance of police security personnel on the street. Police who take pride in their appearance, the appearance of their vehicles, and who make themselves visible to the public in the performance of their duties can usually be relied upon to provide dependable police coverage throughout the community.

c. Try to determine the attitude of the government and the populace toward other nationals, and particularly Americans. A strong anti-American attitude could be cause for you to have diminished faith in local police responsiveness.

4. Background Information on Local Criminal Activity

a. Investigate local crime activity in the area to which you are considering moving.

(1) The level of criminal or terrorist activity throughout a community is rarely uniform. Street crime can be expected to occur in lower income, crowded, and congested areas. It is generally recommended that residences not be selected in downtown, commercial, or especially isolated areas, especially when local data indicate that such areas are high crime areas.

[redacted]

(3) [redacted] Upon request, the Country Desk will try to provide appropriate information generally available to all persons who ask for such information.

5. Utilities Service and Protection

EXPLORE THE RELIABILITY OF LOCAL UTILITY SERVICE in order to determine whether or not emergency or backup power and utility service will be required. The availability and reliability of utilities in any given location should be a primary factor in the selection of a residential site. Reliability of utilities should be determined and in cases were they are erratic, acquisition and use of backup systems should be assumed. Disruption of utilities service (particularly electricity and telephone) would facilitate unauthorized access to a residence by an intruder.

6. Fire Protection

CONSIDER THE AVAILABILITY AND EFFECTIVENESS OF LOCAL FIRE PROTECTION services in each neighborhood being investigated for potential residence. The proximity of prospective residences to and the effectiveness of the fire protection services is a major consideration in residential site selection. The availability of water or other substances to

fight a fire should be determined. The locations of fire hydrants or other water sources and means by which they can be accessed and brought to the residence by its occupants before the arrival of the local fire brigade should be considered.

7. Physical Environment Considerations

a. Investigate potential hazards in the physical environment in and around neighborhoods of potential residential interest.

(1) Residential areas under consideration should be well removed from known environmental hazards such as flood plains, active geological faults, steep slopes of hills subject to mud slides and/or brushfires. Residential areas close to breeding areas for disease vectors such as insects or rodents should also avoided if possible.

(2) Sometimes, housing availability restricts residential selection to areas at risk from at least some of the environmental hazards noted above. If placed in this situation, take the following measures, plan additional, necessary precautions to prevent loss or injury from environmental disasters in addition to potential terrorist actions.

b. Be sure to include access to and storage of emergency rations, lighting, power, and communications, as well as backup or alternatives to any other systems that could be disrupted as a result of an environmental disaster as part of your moving plans.

8. Residence Access Routes

a. Select candidate residences with access routes that allow many choices of approach or departure.

(1) It is essential that access routes to and from residences allow occupants many choices of approach or departure to make detection of arrival and departure patterns difficult and to avoid ambush or attack once it is spotted. Some considerations should include:

(a) Clear delineation of the street or roadway.

(b) Sufficient street width to allow two cars to pass, even if vehicles are parked on both sides of the roadway.

(c) Sufficient neighborhood lighting at night.

(d) Unobstructed view of the road from the residence.

[redacted]

9. Parking

a. Consider the location and availability of parking for privately owned vehicles, motorcycles, and bicycles when examining candidate residences and their surrounding neighborhoods.

(1) In selecting a residence, consideration must be given to securing personal property including means of transportation. Bicycles, motorcycles, mopeds, and other two-wheeled vehicles are usually relatively east to secure. Often they will fit in a storage shed, or can be locked close to the residence where they can be observed.

(2) The family automobile, and in some cases, official vehicles that have been approved for transportation between home and office, present another problem. The best solution is to store the vehicle in a garage that can be kept locked at all times. Carports and driveways within a fenced or guarded area are the next best alternative. Off-street parking alternatives represent still another although far less desirable alternative. Personal or official vehicles should not be parked on the street overnight in the vicinity of personal residences.

C. SECURITY COMPARISONS BETWEEN SINGLE AND MULTIPLE FAMILY RESIDENCES

1. General Recommendation

a. After a careful review of the general security atmosphere and specific indicators of local crime, there may be an opportunity to choose either a single family or a multiple family residence. Overall housing costs, availability of dependent care or playmates for dependents, and location convenience factors noted above can be important determinants of residential choice. There are some specific security considerations, however, that should also be evaluated in choosing between multiple or single family residences:

b. In most cases, APARTMENTS ARE GENERALLY PREFERRED TO SINGLE FAMILY DWELLINGS WHEN SECURITY IS A PRIMARY CONSIDERATION. Apartments above the first floor are more difficult to get to, usually have only one entrance, and provide some degree of anonymity for the resident. Thus, they present a more difficult target for the terrorist or burglar, and are often less expensive to modify with security hardware. Living in an apartment provides benefit of close neighbors. In the event of an emergency and loss of communications, neighbors can often be relied upon to provide assistance. At the very least, they can call the police if American occupants of apartments cannot.

[redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

d. [redacted] Common in many overseas areas, a number of separate homes are clustered in the same general area. These are often occupied by American or other foreign families. Such arrangements offer excellent opportunities for cooperative security arrangements. These enclaves may or may not be fenced, and the families may share the costs for guards, lighting systems, and alarm systems described in the preceding chapter on physical security arrangements.

e. A separate residence in a suburban neighborhood can be adequately secured, [redacted]

2. Apartment Selection Suggestions

a. The following features of apartment living are recommended as part of a good security foundation for a private residence:

(1) Find an apartment which:

(a) Features lobby and parking area security provided by guards, closed circuit television, or locking devices which can only be operated by the tenants;

(b) Does not have fire escapes, balconies, or overhangs that could be used to gain surreptitious entry to the building;

(c) Has only one door for general entry and exit and one door for services and deliveries, both of which have controlled access via guards, keys, or key-card devices ;

(d) Has well-lit hallways and stairwells, preferably monitored by closed circuit television, which cannot conceal intruders.

b. [redacted]

c. If adequate security measures are not present, apartment living affords the opportunity to provide necessary security at a reasonable price, as a shared expense.

3. Single Family Home Selection Suggestions

a. Although a well-designed and well-managed apartment is more secure than a separate house there are often other reasons that result in the selection of a single family residence by DoD-affiliated personnel. Need for three or four bedrooms to accommodate children or other dependents, an exercise area for pets, or large areas for official entertaining are examples of considerations that may eliminate an apartment as a residential choice.

b. The main ingredient to be used in selecting a single dwelling residence is finding an established residential development or neighborhood where income levels and lifestyles are compatible. Neighbors routinely looking out for each other are a critical factor in a well protected residential area. A good overview of the entire neighborhood such as streets, sidewalks, lighting, and adjacent homes is necessary. Each of these features affect the security of the neighborhood and therefore, the natural protection afforded the residence.

c. In selecting a single family residence, seek out residences with the following characteristics:

(1) Find a single family residence that:

(a) Has architectural and natural features which provide opportunities for occupants to observe activities on the street, the sidewalks, adjacent yards, and public areas;

(b) Is placed in the neighborhood such that a stronger or potential intruder will be readily observed by neighbors; and

(c) Is situated within clearly defined boundaries, making an inadvertent intrusion virtually impossible.

4. Apartment Security Enhancements

a. The apartment should possess a good solid door and the door frame should be well-constructed. Most residential security hardware that is suitable for single family dwellings is also suitable for apartments. Most essential of these is a 190-degree optical viewer and a strong secondary deadbolt lock. In the absence of a fire escape, there are a variety of devices sold commercially that will facilitate exiting an apartment from a window. The devices include rope or chain ladders, and mechanical rope slings that provide a controlled descent to the ground.

b. Additional security measures employed in single family residences described below can be added to apartments as well if necessary.

5. Single Family Residence Security Enhancements

a. Most of the common enhancements to single family residence security focus on improving resistance to intrusion and penetration. Following the general approach presented above with respect to enhancing the security of an installation or a facility, consider the following measures:

(1) Ensure the single family residence is surrounded by a barrier clearly delineating the property from adjacent homes.

An aesthetically acceptable barrier such as a picket fence can provide a good psychological deterrent to intrusion. Other fencing materials such as split rail, board-on-board, decorative wire mesh, decorative walls constructed of masonry or stone can serve the same purpose.

[redacted] The mechanisms used to secure such penetrations should be comparable in their resistance to penetration as the perimeter barrier itself. It makes no sense to build a high security fence and use a 50 cent low-security hinge on a pedestrian gate. Installing a high security cypher lock on a common exterior door through a decorative wall will add no more security than the security value of the door itself.

(3) INCREASE THE RESISTANCE OF DOORS, WINDOWS AND EXTERIOR WALLS TO PENETRATION.

Doors can be strengthened and made more resistant to penetration using techniques [redacted] Windows can also be made more resistant to penetration [redacted] Depending on the nature of the terrorist threat exterior walls can be made more resistant to penetration. [redacted]

6. Common Security Enhancements for Residences

a. Whether selecting an apartment, a single or multifamily dwelling in a secured compound, or a single family dwelling, the following considerations should be addressed:

(1) DO NOT LEAVE UTILITY CONNECTIONS INCLUDING TELEPHONE TERMINAL BOXES, ELECTRICAL SERVICE WIRING, POTABLE WATER CONNECTIONS, NATURAL GAS CONNECTIONS, ETC., ACCESSIBLE FROM THE EXTERIOR OF THE HOUSE.

Consider relocating utility service or placing the utility connections inside secured enclosures to prevent tampering or unauthorized access. Add internal backup systems such as batteries, bottled gas, and two-way radios. Consider finding an alternative residence as well.

(2) Select a residential structure that is not vulnerable to fire.

Residences should be constructed from materials that are not readily combustible. Furthermore, electrical wiring and fixtures as well as natural gas and/or propane ovens, ranges, water heaters, and other appliances should be in good condition. Be sure that the residence has sufficient number, location, and accessibility of potential emergency exits which can be used in the event of a fire. If necessary, acquire hinged high security window grills to permit use of windows as a fire escape. Be sure to keep fire extinguishers charged and available; install a smoke detector in the residence if it does not already have one.

D. SUPPLEMENTAL RESIDENTIAL SECURITY MEASURES FOR HIGH-RISK BILLETS AND HIGH-RISK PERSONNEL

1. Overview

a. [redacted] The balance of [redacted] chapter will address specific security measures that may be provided in the residence of a HRP or a person assigned to an HRB.

b. Before supplemental security measures are provided, an integrated terrorist threat estimate must be prepared. This document examines the terrorist threat as analyzed by the intelligence community. The document will also include an assessment risk of a terrorist attack by the Service, CINC, Service component commander, the local command, and for DoD personnel assigned to the American Embassy, the State Department's Regional Security Officer. The document should include an assessment of the vulnerability of DoD missions as supported by the local activity in the event of a terrorist attack. An assessment of the criticality of the HRP or HRB should also be prepared. The vulnerability and criticality assessments dealing with DoD personnel assigned to the CINC or a component command should be coordinated with chain of command through the CINC to ensure that assessments of vulnerability and criticality through all echelons of command are fully informed if not in full agreement.

c. If supplemental security measures are warranted by the integrated terrorist threat assessment, several steps should be taken at government expense. Many of these measures may also be taken by personnel at their own expense should they feel a need for additional security in their residence.

2. Enhanced Protective Measures for High-Risk Personnel Residences

a. Install high security perimeter barriers equipped with high security locks and intrusion detection devices.

(1) As noted above, a single family residence should be surrounded by a perimeter barrier to define the boundaries of the property. Residences housing HRPs may require high security perimeter barriers such as reinforced masonry walls, high security steel fences, etc.

(2) All barriers in the perimeter should be gated. The gates should be operated either by a key-type device (either a physical key or a cipher lock) or by a remote control lock by someone in the residence. The gate and its supporting hardware should be able to withstand the same type of attack that might be mounted against the residence perimeter. If the residence is surrounded by a metal picket fence designed to withstand vehicular assault, then so too should gates be capable of withstanding vehicular assault.

b. All residential doors should be hardened to withstand penetration.

(1) Depending on the type of door construction used, several approaches can be implemented. Consider methods outlined in Figure 11-1

DELETED

Figure 11-1. Door Hardening Techniques

(2) Door frames, door jambs, door hinges, and door locks should be examined and hardened as outlined above and in Appendix E.

(3) In addition, consider building a screened vestibule in front of each door. Such vestibules should be equipped with doors, security hardware, and intrusion detection sensors to provide early warning of an attempted intrusion and to increase delay of an attack.

(4) [redacted]

2 The National Association of Architectural Metal Manufacturers is located at 600 S. Federal Street Suite 400, Chicago, IL 60605-1895. It may be reached by commercial telephone at 3120966-6222; its FAX telephone number is 312-922-2734.

c. Make sliding glass doors as resistant to forcible entry as possible.

(1) Consider substituting glass-clad polycarbonate materials for the glass panels in the door. [redacted]

(2) Windows should be secured as described [redacted] Consider replacing windows in areas where family members will spend large amounts of time with glass-clad polycarbonate plates. [redacted] Any window accessible from the ground, neighboring structures, trees, walls, or readily accessible platforms (e.g., parked cars) should be protected with a high security screen, grillwork, or bars. In addition, such windows should be equipped with IDS sensors.

d. INSTALL AN INTRUSION DETECTION SYSTEM PROVIDING COVERT SURVEILLANCE OF ALL EXTERIOR OPENINGS IN THE RESIDENCE, ALL GATES THROUGH THE EXTERIOR PERIMETER, AND ALL UTILITY CONNECTIONS TO THE RESIDENCE.

Depending on the nature of the threat, the relations between the U.S. Government and the host government, and the security resources available to U.S. forces, consideration should be given to installation of IDS annunciators both in the home and in the central security office at the appropriate U.S. military installation. Local annunciation would alert all the HRPs in the residence to immediate action in their own defense; remote annunciation at the appropriate U.S. military installation would permit notification of local authorities of a possible incident and dispatch of U.S. security personnel to assistance host national law enforcement and security personnel in accordance with SOFAs and other MOUs in effect.

e. Consider installation of a secondary security wall equipped with a medium security door separating family sleeping areas from the rest of the residence.

In addition, install IDS sensors in hallways, entryways, and stairways. The secondary security door which forms a barrier between the sleeping areas and the rest of the residence should be equipped with a vibration type sensor to detect intrusion attempts.

f. Consider adding appropriate external security lights.

Such lights should provide sufficient light to facilitate functioning of covert CCTV or other surveillance systems. They may also be aimed in a manner that creates glare in the eyes of those outside the perimeter of the residence, complicating terrorist surveillance and intelligence collection. Lights may be either automatic (turned on and off by timer or photoelectric cell), motion detector initiated, or both.

g. CONSIDER INSTALLING A SAFEHAVEN. [redacted]

(1) Safehavens can be applied in residences as well as offices. Figure 11-2 illustrates the installation of a safehaven in an apartment or single family residence hallway area.

DELETE

Figure 11-2. Safehaven Concept Including Residence Hall Security Barrier

(2) Safehavens installed in residences should be supported by covert CCTV cameras scattered around the house connected to CCTV monitors installed in the safehaven. The use of covert CCTV cameras provides surveillance information to the occupants of the safehaven regarding the presence of intruders, law enforcement personnel, or both. Occupants of the safehaven may also be able to provide additional information about the presence, location, and armament of intruders based on observations by covert CCTV cameras.

(3) It is possible to link CCTV displays in the safehaven to a central station along with other IDS sensors. In normal situations, the CCTV signal would not be transmitted to the central station. If, however, the occupants had to retreat into the safehaven, the IDS might be equipped with a device permitting either manual or automatic relay of CCTV data. IDS and CCTV information is vitally important to response forces. They need to know whether or not intruders remain in the residence, if the intruders are armed or injured, and if there are other persons in the residence that might have a bearing

[redacted]

(4) [redacted]

3. Residential Security Guards

In certain high threat areas overseas, residential security guards are recommended. In some cases, the nature of the threat and DoD presence in country will be such that the U.S. Embassy will provide residential guards.[3] [redacted]

4. Animals

a. A variety of animals have been used a one time or another in different parts of the world as living alarm and security protection systems. While geese, ducks, and monkeys can be depended upon to create a racket when disturbed, the most commonly used animal has been the dog.

b. A dog possesses many security assets. A dog's greatest asset is his alertness to danger. His senses are far more highly developed that those of a human. For example, his sense of smell is one hundred times greater than that of a human. A dog can discriminate between odors which seem to a human to be identical. A trained dog can detect an intruder's scent in excess of 250 yards. A dog's ability to hear surpasses a human's in both range and pitch. His upper frequency limits are twice that of a man. A dog's senses of sight and touch for the most part are no greater than a man's. In fact, his vision is generally considered to be weaker than man's. Dogs are believed to be color blind, and all objects appear blurred and out of focus to a dog. However, they are generally more cognizant to movement despite other visual weaknesses.

c. The dog's sensitive and discriminating senses of smell and hearing enable him to quickly detect a stranger who is not normally present in the residential area, and the well trained dog will normally bark when approached by an intruder. Thus, they can be classified as living audible alarm systems. Like all alarm systems, dogs are sometimes subject to false alarms. A nervous or high strung dog barking at almost any distraction negates his effectiveness. To avoid the wrath of neighbors and for the owner's peace of mind, the dog should be trained to react only to the introduction of strangers into the neighborhood, and trained to stop barking at the command of the owner.

---

3 For detailed discussion on the procedures used to i[redacted]

E. RESIDENTIAL SECURITY SUMMARY

1. Functional analysis of the physical security system applied to DoD installations and facilities can also be applied to residences of DoD personnel. All physical security system functions performed in defense of an installation are performed in defense of a residence. While resource limitations may constrain the level of protection available, the principles do not change. If terrorist threats can be detected, classified and identified, and annunciated, residential physical security systems can be designed to delay terrorist attacks long enough to permit local law enforcement and DoD security forces to provide relief.

2. Residential security is an important facet of protecting DoD personnel assets. Protection is provided by DoD and the DoS on the basis of the terrorist threat to DoD personnel, the risk of attack, the probability that if an attack is undertaken at the DoD persons residence, it will be successful, and the importance of the DoD personnel to the successful accomplishment of DoD and U.S. Government policies. Provision of residential security services to DoD personnel is unusual.

3. DoD personnel should not feel helpless in the face of a terrorist threat. There are many measures to be undertaken by individuals and their families to reduce their risk of becoming the victim of a terrorist attack. [redacted]

CHAPTER 12

INDIVIDUAL PROTECTIVE MEASURES

A. INTRODUCTION

DoD Directive 0-2000.12 (reference (a)) declares DoD policy "to protect DoD personnel and their families, facilities, and other material resources from terrorists acts." Physical security measures to enhance the security of DoD-affiliated personnel have been examined. In this chapter, attention turns to steps that can be taken by each and every person affiliated with DoD to reduce or mitigate the dangers of becoming victims of terrorist attack.

B. GENERAL APPROACH TO INDIVIDUAL PROTECTIVE MEASURES

1. Personnel Protection: Plan and Leadership

a. U.S. Government civilian and military personnel, as well as civilian contractors associated with the U.S. Government are often targets for terrorist activity. Heads of DoD components have two major antiterrorism responsibilities:

(1) Provide as much security for personnel under their authority and control (to include dependents) consistent with threat, risk, vulnerability, criticality assigned roles, missions, and resources; and

(2) Provide awareness information and educational materials to assist Service members, DoD civilians, and contractor personnel prepare themselves and their dependents to reduce their individual risk and vulnerability to terrorist attack.

b. Security managers or others designated by Heads of Defense Agencies, the Military Services, the Unified and Specified Commands, commanders of military installations, and commanders at all echelons should develop a personnel protection plan. An antiterrorism personnel protection program has three phases.

2. Planning Phase

The Planning Phase has four steps as outlined below.

a. Threat Analysis

(1) All civilian managers or military commanders should obtain a TERRORISM THREAT ANALYSIS from counterintelligence, intelligence, and law enforcement organizations to identify the presence of terrorist threats to security in their respective areas of operation. Such assessments should include data on threat factors as existence, history, capability, intentions and targeting.

(2) As part of the threat assessment, information on terrorist intelligence collection and targeting methods used against past victims should be obtained. Such information is essential in the development of awareness and education plans, programs, and activities.

b. Risk, Vulnerability, and Criticality Assessments

(1) A RISK ASSESSMENT examining the likelihood of terrorist attack on DoD personnel and their dependents assigned at each DoD post should be undertaken. Those personnel who meet the definition of "high-risk personnel" or who occupy "high-risk billets" should be specifically identified and individually assessed.

(2) A CRITICALITY AND VULNERABILITY ASSESSMENT of all individuals who are at risk should be assessed to be at high or even moderate risk should also be undertaken. The purposes of such assessments is to identify those individuals who are mission-essential and who therefore may because of their vulnerability to terrorist attack, warrant special protective measures, including but not necessarily limited to the following:

(a) Augmentation of security devices used in the office, home and vehicle environments;

(b) Assignment to DoD antiterrorism resident or mobile training course;

(c) Provision of Protective Security Details for periods or tasks at which the risk is highest; and

(d) Assignment of transportation on a domicile to duty basis.

(3) Other individuals may be identified as being vulnerable because of high visibility, because they are assigned to remote locations far removed from security support, or because the nature of their work brings them into close contact with others who are considered to be at high risk. Even if such individuals are not mission critical, special security provisions including some of those outlined above may be appropriate.

c. Resource Requirements and Availability

After completing assessments of threat, risk, criticality, and vulnerability, an assessment of available personnel security resources must be completed. In performing this assessment, it is essential that planners consider those cases in which resources usually available for personnel security are allocated to other tasks. The personnel security plan should have preplanned alternate security arrangements to take such considerations into account.

d. Continuing Review

The last step in the planning process is the periodic review of all planning inputs. Terrorist threat levels change almost daily in certain parts of the world; rapidly changing missions and responsibilities may alter assessments of personnel criticality and vulnerability. Hence, antiterrorism personnel protection planning is best conceived as a continuing, iterative process, not an annual exercise. It must be performed in light of daily or weekly programs of assigned missions and functions at each installation, facility, activity.

3. Personnel Protection and/or Terrorism Awareness

a. The second phase in a personnel protection program is to increase awareness of the possible threat of terrorism. Officials responsible for AT programs should inform all DoD personnel including dignitaries, civilian employees, and dependents of the terrorist threat in general, as well as the perceived threat level in the general area of the installation or area of operations of the DoD activity. This can be accomplished through periodic briefings and through the preparation and dissemination of printed materials.

b. The need for personnel security procedures should be explained during the awareness stage of the personnel protection program. The specific procedures to be followed are presented during the education phase of the personnel protection program. Since it is logistically impossible to protect all possible terrorist targets, SELF-PROTECTION AND EFFECTIVE CRIME PREVENTION PROCEDURES WILL DETERMINE THE OVERALL EFFECTIVENESS OF THE ANTITERRORISM PROGRAM.

c. All personnel including dependents and contractor personnel should receive crime prevention training. CRIME PREVENTION IS THE CORNERSTONE OF A PERSONNEL SECURITY PROGRAM. Military personnel and dependents alike should be encouraged to participate in crime-watch programs. They must know how to report suspicious activities. Checklists which can be used in crime prevention surveys are included in Appendix O and Appendix P. A self-protection guide can be found in Appendix F. People who carry out crime prevention procedures in their homes, their offices, and their day-to-day operations will significantly decrease their possibility of becoming a terrorist target.

d. Terrorist threat information should be included in briefings on security and espionage directed against the DoD personnel and DoD contractor personnel. The public affairs office for each DoD component should routinely keep track of open source information on terrorist activities and assist in the development and presentation of awareness briefings. Presentations can be made in schools and to social and service organizations. The purpose of these briefings is not to scare participants, but to make them aware of the personnel security threat in the area. Such briefings should present factual information about the strategies and tactics being used by terrorists and the types of facilities and/or personnel that have been targeted. In addition, such presentations should make DoD audiences aware of changes in the overall security environment.

4. Personnel Protection Education and Training

a. The third step in the personal security process is the acquisition of specific knowledge and education which can be applied by DoD-affiliated personnel to reduce the likelihood of becoming the victims of terrorist or other criminal acts. In the sections that follow, several specific antiterrorism measures that can be used by all persons to reduce the risk of attack are presented. Additional material appears in Appendices F through S.

b. Commanders and managers have a continuing responsibility to ensure that DoD-affiliated personnel receive comprehensive security awareness briefings. These security briefings, which should include such topics as hostile intelligence service threats, protection of government property, crime watch, and physical security as well as

information on terrorist threats, are an essential ingredient in reducing the risk of harm to DoD-affiliated personnel from all potential sources.

5. Leadership by Example

a. THE ATTITUDE DISPLAYED BY MANAGERS AND SENIOR OFFICERS TOWARDS PHYSICAL SECURITY, INFORMATION SECURITY, AND PERSONNEL SECURITY IS MOST IMPORTANT. The example set by senior officials and officers at each organizational level will send an unmistakable message to all personnel assigned to or coming into contact with the organization. Those leaders who view the threat of terrorism seriously, who heighten awareness of the threat, and who actively practice antiterrorism measures in their daily lives will encourage others to do the same.

b. While some antiterrorism precautions are more applicable overseas than in CONUS, development of good security and antiterrorism habits is the key to personal safety for DoD personnel and their dependents. Practice of antiterrorism measures even in countries or regions where the terrorist threat level is considered NEGLIGIBLE is excellent preparation for deployment, temporary duty assignments, or other activities where the terrorism threat level is MEDIUM or HIGH.

c. Information on specific personnel security topics appears in Appendices E through S. Local reproduction and distribution to DoD personnel, their dependents, and DoD contractor personnel is encouraged. All DoD-affiliated personnel and their dependents should review these precautions on a regular basis.

C. PERSONAL PROTECTION MEASURES FOR DoD PERSONNEL

1. General Guidance

a. As noted in Chapter 2 of this Handbook, terrorists frequently emulate military organizations as they develop, plan, train, and carry out terrorist attacks attacks against DoD assets. Like all military or paramilitary organizations, terrorists have a critical need for information regarding the whereabouts, habits, working environments, home environments, and other potential points of leverage against their targets. Intelligence collection and analysis is therefore a major function within terrorist organizations.

b. Three intelligence collection methods used by terrorists against their potential targets have been noted:

(1) Human Intelligence (HUMINT) - Terrorists attempts to use people to gather information about military capabilities and intentions can be countered by adhering to physical and information security practices. HUMINT collecting can include seemingly unimportant bar or restaurant conversation concerning operations or the release of telephone numbers and addresses of key personnel.

(2) Photographic Intelligence (PHOTINT) - Terrorists attempts to gather information through photography of surveillance procedures. Established patterns provide information to a terrorist, to counter, eliminate routines and/or when possible use deception to mask an established pattern.

(3) Signals Intelligence (SIGINT) - Terrorist attempts to intercept communication signals; to counter this activity, classified material must be discussed only on secure lines; other sensitive material including personal schedules, travel itineraries, and VIP visits, should also be discussed only on secure lines.

c. One of the most important individual protective measures that can be taken by DoD-affiliated persons is to develop personal habits and practices that frustrate terrorist attempts to determine their nationality, their professions, their individual job responsibilities, their association with the Department of Defense, and their overall importance to the Department of Defense. The following are a few general observations that apply to DoD personnel, DoD contractors, and dependents.

2. Overcome Routines

Most persons and organizations fall into habits or routine behaviors. Work begins and ends at the same time every day; meals are eaten in the same cafeteria; exercise takes place at the same time and at the same location every day; and individuals follow the same route to and from the office every day. Terrorists normally plan their actions carefully. They will observe the potential target's routines in order to decrease their risks and increase the probability of success. The ability to be unpredictable increases the risks to terrorists and severely decreases the chances of their success. Reduced probability of success in kidnapping or killing a target makes target far less desirable.

a. VARY YOUR ROUTE TO AND FROM WORK, AND THE TIME YOU ARRIVE AND LEAVE.

b. Exercise on a varying schedule, utilizing different routes and distances. It is best not to exercise alone.

c. Avoid routines (time and location) for shopping, lunch, etc.

d. Do not divulge family or personal information to strangers.

e. Enter and exit buildings through different doors, if possible.

3. Maintain a Low Profile

a. Americans are fairly easy to identify in an overseas area.

(1) DOD PERSONNEL, DOD CONTRACTORS, AND THEIR DEPENDENTS SHOULD DRESS AND BEHAVE IN PUBLIC IN A MANNER CONSISTENT WITH LOCAL CUSTOMS. Items that are distinctively American should not be worn or displayed outside American compounds unless necessary to accomplish official business.

(2) Examples of such items include:

(a) Cowboy hats, cowboy boots, Western belts.

(b) Clothing adorned with American flags or other national symbols (Statute of Liberty), city, or commercial logos.

(c) Suitcases, backpacks, brief cases, attache cases, or shopping bags with stickers, decals, or other distinctively American symbols.

(d) Tattoos, patches, military duffel bags, or military style clothing, with or without unit or American identification markings.

(3) SHOW RESPECT FOR LOCAL CUSTOMS.

Refrain from smoking in public; wear proper attire when visiting national monuments, houses of worship and other religious shrines or institutions, public buildings; and limit public displays of affection to the mannerisms used by local residents to show affection and respect for spouses, elders, and children.

(4) REDUCE VISIBILITY IN THE LOCAL COMMUNITY.

DoD-affiliated personnel are good citizens and often desire to participate in all community activities. Reducing the visibility of DoD-affiliated persons within a community should not mean that DoD-affiliated persons should give up active community life as PTA members, Scout leaders, memberships in religious or educational organizations. It does mean that DoD-affiliated persons should reconsider running for elected leadership positions in community organizations. They should shun publicity where possible, and avoid serving in civic positions where publicity cannot be avoided.

(5) DO NOT FLASH LARGE SUMS OF MONEY, EXPENSIVE JEWELRY, OR LUXURY ITEMS.

4. Be Sensitive to Changes in the Security Atmosphere

Security awareness should be encouraged at all times. Specifically, watch out for the following:

a. BE ALERT FOR SURVEILLANCE ATTEMPTS, OR SUSPICIOUS PERSONS OR ACTIVITIES, AND REPORT THEM TO THE PROPER AUTHORITIES.

Trust your gut feelings. If you think something is wrong, you are probably right. Report suspicions and concerns to the installation or unit security officials immediately; if they are not available, report such information to the nearest intelligence activity

b. WATCH FOR UNEXPLAINED ABSENCES OF LOCAL CITIZENS AS AN EARLY WARNING OF POSSIBLE TERRORIST ACTIONS.

c. Avoid public disputes or confrontations. Report any trouble to the proper authorities.

d. Do not unnecessarily divulge your home address, phone number, or family information.

5. Be Prepared for Unexpected Events

Even though DoD personnel, DoD contractors, and their dependents may do everything recommended above and elsewhere in this Handbook, they may still be threatened by or become victimized by a terrorist act. Therefore, all DoD personnel, DoD contractors, and their dependents should implement the following general measures.

a. Get into the habit of "checking in" to let friends and family know where you are or when to expect you.

b. KNOW HOW TO USE THE LOCAL PHONE SYSTEM. Always carry "telephone change."

Know the emergency numbers for local police, fire, ambulance, and hospital. Memorize the phone numbers for local military police, the nearest U.S. Embassy or consulate, or other U.S. Government missions who might be in a position to summon aid should assistance be needed.

c. KNOW THE LOCATIONS OF CIVILIAN POLICE, MILITARY POLICE, GOVERNMENT AGENCIES, THE U.S. EMBASSY, AND OTHER SAFE LOCATIONS WHERE YOU CAN FIND REFUGE OR ASSISTANCE.

d. Know certain key phrases in the local language.

Such phrases include "I need a policeman," "Take me to a doctor," "Where is the hospital?," and "Where is the police station?" If such phrases are difficult to learn or time is too short, have someone write them down on small file cards. A 3 × 5 card can contain several phrases written out phonetically that can be read to summon assistance; alternatively, they can be written down so that a person in need of assistance can merely show a card to someone competent in a local language, thereby summoning help.

e. SET UP SIMPLE SIGNAL SYSTEMS THAT CAN ALERT FAMILY MEMBERS OR ASSOCIATES THAT THERE IS A DANGER. Do not share this information with anyone not involved in your signal system.

f. Carry identification showing your blood type and any special medical conditions. Keep a minimum of a one week supply of essential medication on hand at all times.

g. Keep your personal affairs in good order. Keep wills current, have powers of attorney drawn up, take measures to ensure family financial security, and develop a plan for family actions in the event you are taken hostage.

h. Do not carry sensitive or potentially embarrassing items.

6. Working Environments

a. The working environment is not immune from attempted acts by criminals or terrorists. DoD installations in CONUS and U.S. Government installations outside of CONUS usually provide a level of basic security comparable to or superior to the basic level of security provided in the surrounding community. Nevertheless, it is important that a sense of complacency not set in merely because the office is located in a nominally secure area.

b. The following are general practices that will aid in reducing the likelihood of terrorist attack:

(1) General Suggestions for Office Security

(a) Establish and support an effective security program for the office.

(b) Discourage use of office facilities to store objects of significant intrinsic value unless essential for the mission or function of the activity (such items include

petty cash boxes, firearms, personal stereos, binoculars, negotiable securities, original artwork of potential commercial interest, etc.).

(c) Ensure that all persons working in an office are trained to be alert for suspicious activities, persons or objects.

(d) ARRANGE OFFICE INTERIORS SO THAT STRANGE OR FOREIGN OBJECTS LEFT IN THE ROOM WILL BE IMMEDIATELY RECOGNIZED. Consider removing obvious obstructions behind which or within which improvised explosive devices could be concealed such as draperies, closed waste baskets, unsecured desks and filing cabinets, and planters.

(e) Provide for security systems on exterior doors and windows.

(f) Ensure that access control procedures are rigorously observed at all times for access to:

1 The installation.

2 Buildings within an installation.

3 Restricted and/or exclusion areas with a building.

(g) USE AN IDENTIFICATION BADGE SYSTEM CONTAINING A PHOTOGRAPH.

Photo badge systems facilitate security by making it easy to identify employees, visitors, maintenance personnel, and facilities management and/or security personnel. Badges should be renewed periodically; badging systems should be modified every two or three years to preclude use of altered, expired or stolen badges.

(h) Locate desks in a way that persons entering the office or suite can be observed.

(i) IDENTIFY OFFICES BY ROOM NUMBER, COLOR, OR OBJECT NAME, and not by rank, title, or name of incumbent (room 545, the gold room, the Berlin room, the maple room, not the General's office, the Assistant Attache's office, or the S-2's office).

(j) DO NOT USE NAME PLATES ON OFFICES AND PARKING PLACES.

(2) Office Procedures

Day to day activities within an office can help establish an environment in which it is more or less difficult for terrorists to gain knowledge needed to successfully attack DoD personnel, facilities, material, or DoD contractors. The following steps can be taken to make intelligence collection and targeting more difficult for terrorists, forcing them to spend more time collecting information, leaving them exposed and visible for detection by counterintelligence and law enforcement efforts, and leaving them more vulnerable to counterterrorism as well as antiterrorism actions.

(a) Telephone and Mail Procedures

1 Rank or title should not be used when answering telephones.

2 When taking telephone messages, do not reveal the whereabouts or activities of the person being sought unless the caller is personally known to the individual taking the message.

3 COLLECT TELEPHONE MESSAGES IN UNMARKED FOLDERS; do not leave exposed for observers to identify caller names and phone numbers, persons called, and messages left.

4 Observe caution when opening mail. In particular, be on the lookout for letters or packages which might contain improvised explosive devices. A checklist to aid in letter bomb or packaged IEDs appears in Appendix Q.

(b) Visitor Control Procedures

1 Access to the executive office area should be strictly limited; during periods of increased threat, access to additional office, shop, laboratory, and other areas within the installation should also be controlled.

2 Doors from the visitor access area to executive offices or other restricted areas of a facility should be locked from within; there should be only one visitor entrance and exit to a restricted access or exclusion area.

3 Have a receptionist clear all visitors before they enter inner offices.

4 Permit workmen or visitors access to restricted areas or exclusion areas only with escort and only with proper identification; confirm work to be done prior to admitting workmen to restricted areas of the facility.

5 Limit publicity in public waiting areas to information that does not identify personnel by name, position, or office location.

6 DO NOT POST UNIT ROSTERS, MANNING BOARDS, OR PHOTO BOARDS WHERE THEY CAN BE VIEWED BY VISITORS OR LOCAL CONTRACTORS PROVIDING CLEANING SERVICES, FOOD AND BEVERAGE SERVICES, DELIVERY OF OFFICE SUPPLIES, REMOVAL OF TRASH OR WASTE, CARE OF PLANTS, ETC.

7 Restrict use of message boards, sign in-out boards, and other visual communications to general statements of availability; do not list publicly local travel itineraries or phone numbers where visitors have easy, unrestricted access to such information.

(3) General Working Procedures

(a) Avoid carrying attache cases, brief cases, or other courier bags unless absolutely necessary.

Brief cases and attache cases have become symbols or power and prominence in many cultures. Individuals carrying such items are often assumed to be very important persons. Use satchel, bag, or other locally obtained book bag instead.

(b) Do not carry items that bear markings which identify the owner by rank or title, even within the office environment.

Coffee mugs labeled "General, Attache, Boss" may be seen in use by a visitor sent to gather intelligence to aid in targeting.

(c) Avoid working alone late at night and on days when the remainder of the staff is absent.

(d) IF LATE NIGHT WORK IS NECESSARY, WORK IN CONFERENCE ROOMS OR INTERNAL OFFICES WHERE OBSERVATION FROM THE OUTSIDE OF THE BUILDING IS NOT POSSIBLE.

Persons working at night should turn lights on and off in several offices before going to their own offices to disguise the purpose of their activities to outside observers.

(e) Office doors should be locked when vacant for any lengthy period, at night and on weekends.

Keys to the office should be retained by the security office and the incumbent.

(f) Papers, correspondence, communications materials, and other documents should not be left unattended overnight.

[redacted]

(g) Maintenance activity and janitorial services in key offices, production, maintenance or other areas installation areas should be performed under the supervision of security personnel.

(h) Removal of property, materiel, or information stored on any media from the facility should be prohibited without proper written authorization.

(i) Consider prohibiting the importation of property, materiel, or information stored on any media into the facility unless such items have been properly inspected.

Inspection of boxes, briefcases, handbags, and other containers should focus on improvised explosive devices, fire arms, incendiary devices and accelerants, and information collection devices. Inspection of electronic media should focus on computer viruses or other programs which might be used to modify operating systems or applications programs permitting unauthorized access to information stored on or accessed through the facility's computers.

(j) Offices not in use should be locked to prohibit unauthorized access or the storage of material which could be used to hide improvised explosive devices or intelligence collection devices.

(k) Use of vehicles or vehicle markings which make it possible to readily identify the vehicle and its occupants as U.S. Government or DoD contractor personnel should be minimized.

(l) ALL PERSONNEL SHOULD HAVE ACCESS TO SOME SORT OF DURESS ALARM TO ANNUNCIATE AND WARN OF TERRORIST ATTACK.

(m) Secretaries and guard posts should be equipped with covert duress alarms which can be used to alert backup forces, summon assistance, or otherwise alert critical personnel for the need to take special actions to avoid a terrorist incident.

(n) Placement of office furnishings directly in front of exterior windows is to be avoided if at all possible.

(o) Armed Forces Radio and Television broadcasts should refer members of the American community to written announcements of public events, recreational activities, town meetings, etc., and refrain from announcing specific times, dates, and places where DoD-affiliated personnel might be expected to congregate.

(4) Special Procedures for Executive Assistants

Many critical personnel will have secretaries or executive assistants assigned to their offices to provide additional clerical and professional support. These assistants can be significant security assets if properly trained, and can represent the difference between a successful or unsuccessful terrorist attack. The following suggestions are intended to be a guide for secretaries and executive assistants who may find themselves performing personnel security duties as collateral duty.

(a) Request installation of physical barriers such as electromagnetically operated doors to separate offices of senior executives from other offices.

(b) REQUEST INSTALLATION OF A SILENT TROUBLE ALARM BUTTON, with a signal terminating in the Security Department or at another the secretary's desk some distance away to ensure that in the event of an emergency it will be possible for someone other than the executive to summon assistance.

(c) Do not admit visitors into the executive area unless they have been positively screened in advance or are known from previous visits.

If the visitors arrive without appointments, they should not be admitted are until satisfactory identification and valid reasons for the visit have been established. In such instances, installation security should be notified and a security officer asked to come to the scene until the visitors establish legitimate reasons for being in the office. If the visitors cannot do so, the security officer should be asked to escort the visitor out of the building.

(d) Unknown callers should not be informed of the whereabouts of the executive, his/her home address, or telephone number.

(e) A fire extinguisher, first-aid kit, and oxygen bottle should be stored in the office area.

(f) When receiving a threatening call, including a bomb threat, extortion threat, or from a mentally disturbed individual, remain calm and listen carefully.

Each secretary and/or receptionist should have a threatening telephone call checklist which should be completed as soon as possible. A recommended checklist is attached as Appendix Z.

(g) Do not accept packages from strangers until satisfied with the individual's identity and the nature of the parcel.

(h) TRAVEL ITINERARIES FOR ALL PERSONNEL SHOULD BE KEPT ABSOLUTELY PRIVATE. Distribution should be limited strictly to those with a need to know.

(i) DAILY SCHEDULES FOR SENIOR OFFICERS AND CIVILIAN OFFICIALS SHOULD BE DISTRIBUTED ON A LIMITED BASIS AND SHOULD CONTAIN ONLY THAT INFORMATION NEEDED BY EACH RECIPIENT.

For example, if the Defense Attache is scheduled to meet with his staff and the Embassy's foreign military training staff, the schedule distributed within the Embassy should only indicate that the Attache will be in a meeting during the scheduled block of time. Those participating in the meeting should be given specific, supplemental information in a separate package.

7. Safehaven

Although substantial physical security, personnel security, and operational security measures can be promoted and implemented, there always remains the possibility that a terrorist incident will transpire. DoD personnel who are identified as mission critical to a unit, an installation, a command, or an activity, should be familiar with the location of safehavens available within U.S. Government and DoD installations. They should be briefed on emergency routes to and from their scheduled locations to such safehavens. Executive assistants and security personnel should regularly train and exercise procedures to be used in the event that it is necessary to evacuate mission critical personnel to safehavens.

8. At Home

DoD personnel, DoD contractors, and their dependents spend approximately half of each day in and around a primary residence. Almost everything done from day to day starts or ends in the vicinity of this residence. The following discussion is intended to assist personnel in formulating plans to obtain housing outside U.S. Government compounds or DoD facilities. However, given varying degrees of threats to life and property from common street crime as well as terrorist acts at home or abroad, even personnel assigned to government housing may find antiterrorism and security tips presented below to be helpful in reducing the threat of violence and loss of property.

a. DoD Member General Residential Security Routines

DoD personnel should SET AN EXAMPLE FOR ANTITERRORISM AND CRIME PREVENTION AWARENESS FOR THEIR FAMILIES AND FRIENDS. It is important that the DoD member explain how carelessness by any family member can place the DoD member and all other family members at risk of terrorist attack. Such discussion should be

appropriate to the family member audiences. Discuss with family members the importance of:

(1) Varying routines in their daily activities.

(2) Blending in with the local environment.

(3) Avoiding unnecessary publicity and photographs which identify individual family members or which associate family members and DoD personnel.

(4) Being alert to the presence of individuals, parked or abandoned vehicles, unusual utility work, or gatherings of people inconsistent with the residential environment.

b. Security Practices at Home

The following measures are specifically recommended for residential implementation as an extension of office antiterrorism security practices:

(1) Do not use name plates or uniquely American symbols on the exterior of residences occupied by DoD personnel overseas. House numbers alone should be used to identify residences occupied by DoD personnel.

(2) Do not use name plates on parking places; avoid parking private or government vehicles in the same location day after day.

(3) All family members should answer the telephone politely but should provide no information as to the name of the occupants until the identity of the caller has been established.

(4) ALL FAMILY MEMBERS SHOULD TREAT ALL TELEPHONE CONVERSATIONS AS THOUGH ANYONE WHO WANTED TO LISTEN IN WAS DOING SO.

(5) All mail delivered to the residence should be carefully examined; any mail or packages from senders who cannot be immediately identified should be set aside for opening by the DoD member.

c. At Social and Recreational Activities

DoD personnel are encouraged to participate in many social and recreational activities. Participation in such activities does not in and of itself add to the risk or vulnerability of DoD personnel or their dependents to terrorist attack. However, some precautions are noteworthy.

(1) Respond to formal social invitations by personal visit where possible, or direct telephone contact with the principal; avoid widespread uncontrolled dissemination of social or recreational plans.

(2) Be attentive to the security environment of social gatherings; do not remain at a function if it does not appear to be adequately protected.

(3) Avoid the development of patterns with respect to time of arrival or departure at social events; do not always arrive promptly on time or be consistently fifteen minutes late; do not always leave early or be the last person to leave the function.

(4) Try to avoid prolonged presence at social functions where there is a high concentration of persons thought to be terrorist targets; try to limit known exposure to risk.

(5) REFRAIN FROM EXCESSIVE USE OF ALCOHOL AT SOCIAL FUNCTIONS; REMAIN CLEAR HEADED AND UNIMPAIRED; BE READY FOR THE UNEXPECTED.

(6) Vary routes to and from social events held at a central facility; use different entrances and exits.

(7) Minimize appearances in uniform or formal attire.

(8) DECLINE INVITATIONS TO APPEAR IN PUBLICITY PHOTOS; if photos are taken, discourage publication of names associated with persons appearing in the photo.

(9) Participate in recreational activities within the American compound or at a DoD installation whenever possible; try to select playing fields or recreational areas in secured installations or within easy reach of such installations if it is thought that terrorist activity is particularly likely.

D. FAMILY MEMBERS OF DoD-AFFILIATED PERSONS

All family members of DoD-affiliated persons should become informed about personal security measures. Whether they become victims themselves, or must respond to the victimization of another family member, each individual within the family unit should be aware of basic security procedures. DoD personnel should cultivate an interest in and attract participation from all family members in the security effort. This should include a predetermined plan for responding to potential criminal or terrorist acts. The following tips are provided for a more effective family effort:

1. General Guidance

a. Develop a family oriented antiterrorism awareness, education, and training plan as part of preparing for each new assignment.

(1) Family members require awareness, education, and training in personnel security antiterrorism techniques just as DoD personnel do. The DoD members should begin by developing a plan for personal protection, acquiring and maintaining information on terrorist threats operating in the vicinity of their assignment and their family members, and developing specific personal security measures and other precautions appropriate for their dependents.

(2) Preparation should begin prior to departure for a new assignment. All family members should try to learn about the customs, culture, history, and geography of the area to which the DoD member has been assigned. Study efforts need not be confined to "book learning." Use videos, museum trips, travel magazine articles, and visits with friends who have been assigned to the same or a nearby location. Family security and awareness briefings may be available upon request of the unit, installation, command, or other security or intelligence office. All the family members can begin to scan the newspapers for current events coverage of the region to which they are going. Learning about the area of assignment, its culture, its people, and its customs, whether in CONUS or overseas, is an important part of becoming aware of the security environment.

Investment in education will pay large dividends in all facets of a new assignment, not merely in reducing the risk of becoming a terrorist's victim.

(3) The general antiterrorism security measures discussed in Section B, above, apply equally to family members as well as DoD personnel. The key elements noted earlier are the following:

(a) Overcome Routines

1 Vary routes, arrival, and departure times to and from school, after school activities, day care, religious school, music lessons, and other regular, recurring family member activities.

2 Vary times and places for shopping, lunch, and other appointments.

3 Go to church or synagogue at different locations, at different times, and even on different days.

(b) Maintain a Low Profile

DoD Personnel should explain the risks and benefits of high profile, high visibility lifestyles to their dependents.

1 It is sometimes very difficult for many families to go from being highly visible members of a community to being nearly invisible. Visibility is often especially important to adolescents and non-working spouses of DoD personnel. The differences and distinctions among participation in community events such as school plays, sports, and social clubs as opposed to high profile participation should be discussed. DoD personnel should explain to their dependents the benefits and risks associated with high profile, highly visible lifestyles in certain environments.

2 Tips on reducing the distinctly "American" or "U.S. Military" profile discussed above apply equally to family members.

(c) Be Alert to and Changes In the Security Atmosphere

All DoD personnel and their dependents should be alert to their security environment and changes that may occur in it. Dependents should be told:

1 Be alert for surveillance attempts, or suspicious persons or activities, and report them to the proper authorities.

2 Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.

3 Avoid public disputes or confrontations. Report any trouble to the proper authorities.

4 Do not unnecessarily divulge your home address, phone number, or family information.

(d) Be Prepared for Unexpected Events

Dependents of DoD should be instructed on steps they can take to deal with unexpected events. Measures listed below should be adapted to meet the needs of each family member:

1 Get into the habit of "checking in" to let friends and family know where you are or when to expect you.

2 Know how to use the local phone system.

3 Know the locations of civilian police, military police, government agencies, the U.S. Embassy, and other safe locations where you can find refuge or assistance.

4 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?"

5 Set up simple signal systems that can alert family members or associates that there is a danger. Do not share this information with anyone not involved in your signal system.

6 Carry identification showing your blood type and any special medical conditions.

2. Routine Family Security Precautions

a. Develop a family duress code so that family members can warn each other when they are in danger.

b. Develop emergency procedures and practice them.

c. Maintain emergency telephone numbers for all family members.

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

e. DO NOT "HIDE" KEYS OR GIVE THEM TO VERY YOUNG CHILDREN.

f. Never leave young children at home alone.

g. Never admit strangers to your home without proper identification.

h. TEACH CHILDREN HOW TO CALL THE POLICE AND ENSURE THEY KNOW WHAT TO TELL THE POLICE (NAME, ADDRESS, ETC.).

i. Carefully screen all potential domestic help.

j. Use off street parking at your residence, if at all possible.

k. Avoid frequent exposure on balconies and in windows.

l. Do not store items of high intrinsic value in your home unless they are frequently used; e.g., keep heirloom jewelry, rare stamp and coin collections, negotiable securities, etc., in bank vaults or safety deposit boxes.

m. Do not tack notes on the door for family and friends to read; remember, criminals and terrorists can read too.

n. Keep tools, particularly ladders, under lock.

3. Family "Operations Security" Procedures

Families can improve their security posture by bringing to bear operations security concepts. The purpose of operations security is to frustrate adversary collection of information about one's activities. [redacted] The following measures are only a small number of examples of steps that should be implemented to make it harder for terrorists to learn the nationality, specific identity, position, and responsibilities of DoD personnel, as well as the day-to-day activities of DoD families.

a. Do not place your name on exterior walls of residences.

b. Do not answer your telephone with your name and rank; children and domestic employees should be instructed not to identify the name, title, or affiliation of the occupants when answering the telephone

c. Do not list your telephone number and address in local directories.

d. CREATE THE APPEARANCE THAT THE HOUSE IS OCCUPIED BY USING TIMERS TO CONTROL LIGHTS AND RADIOS WHILE YOU ARE AWAY.

e. Personally destroy all envelopes and other items that reflect personal information.

f. Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.

g. Don't let your trash become a source of information.

4. Potential Threats

Even after implementing all of the measures outlined above, there is always a possibility that unexpected events will occur. Some may be strong indicators or warnings of an imminent terrorist incident. The following steps should be implemented when appropriate:

a. Any unusual occurrence such as anonymous phone calls, threats, etc., should be reported immediately.

b. CHILDREN SHOULD BE ON GUARD AGAINST ANY APPROACH OR INTERROGATION BY STRANGERS; efforts by strangers to pick up children, engage them in long conversations about their home life or find out what their parents do for a living should be reported to law enforcement and intelligence activities immediately

c. Never accept unexpected package deliveries.

d. Examine all mail carefully and look for signs that an improvised explosive or incendiary device has been received. See Chapter 16 and Appendix Q for additional information on detection and identification of IEDs.

e. REPORT FREQUENT WRONG NUMBERS OR NUISANCE TELEPHONE CALLS TO THE TELEPHONE COMPANY AND THE POLICE. Someone may be attempting to determine the presence of family members.

f. REPORT ANY INTERRUPTION IN TELEPHONE OR ELECTRICAL SERVICE, STRANGE NOISES ON TELEPHONE LINES, OR ANY UNUSUAL INTERFERENCE WITH RADIO, TELEVISION, OR HOME COMPUTER OPERATIONS TO THE NEAREST INTELLIGENCE OR LAW ENFORCEMENT ACTIVITIES. In the event that such utility service problems are unique to residences occupied only by DoD personnel, DoD contractors, or their dependents, report such disruptions immediately to the local security and law enforcement agencies as well as DoD law enforcement or intelligence activities.

g. Do not automatically open your door to strangers; use the peephole and always check credentials.

h. Be wary of talking to or admitting poll-takers and salespersons to your home. Terrorists are known to have gathered substantial information relative to their victims using these ruses.

i. Be alert to peddlers and all strangers.

j. Be alert to public utility crews or other workmen who request access to your residence. Check identities. If there is any doubt, refuse them admittance.

k. Report the presence of strangers in the neighborhood to military law enforcement or military intelligence activities as soon as their presence is detected.

l. Watch for strange cars cruising or parked frequently in the area, particularly if one or more occupants remain in the car for extended periods. Make a note of occupants, license numbers and province designators of suspicious vehicles.

m. If you come home and suspect that an unauthorized person is inside, do not go in to investigate and do not call out to the possible intruder. Contact the police or your security patrol.

n. Do not accept unsolicited packages. All mail should be routed through normal office channels.

5. Kidnapping and Hostage Issues

DoD-affiliated persons and their families should discuss steps to be taken if a member is kidnapped or otherwise becomes the victim of a terrorist attack. Families should understand the U.S. Government makes every effort to effect the rapid, safe release of any U.S. citizen held hostage. The importance of family cooperation in such a situation should be stressed. See Chapter 14 for additional discussion on techniques to survive kidnapping and being held hostage.

6. Special Guidance for Children

a. Parents have special responsibilities when providing personal security instruction for children. There are several children oriented or children specific measures that can be taken to enhance their and reduce the risk of terrorist attack against them:

(1) Never leave young children alone or unattended. Be certain when they are left, they are in the care of a trustworthy person.

(2) Instruct children to keep doors and windows locked, and never to admit strangers.

(3) Try to locate children's room(s) in a part of the residence that is not easily accessible from the outside.

(4) Make sure that outside doors and windows leading to children's rooms are kept locked, especially in the evening.

(5) Keep the doors to your children's rooms open so that unusual noises can be heard.

(6) Teach children how to contact the police or a neighbor in an emergency; also teach them how to contact DoD security or intelligence activities nearby; teach them how to contact the U.S. Embassy if overseas.

(7) If it is necessary to leave children at home, keep the house well lighted and notify the neighbors.

(8) Know where your children are all the time--morning, noon, and night.

(9) Be sure that anybody with whom children are left for day care, evening baby sitting, tutoring, or companionship is responsible and trustworthy.

(10) ADVISE SCHOOL OFFICIALS THAT CHILDREN ARE NOT TO BE RELEASED TO STRANGERS UNDER ANY CIRCUMSTANCES.

b. Preadolescents and teenagers should be taught and encouraged to take the following personal security steps:

(1) Never leave home without advising their parents where they will be and who will accompany them.

(2) Travel in pairs or groups.

(3) Walk along busy streets and avoid isolated areas.

(4) Use locally approved play areas where recreational activities are supervised by responsible adults and where police protection is readily available.

(5) Refuse automobile rides from strangers and refuse to accompany strangers anywhere on foot, even if the told by strangers that mom or dad sent them or said it was okay.

(6) Report immediately to the nearest person of authority (teacher, police) if anyone tries to pick you up or insists that you go for a ride with them.

c. DoD personnel should join with other parents involved with American community schools overseas, DoD Dependent Schools, and local public and private schools to enhance security. Ask schools to help provide security. Schools should be asked to do the following:

(1) To refrain from disseminating any information whatsoever about students.

(2) TO AVOID ANY KIND OF PUBLICITY IN WHICH STUDENTS ARE NAMED OR THEIR PICTURES ARE SHOWN.

(3) TO RELEASE A STUDENT TO SOMEONE OTHER THAN HIS/HER PARENTS OR CUSTODIAN ONLY AFTER RECEIVING WRITTEN AUTHORIZATION AND THEN ONLY AFTER CONFIRMING AUTHORIZATION BY TELEPHONE. In high-risk situations it is a good idea to allow the child to speak to the parent on the phone before authorizing the release. This practice provides protection against a kidnapper who calls and claims to be the child's parent.

(4) To report to the police if any strangers are seen loitering around the school or talking to students. If such strangers are in a car, the teacher should note its make, color, model, and tag number and pass this information on to the police.

(5) To have teachers closely supervise outside play periods.

E. TRAVEL SECURITY

1. The following section outlines several measures that when applied to official and recreational travel can decrease the likelihood of terrorist attack on DoD personnel and their dependents in transit. Such measures are intended to reinforce the general philosophy underlying personal protective measures:

- avoid routines,
- maintain a low profile,
- be alert, and
- be prepared for unexpected events.

Figure 12-1. General Approach to Personal Travel Security

a. The number of specific measures individuals and groups can take to implement this general approach to personal security while traveling is limited only by the imagination and creativity of the travelers. Use of the security measures should be tempered by the nature or purpose of their travel, the time and fiscal resources available, as well as the means and circumstances under which travel is to be made.

b. Readers are encouraged to expand the list of measures outlined below, as well as to consider the specific circumstances under which a proposed measure might diminish, not increase the security of DoD personnel and their dependents in travel status.

2. DoD Travel Security Policy Implementation

a. Official travel by DoD personnel, DoD contractors, and their dependents is the subject of the DoD Travel Security Policy. This policy document issued periodically by the Office of the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) sets forth special considerations, protections, and authorities to deviate from DoD Joint Travel Regulations in light of the risk of terrorist attacks against DoD personnel or their dependents in travel to or through high risk or high potential physical threat countries.

b. DoD Travel Security Policy authorizes the following deviations from the Joint Travel Regulations when security precautions are deemed necessary by OASD(SO/LIC):

(1) Reimbursement for DoD personnel purchase of U.S. Tourist passports and visa application fees for visits undertaken on official business;

(2) Authority to travel on non-U.S. flag carriers;

(3) Authority to travel via indirect route at greater cost to the U.S. Government to avoid high threat or high potential physical threat airports or other ports of entry.

c. DoD Travel Security Policy further directs tickets issued to DoD personnel and their dependents shall not be marked in any way to indicate that the traveler is affiliated with the U.S. Government. The Travel Security Policy further states itineraries for General Officers and other senior DoD Officials shall be marked "For Official Use Only" and shall be handled in accordance with command regulations for the dissemination of information so identified.

d. OASD(SO/LIC) staff, who review countries assessed by the intelligence community as having HIGH or MEDIUM Threat Levels, consider additional factors in determining whether or not waivers available under the DoD Travel Security Policy should be provided. Among the factors considered are the following:

(1) The risk of terrorist activity directed at personnel who are on TDY/TAD status in a country and who will be resident for less than 72 hours;

(2) The risk of terrorist activity directed at personnel who are on TDY/TAD or are merely itinerant passing through an airport with stopovers less than 12 hours;

(3) The ambient level of street crime and violence

(4) The ambient level of anti-American violence.

e. As a result of such assessment, OASD(SO/LIC) may determine that a country or region which has been assessed as having a CRITICAL or HIGH threat level does not qualify as a High Physical Threat or High Potential Physical Threat Country for purposes of application of the DoD Travel Security Policy.

f. It is possible, for example, that a country is assessed to have a HIGH Terrorist Threat Level because of attacks on government outposts, including attacks on American military personnel serving as advisers. However, on further review, it might also be shown that there is very good security at the major international airport, that the

international in-transit lounge and VIP waiting areas are especially well secured, and there is little or no history, evidence of intention, or capability information to suggest that American personnel passing through the international airport are at HIGH risk.

3. FAA Security Bulletins

[redacted] DoD will disseminate all FAA security information in a manner that is consistent with this policy. If FAA security information deals with threats to DoD personnel only, then such information will be disseminated in accordance with DoD component procedures. [redacted]

4. Department of State

a. The DoS monitors security conditions in countries with U.S. Embassies and Consulates. It provides a wide variety of security related information and advice upon request. It is the releasing authority for all unclassified and unlimited distribution information on international terrorism.

b. DoD-affiliated personnel seeking the most current public information on international terrorist threat concerns may call the DoS in Washington, DC, (202) 647-5225, to obtain the most recent unclassified unlimited information regarding the international terrorist threat and international travel.

5. General Travel Security Suggestions

The global distribution of DoD personnel, facilities, and contractors ordains much international and long-haul domestic travel for DoD personnel. Even local travel is not without its security risks. The following are some general comments that apply to all official travel. Additional travel security tips are to be found in Appendices I through N.

a. Do not assume that acts of terrorism "can't happen to me."

A common thread among accounts of individuals held hostage by Hizballah terrorists in Lebanon after their release was their own cavalier attitude towards warnings issued by the DoS and other governments' foreign ministries regarding travel to Lebanon.

b. Realize the impact of security on your travel itinerary.

Consider the security implications of destination, routing, and timing of travel and allow extra time for investigating, planning, and using alternative, more secure itineraries. Allow extra time between connections, if any, to allow for security inspections at airports, ports of entry, and other inspection points.

c. Avoid routine schedules.

Whether planning a trip or executing a plan assembled by others, avoid following travel routines used by others. Select unusual departure and arrival sites;

schedule personal time and business activities at odd hours, during evenings, or on weekends. Be particularly sensitive to the possibility of surveillance. Arrival and departure times, as well as routes taken to and from work and/or home, should be varied as often as possible. Different vehicles should be used to make targeting more difficult. For official business, consideration should be given to using unmarked Government vehicles where available.

d. Travel in groups when possible where appropriate.

Isolated travelers make easy targets; small groups provide a sufficient number of eyes and ears to be alert to local security matters.

e. Avoid wearing military clothing.

Wearing military uniforms during periods of travel and recreation could attract unwanted attention. Even wearing "military style" clothing may arouse more attention than desired.

f. Carry identification.

When asked for identification give only the information requested. Never surrender your entire wallet or purse or leave your wallet and/or purse unattended. Carry identification that gives your blood type, as well as any special medical condition or medication requirement. Keep on hand at least a one-week supply of essential medicines.

g. Carry extra medication, eyeglasses, and other medical necessities.

If you take any medication regularly, take at least one week's extra supply with you. If you wear glasses, take an extra pair along. Keep all medication in its original container for customs inspections. if your medication is a narcotic, make sure you have a letter from your doctor in your possession. Carry all necessary medication with you in your purse or briefcase; do not put it in checked luggage.

6. Travel Arrangements

The process of making travel arrangements can provide terrorists copious quantities of information about travelers, their authorities and responsibilities, their importance to the Department of Defense and the U.S. Government, and their personal tastes in matters of lifestyle. Such information is of incalculable value for purposes of targeting The steps outlined below are intended to deny access to such information by terrorists. Other measures may be equally helpful in preserving the anonymity of DoD travelers, thereby complicating detection, identification, and targeting of such personnel for terrorist acts.

a. If available, consider using U.S. Transportation Command and/or Military Airlift Command flights or military contract carriers.

b. Try to arrange international travel through American military air terminals if possible.

c. Avoid travel through high threat areas, if possible.

d. Travel under an assumed name if appropriate.

e. Make travel arrangements at the last minute, or alternatively, make last minute changes in travel plans at minimal additional cost, to foil efforts at targeting based on data stored in travel reservation computers.

f. Do not discuss military affiliations with strangers.

g. Consider using a tourist passport.

h. [redacted]

i. [redacted]

j. Do not use luggage that clearly labels its owner as a DoD civilian employee or military member; e.g., B-4 bags, duffel bags, and sea bags.

k. REMOVE ALL DESTINATION AND BAGGAGE CLAIM TAGS FROM LUGGAGE, as well as decals, stickers, and other markings which unambiguously identify the luggage as having been through the United States (e.g., U.S. Customs stickers).

l. Use baggage identification tags that require some manipulation before the name of the bag owner is visible; try to use baggage tags that allow airline officials and customs inspectors to identify the owner of the bag by name, but otherwise do not provide information on the owner's address or country of origin.

m. Do not include controversial or inflammatory reading material in carry-on bags or checked luggage on international travel.

7. Vehicle Travel Tips

a. DoD personnel make millions of trips each year by automobile. Most occur without any incident. Automobile trips have become so integrated with official business, it is easy to dismiss use of vehicles as much more dangerous than a walk down a corridor from one office to another.

b. Indiscriminate use of automobiles for the conduct of official business can be a major weakness in personal security efforts. As in the foregoing discussion of travel arrangements, consider steps to be taken to reinforce efforts of DoD personnel and their dependents to make identification of DoD personnel difficult, to make determination of the prominence or importance of individuals by direct observation difficult, and to reduce the vulnerability of DoD personnel to successful attack while they are in a vehicle between two secure facilities, between a security facility and their homes, or between a secure facility and a secure transfer point for a change in travel mode.

c. Appendix L contains several tips on reducing terrorist risk while operating a vehicle.

8. Precautions While Flying

In most instances, the safest, most reliable, and least risky mode of transportation from the perspective of terrorist attack is by air. U.S. TRANSCOM and Military Airlift Command flights are the most secure means of flying between two points. DoD charted aircraft flights are also unlikely targets for highjacking or assaults on passengers. Appendix K offers several tips for "defensive flying."

9. Rail Travel

a. Travel by rail is the least secure means of commercial travel possible. Rail schedules and routes are highly regular and predictable; they afford terrorists multiple opportunities to board and leave the train without arousing suspicion. Rail travel is strongly discouraged in high risk areas or high physical threat and/or potential physical threat countries.

b. If rail travel is necessary, the general precautions outlined above for air travel are equally appropriate. In addition, the following measures should be implemented:

(1) Avoid travel through high-risk areas; leave the train and switch to foreign flag airlines if to avoid such areas.

(2) Select a window seat in the middle section of open coach (U.S. style) rail cars; select a compartment towards the middle of a rail car in multi-compartment European rail cars; avoid taking seats near passageways between two rail cars if at all possible.

10. Travel at Sea

a. Although DoD personnel and their dependents do not frequently use ferries, transoceanic passenger liners, or cruise ships for official travel, there are many international waterways for which these modes of travel are appropriate for recreational travel. Unfortunately, there have been several instances of either terrorist attack or criminal assault on international passenger travel. The purpose of personal security precautions at sea remains unchanged:

(1) Frustrate intelligence collection and targeting.

(2) Camouflage affiliation and importance.

(3) Reduce likelihood of being attacked.

(4) Mitigate the effects of an attack should it occur.

b. In addition to the travel precautions appropriate for flying outlined above, some additional precautions should be considered:

(1) Select ferry lines, cruise lines, or transoceanic passenger lines noted for good safety and public health records.

(2) Avoid travel through high-risk areas; avoid sailing on vessels which made port calls in high-risk areas.

11. Hotel Procedures

a. It becomes readily apparent that security precautions taken by DoD personnel and their dependents at home have direct counterparts when staying in hotels, motels, or guest quarters on U.S. military installations. The approach taken, from site selection, to installation of additional physical security precautions, to family "operations security" measures are quite similar.

b. As in the case of other travel-oriented antiterrorism measures, the goals remain as outlined in Figure 12-1.

c. The list of measures that follows is long, but by no means exhaustive. DoD travelers should use their own imagination and develop additional measures that address the goals of antiterrorism measures spelled out above.

(1) Stay at DoD facilities while on TDY/TAD whenever possible.

(2) Avoid staying in hotels with distinctively American names or predominantly American guests.

(3) Make reservations in two or more hotels and use an assumed or modified name.

(4) AVOID TAKING STREET-LEVEL ROOMS, TERRACE LEVEL ROOMS WITH DIRECT ACCESS TO HOTEL GROUNDS, OR STAIRWELLS.

When checking into guest quarters and hotels, avoid taking a street-level room if at all possible. Similarly, seek out alternatives to terrace, veranda, or other rooms that open directly on to areas that can be easily accessed from other rooms, common areas of the hotel, the street, or walkways along seawalls, beaches, lakes, etc. Use elevators in buildings rather than risk attack in stairwells. Stand near the elevator control panel; if threatened, push the alarm button.

(5) Retain control over all luggage upon arrival in a hotel lobby.

Upon arrival at a hotel, the family should move all their luggage inside promptly. In some countries, it may be customary for bellboys to carry their guests' luggage from the car and deliver it later to their room. However, it is again recommended that the family never let the luggage out of their sight. This will ensure that no explosive device has been added to a bag and timed to detonate later in the family's room.

(6) When in a hotel, note all escape routes.

Shortly after arriving in a strange hotel or other public place, try to find out the locations of fire escapes, emergency exits, fire alarms and fire extinguishers that you may need in an emergency.

(7) Vary your pattern of entering and leaving your hotel.

Alternate entrances and exists to the building should be used if they are available to avoid setting an identifiable pattern of coming and going.

(8) Do not discuss travel plans over hotel phones.

(9) Use extra caution in hotel lobbies and other public places where bombs may be placed.

Public lavatories have been favorite sites for terrorists to hide bombs in the past. Use of public rest rooms should be avoided to the maximum extent possible. Discovery of objects such as shopping bags, briefcases, boxes and items wrapped in newspaper which have been left unattended or which look out of place, should be reported to someone in authority. Exposed wires or noise, such as a hum or ticking should also cause an object to be considered suspect. DO NOT TOUCH SUSPECT OBJECTS. Notify authorities.

(10) Bellboys and other strangers in hotel lobbies should not be asked directions for specific places you intend to go.

Preserve anonymity and camouflage the nature of your business travel. Ask directions from local police or from U.S. military personnel, if possible, not hotel staff or other guests.

(11) Do not conduct official business nor meet casual acquaintances in your temporary living quarters; do not divulge the location of your quarters.

(12) Discourage efforts to enter your room while you are gone by preserving a "lived in" look in your room.

Leave a light and radio or television on in your room when you go out. This will give the appearance that the room is occupied. A light will also make it easier for you to see what or who is in the room when you return. Keep your hotel room key with you at all times as well. This, too, will make it more difficult to determine when the room is occupied and when the room is vacant.

(13) Keep your room neat.

Neatness will make it hard for things to be placed in your room without your knowledge. Luggage, briefcases and packages that appear to have been moved or otherwise disturbed should be treated with caution. A light dusting of talcum powder can be spread on the surface of suitcases, a dresser, or a desk just before you leave the room. A package that appears to have been opened and resealed should not be touched. Report such things promptly to military or civilian police.

(14) Hallways should be checked before exiting from an elevator or your room, for out of place objects or for persons who seem to be loitering.

The management should be asked to remove any boxes, trash cans or other receptacles near your room which may be used to hide a bomb, or which might get in your way in case of a fire or other emergency evacuation.

(15) PACKAGES SHOULD NOT BE DELIVERED TO YOUR ROOM.

Purchases should be picked up in person and wrapped in your presence. Suspicious deliveries to your room should be refused and the article removed from the building until it can be checked out. Doors should not be opened for strangers or to accept an unexpected delivery.

(16) Unexpected mail left for you at the desk or slipped under the door of your room should be viewed with suspicion.

(a) Mail, packages, or other articles with any of the characteristics listed in Figure 12-2 should be treated as potential improvised explosive devices.

(b) Suspect letters or packages should be isolated. They should not be put in water, because this could weaken wrappings, allowing mechanical devices to operate (or otherwise cause detonation) if the letter or package is in fact a bomb. DO NOT OPEN OR TAMPER WITH THE SUSPECT ITEM IN ANY WAY. Notify military or civilian authorities and follow their advice.

- Excessive postage or no postage.
- No return address.
- Incorrect title or titles without name.
- Hand printed or poorly typed address.
- Postage cancellation stamp does not match location of return address.
- Rigid envelope.
- Excessive securing materials, such as tape or string.
- Lopsided or uneven envelope.
- Oily stains or discolorations.
- Protruding wires or tinfoil.
- Misspelled words.
- Presence of peculiar odor of shoe polish, almonds or marzipan.
- Restricting markings, such as "Personal," "Confidential," and so forth.

Figure 12-2. Indications of Package or Letter Bomb

F. SUMMARY

1. The Department of Defense acknowledges its responsibility to protect its own assets and resources from terrorist attack. Toward that end, the Department of Defense has expended substantial resources to improve physical security at Department of Defense and other U.S. Government facilities around the world. It has developed extensive residential and mobile training courses. It has incorporated blocks of instruction in accession training and general military training carried out by the Military Services. The Department of Defense has expanded professional military training opportunities that address personal security issues.

2. Ultimately, however, responsibility for personal protection is in the hands of each and every member of the Department of Defense, whether they are in uniform or in the civil service. Toward that end, readers are reminded that the goals of personal protection measures are as follows:

a. Frustrate efforts by terrorists to collect information necessary and sufficient to identify American personnel as Americans, to determine their position, their prominence, and their importance, and translate such information into effective, executable targeting plans;

b. Camouflage the importance of DoD personnel, thereby reducing the value to terrorists of targeting individuals who can be identified as Americans;

c. Reduce the accessibility and vulnerability of DoD personnel and their dependents whose prominence or mission criticality have been correctly identified and evaluated by terrorists, and who have been targeted for attack if only the right opportunities are presented; and finally,

d. Mitigate the effects of terrorist attacks on DoD personnel in the event that they do occur, by minimizing the number of personnel involved, minimizing the extent of casualties as a result of the incident, and minimizing the long-term effects of terrorist actions on the survivors should such attacks be successful in taking hostages.

3. The measures outlined above are reasonable approaches to be followed in general cases. Rote application of these measures without careful attention to local circumstances, changes in the national and international security climate, and continuing assessments of terrorist threat, risk of terrorist attack, vulnerability to attack, and mission criticality of DoD assets may leave DoD personnel and their dependents no better off than if no antiterrorism measures were applied.

4. Implementation of effective antiterrorism measures for the protection of DoD personnel and their dependents must be part of a comprehensive program of force protection, interwoven with physical security measures, crime prevention, crisis management planning, and wartime mobilization training.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 13

EXECUTIVE PROTECTION

A. INTRODUCTION

1. DoD Directive 0-2000.12 (reference (a)) recognizes a need to provide protection to those military officers and DoD civilians who are assigned to **high-risk billets**, who are by the nature of their work, **high-risk personnel**, or who are assigned to facilities identified as **high-risk targets**. The Directive defines these terms as follows:

a. High-Risk Billet. Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

b. High-Risk Personnel. U.S. personnel and their family members whose grade, assignment, travel itinerary, or symbolic value may make them an especially attractive or accessible terrorist target.

c. High-Risk Target. U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target.

2. The following material is intended to supplement information provided in the preceding chapters. Readers are encouraged to examine Chapter 14, Hostage Survival, as well. For purposes of this chapter the term "executive" will be applied to all persons requiring additional security protection who are:

a. Assigned to High-Risks Billets;

b. Designated as High-Risk Personnel; or

c. Identified as High-Risk Targets persons who are assigned to High-Risk Billets or designated High-Risk Personnel.

3. The specific supplemental security measures that may be furnished to executives is subject to a wide range of legal and policy constraints. U.S. law establishes stringent requirements that must be met before certain security measures may be implemented. DoD Component regulations, instructions, and legal opinions may further constrain implementation of some protective measures described in this chapter. SOFAs and MOUs between the U.S. Government and a foreign government will also limit use of some supplemental security measures. Leases and other conditions imposed by contract for purchase of land or buildings by the U.S. Government for use by the Department of Defense may also limit application of certain security techniques. All of these constraints

should be carefully considered when conducting security surveys, developing plans, and implementing additional security measures to protect high risk personnel.

B. EXECUTIVE PROTECTION GOALS

1. In the discussion that follows, several measures are outlined that can afford senior military officers and DoD personnel additional protection against terrorist acts. The purpose underlying these measures is to:

a. Increase the interval of time between detection of a threat and the onset of hostile action against executives and their dependents, or

b. Increase the amount of time required by terrorists to gain physical access to executives from the onset of hostile actions whether executives are at home, at the office, or in transit.

2. Implementation of supplemental security measures should strive to achieve the following prioritized goals:

a. Enhancements should hold the terrorist threat at bay until a response force arrives (Delay at a Distance).

b. Enhancements in physical security should enable executives to flee to safety (Delay to Permit Flight).

c. Enhancements should permit the executive to retreat into a safehaven of sufficient strength and survivability such that a response force can wage an effective counterattack to liberate executives and others accompanying them to a safehaven, including dependents at home and colleagues and visitors at work (Delay, Hold, and Counterattack).

3. All measures discussed below should be applied with care. THERE IS A TRADE-OFF BETWEEN INCREASING THE LEVEL OF PHYSICAL SECURITY AT THE OFFICE AND AT HOME AND PRESERVING THE ANONYMITY OF EXECUTIVES, thereby avoiding telltale signs of activity that point to prominence or criticality.

4. Supplemental physical security measures described below can be expensive. Expense can be measured not just in terms of dollars, but also in terms of changes to organizational routine. Therefore, two questions must be resolved before implementing bold, disruptive, and expensive supplemental security enhancements:

a. What are the most cost-effective means of enhancing the security of executives at risk? How many changes in organizational routines and personal behaviors will have to be made in order for security measures to be effective in reducing risk of terrorist attack and the vulnerability of executives to such attacks?

b. What are the anticipated costs of additional security measures in terms of dollars, organizational functionality, and mission capability?

5. Security enhancements can be made to improve the security of executives. But security enhancements can be even more effective if executives and their families take full advantage of and reinforce the security measures described in Sections C, D, and E, below.

If executives do not change their behavior to accommodate additional security and protective measures, then the behaviors can effectively defeat the purpose of additional protection.

6. The second issue is cost. Additional increments of security can be obtained sufficient to defeat virtually any threat. However, there is a point at which it is simply no longer economical to add layer upon layer of protective measures to defeat a threat that is either more potent than available protective means or can be evaded by adopting an alternative security posture.

C. SUPPLEMENTAL PHYSICAL SECURITY MEASURES

1. Office

The office environment should, in principle, afford executives the greatest degree of physical security. The office environment usually places executives in facilities where attackers must pass by guards, security check points, office workers, aides, and/or secretaries before reaching them. [redacted]

a. Physical Security Survey

(1) A thorough physical security survey should be undertaken. Offices of Defense components attached to U.S. Embassies abroad should have such surveys performed by the DoS. Other DoD facilities should have such facilities performed by the cognizant physical security and facilities engineering staffs. Appendix C contains physical security survey materials that can be used to verify assessments of physical security generated by use of other survey instruments.

(2) The best way to approach a physical security site survey is to think like an intruder. Consider how approaches to the installation or facility could be made; how access to the building housing executive offices could be gained, and how attacks on offices or other frequently used facilities could be mounted.

b. Technical Threat Assessment

(1) The next step in evaluating the need for supplemental physical security measures is a thorough and detailed assessment of the weapons and tactics terrorists might use to attack the structure in which DoD executives work. Security engineers and architects need technical threat data or assessments containing the following information:

(a) Mode of attack.

1 Standoff weapons (mortar, rocket grenade, man-portable anti-tank and/or antiaircraft weapon, sniper rifle).

2 Close combat (sub-machine gun, pistol, knife, garotte).

3 Contact weapons (bombs, incendiary devices, mines).

4 With or without perimeter penetration aids such as power tools, handtools, or explosives.

(b) Time of attack.

(c) Attacking force size.

(d) Anticipated degree of outside support or autonomy.

(2) Such assessments are used to develop engineering design requirements. The data are used to:

(a) Calculate forces to be withstood by bearing structures in buildings;

(b) Identify appropriate security window glazing materials and calculate the thickness necessary to achieve desired penetration resistance times for anticipated threats;

(c) Calculate the total amount of delay time that must be achieved through use of camouflage, deception, barriers, and semi-active security devices to permit response forces to reach the scene of a terrorist attack in time to thwart the attack, capture or eliminate the terrorists, and rescue executives and their staffs or dependents.

c. Technical Assessment of Responses

(1) Having established a basic design threat, engineers need data on the anticipated performance of response forces to be arrayed against the design threat and the expected or desired behavior of the protected executive(s). Some specific information needed includes but is not necessarily limited to the following:

(a) Response force.

1 Size.

2 Capability.

3 Supporting weapons.

4 Response time.

5 Estimated effectiveness against range of attacks.

(b) Desired options for executive protection.

1 Evacuate on warning.

2 Evacuate on detection.

3 Evacuate only if attacked.

4 Evacuate only if forced to capitulate.

5 Do not evacuate.

(2) Security planners need to know the duration of an attack the structure housing executives must withstand before help arrives. Matching threat capabilities on the one hand and anticipated operations by response forces on the other, establishes significant

physical security system performance parameters. These can be quantified and used to develop detailed plans, drawings, and physical security equipment acquisition plans.

d. Physical Security Enhancement Measures

(1) Several physical security measures intended to provide additional protection for executives can be considered based on the requirements defined through detailed analyses outlined above. The primary purpose of such measures should be to increase time required by persons outside an installation to reach the executives housed at an installation. A secondary purpose of such measures should be to reduce or eliminate hazards to executives that might result from violence in the vicinity. Examples of physical security measures to be considered follow:

(a) Increase Threat Detection Time by Installing Sensors on Perimeters and Barriers

1 PROLIFERATE SURVEILLANCE SYSTEMS including seismic, acoustic, and infrared sensors at or beyond the outer perimeter; supplement with closed circuit TV/imaging IR systems tied into the alert response force staging area.

2 EXTEND RESTRICTED AREAS OR EXCLUSION ZONES and relocate access control points from the executive office area to a point closer to the boundary of the installation;

3 Enlarge, proliferate, and extend intrusion detection sensors from the within the installation or facility perimeter to the installation perimeter, allowing IDS to collection additional data necessary and sufficient to classify and identify an intrusion before response force arrives at scene or track of the intruder;

4 PROLIFERATE BOTH THE NUMBER AND THE PHENOMENOLOGY OF SURVEILLANCE AND DETECTION SYSTEMS within the executive office area as well as approaches leading to and from it in conjunction with measures listed below.

(b) Increase Threat Delay Time Between Perimeter and Executive Office Building

1 Install vehicle barriers and realign roadways to eliminate straight, level stretches of road in excess of 50 meters in length;

2 Proliferate concentric rings of fences, Jersey barricades, planters, bollards, and vehicle and/or personnel barriers;

3 Proliferate access control areas supplemented by fire doors and/or security doors kept in a closed condition between the entrance to the building housing executive offices and the executive office area itself.

(c) Confuse, Camouflage, and Deceive Observers by Hiding Executives' Locations

1 Consider relocating executives to buildings not usually associated with office activities, e.g., barracks, motor pool, R&D facilities.

2 Consider constructing office areas in barrack, motor pool, R&D facilities, etc.

3 Add executive style, decorative lighting and window treatments to several different areas of office buildings to MINIMIZE DIFFERENCES IN EXTERNAL APPEARANCES BETWEEN EXECUTIVE AND NON-EXECUTIVE OFFICES.

(d) Increase Delay Time Between the Entrance to the Building Housing Executives and the Executive Office Area

1 Add fire doors, access control points, dead-end corridors, and mid-corridor physical barriers to complicate access to executive office areas.

2 Consider the addition of security devices which when activated disrupt the ability of intruders to retain their thought processes such as flashing strobe lights, fog generators, noise generators, sirens, fire extinguishing systems, etc.

(e) Increase Delay Time and/or Make Access More Difficult Within the Executive Office Structure

1 Substitute high security doors and door frames for standard doors in areas leading to or from executives offices.

2 Install high security grating, wire mesh, or other materials to bar access to executives office area through utility tunnels or conduits.

3 Strengthen walls, floors, and ceilings against improvised explosive devices, small arms fire, incendiary devices, and powered hand tools by substituting steel plate, concrete filled, steel reinforced cinder blocks, or other ballistic resistant materials for plaster and/or lath or wallboard room dividers.

4 Add steel plates or other ballistic materials in crawl spaces above dropped ceilings; extend walls separating executive office area from other portions of an office building from floor to floor, thereby preventing unobserved and undetected access to space of dropped ceilings.

(f) Increase Protection for Building Occupants Against Ballistic Threats Against Windows and Exterior Walls

1 SUBSTITUTE POLYCARBONATE PANELS FOR GLASS WINDOWS;

[redacted]

2 Add exterior screens and/or plates to cover window areas and protect against gunfire and grenade and/or bomb fragments.

3 Properly install blast curtains, metal blinds, metal shutters or other window treatments in executives offices to protect interior space from glass shards and other small projectiles.

(g) Increase Hold Time to Contain Penetrators

1 Add positive action controls to facility and doors and gates such that gates default to a closed and locked condition unless manually released.

2 Add positive action controls to access control areas such that persons inside an access control area can neither advance nor withdraw without affirmative action by a security officer posted outside the access control area.

a The purpose of these measures is to facilitate apprehension of terrorists.

b There may be some instances, however, when the security of the executive and the response force is enhanced by defeating terrorist attempts to gain access to the executive and then channeling the terrorists out of the facility and installation along one route, leaving alternative routes available to evacuate the executive and other key personnel.

(h) Install Emergency Executive Support Facilities Including a Safehaven and an Emergency Evacuation Facility

1 Consider installation of helicopter landing aids on the roof of a structure or on an adjacent field far removed from parking areas.

2 [redacted]

2. Supplemental Residential Security Measures

a. Site Selection

(1) As noted in Chapter 11 on residential physical security measures, site selection is an important aspect of physical security.

(a) Avoid selecting residences previously used by other senior U.S. Government or foreign government officials.

(b) Avoid selecting residences previously attacked by terrorist groups.

(2) While terrorist groups conduct intelligence operations to identify targets, mistakes have been made in the past. DoD personnel should avoid leasing residences previously used by representatives of governments or organizations known to be targets of various terrorist groups. DoD personnel leasing residences formerly used by representatives of such governments may be placing themselves unnecessarily at risk of being attacked as a result of mistaken identity.

b. Supplemental Physical Security Measures

(1) An executive's entire lifestyle should be included in security surveys used to assess the need for supplemental physical security measures at the office. The executive's home and transportation from home to office and back should also be examined for risk and vulnerability.

(2) The same principles used to identify supplemental security improvements in an office environment apply to executives' home environments as well. Recall that the purposes of physical security enhancements are:

(a) Increase the amount of time terrorists need to initiate and complete an attack on executives' while at home, thereby giving response forces more time to rescue executives and their dependents.

(b) Reduce potential harm that could result to executives and their families as a consequence of a terrorist assault mounted against the residence.

(3) As in the case of providing physical security enhancements to an office, the goals of enhanced residential physical security measures remain the following:

(a) Increase the amount of time between detection of a threat and the onset of hostile actions.

(b) Delay the terrorists as long as possible; prevent their access to the executives and their dependents on the one hand, and make departure from the scene to escape prosecution difficult; provided that in so doing, the lives of executives and their dependents are not further jeopardized.

(c) [redacted]

(4) The following are measures that can be implemented selectively, which may help security personnel achieve these objectives:

(a) Increase Time Interval Between Detection of a Threat and the Onset of Hostile Terrorist Acts

1 Ensure all door locks and/or window clasps are working.

2 Ensure that all doors and windows are properly secured to their frames and the frames are properly anchored to the residential structure.

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

4 Consider installing a through-door viewing device or visitor intercom.

5 Consider installing security lights to aid in viewing entrances.

(b) Increase the Number of Physical Barriers Between the Outer Perimeter of the Residence and the Interior of the Residence

Senior officers and DoD officials deemed to be at high risk or occupying high-risk billets may with to consider the following physical security measures for their homes:

1 Add heavy, remotely operated gates to all fences, walls, and perimeter barriers, consistent with the penetration resistance of the barrier, between the residence, the street, and adjacent neighbors.

2 [redacted]

3 [redacted]

(c) Increase Time Required to Penetrate Exterior Structural Walls by Explosives, Hand-Held Power Tools, and Hand Tools

1 Consider the addition of additional armor covered by aesthetically pleasing materials to exterior walls.

2 Consider the addition of a separate reinforced masonry wall around the residence.

(d) Increase Surveillance of Residence and Decrease Response Time

1 Consider installing closed circuit TV systems to permit remote viewing of all doors and windows accessible from the ground, nearby structures, trees, or easily acquired platforms (e.g., van parked next to a wall).

2 Consider installing area intrusion detection systems between the residence perimeter and the residence itself; proliferate number and types of sensors; add backup communication channels between the intrusion detection system and a surveillance assessment and/or response dispatch center.

(e) Increase the Durability and Survivability of the Residence to Terrorist Attack

1 Consider fitting windows with either Venetian blinds or thick curtains to reduce the observability of activities within the residence and to reduce hazards of flying glass in the event of nearby explosions or gunfire.

2 INSTALL BACKUP POWER SYSTEMS FOR SECURITY DEVICES, e.g., surveillance systems, communication systems, and access control systems.

3 Have backup communication with the installation or embassy security department via secure landline or two-way radio.

4 Consider the fitting of a panic alarm bell to the outside of the house with switches upstairs and down. Such an alarm should also annunciate at the local police and cognizant DoD or DoS security office.

[redacted]

c. Transportation

High-Risk Personnel are most often at their peak accessibility to terrorists when they are in transit in official or privately owned vehicles. In this section, some specific steps that can be taken to reduce the vulnerability of executives in transit are discussed. Implementation of measures to enhance the security of DoD personnel at high risk must be undertaken in full compliance with U.S. laws and DoD Directives.

(1) Domicile to Duty Transportation Policy

(a) As a general rule, Congress has strongly opposed provision of home to office (domicile to duty) transportation by the Federal Government to its officers and employees. [redacted]

(b) Congress did, however, grant authority to the President and the heads of executive agencies and departments to provide domicile to duty transportation under certain circumstances. [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

---

1 See Section 1344 of 31 U.S.C. Annotated (reference (ee)).

2 See U.S. Congress, House Committee on Government Operations, House Report 99-451 on H.R. 3614, To Restrict the Use of Government Vehicles for Transportation of Officers and Employees of the Federal Government (Washington, D.C.: U.S. Government Printing Office, December 19, 1985), p. 8.

3 *Ibid.*, p. 9.

[redacted]

(2) Statutory Authorities and Limitations

(a) [redacted]

(b) The Secretary of Defense and the Service Secretaries also have statutory authority to provide transportation from home to duty stations and back on a limited basis. Such authority is usually implemented by providing to protected persons, a nontactical armored vehicle as described below.

(3) DoD Policy

(a) It is DoD policy to make nontactical armored vehicles available where necessary to enhance the security of DoD personnel, consistent with the requirements and limitations found in statute. DoD issuances, Service regulations, and CINC guidance stipulate detailed procedures by which the Department of Defense manages nontactical armored vehicle programs.

(b) Statute also establishes a procedure for Presidential waiver of the "buy American" requirement; DoD and Service Regulations provide for delegation of Presidential Authority from the President, to the Secretary of Defense, to the Director, Defense Security Assistance Agency and the Director, Defense Intelligence Agency.

(c) [redacted]

(4) Non-Tactical Armored Vehicles

(a) The Department of Defense recognizes two classes of nontactical armored vehicles (armored limousines or sedans).

---

4 *Ibid.*, p. 9, emphasis added.

5 See Section 2637 of 10 U.S.C. Annotated (reference (ff)).

1 Heavy nontactical armored vehicles are fully armored vehicles intended to protect occupants from attack by bombs, improvised explosive devices, grenades, and high velocity small arms projectiles.

2 Light nontactical armored vehicles are less than fully armored vehicles intended to protect occupants from attack by medium velocity small arms projectiles and at least some types of improvised explosive devices.

(b) The dividing lines between heavy and light nontactical armored vehicles have become less distinct over time as armoring techniques and materials have given greater capability to vehicles that are not classified as heavy nontactical armored vehicles. As a practical matter, add-on vehicle armoring kits are now in production that when properly installed in an appropriately powered and suspended vehicle provide a level of protection approaching that of the heavy nontactical armored vehicles. For purposes of discussion that follows, the distinction will be made between heavy and other nontactical armored vehicles.[6]

(5) Heavy Non-Tactical Armored Vehicles

(a) [redacted]

1 [redacted]

2 [redacted]

(c) Each of the Services manages a portion of the DoD Non-Tactical Heavy Armored Vehicle Program. Each Service has issued supplementary mandatory guidance on processing of requests for, as well as allocation and use of these scarce assets.

(d) Heavy nontactical armored vehicles are complex systems requiring specialized maintenance and operation. As a general rule, heavy nontactical armored vehicles will be assigned to DoD personnel with a driver who has been properly trained in the operation and maintenance of the vehicle. The operator is not a chauffeur; he or she is an integral part of a supplemental security package provided by the Department of Defense to meet its obligations to protect its key assets.

---

6 This is also the distinction used in DoD Instruction 5210.84 (reference (dd)).

(6) Light Non-Tactical Armored Vehicles

(a) [redacted] while a less complex armoring system than those used in [redacted] afford substantial protection to occupants against a wide variety of threats. New developments in after-manufacture armoring kits for vehicles is occurring at a rapid pace, increasing the number of vehicle manufacturers and models for which "other NTAV" modifications are suitable.

(b) [redacted]

(7) Privately Owned Vehicles

(a) High-Risk Personnel may wish to consider foregoing use of privately owned vehicles completely during periods of extreme risk. If this is not practical, then it may be appropriate to consider some of the measures identified in Appendix J.

(b) In general,

1 Select measures which deter surreptitious entry, making undetected placement of IEDs in or under the vehicle difficult for terrorists to accomplish.

2 Select measures which enhance the ability of the vehicle to increase distance between the vehicle and pursuers.

3 Select measures which can assist response forces come to your assistance in the event of an incident.

4 Select measures which when implemented make the vehicle appear little different than its standard models.

D. SUPPLEMENTAL INDIVIDUAL PROTECTIVE MEASURES

The procedures outlined below should be employed in conjunction with generally applicable personnel security procedures discussed above in Chapter 12 and in conjunction with physical security equipment described in Chapters 10 and 11 and in the preceding section of this chapter. The purpose of adopting these procedures is threefold: increase the time that elapses between the detection of an imminent terrorist attack and the actual onset of an attack to permit the arrival of response forces or the successful evacuation of executives; increase the amount of time to withstand an attack and terrorist access to executives to permit the arrival of response forces or the successful evacuation of executives under attack; [redacted]

1. Office Security Practices and Procedures

Refer to and implement measures discussed in Chapter 12. In addition, implement the following additional measures as appropriate:

a. Discourage staff from disclosing executives' whereabouts or activities when taking telephone messages.

b. Observe caution when opening mail. In particular, be on the lookout for letters or packages that might contain improvised explosive devices. A checklist to aid in letter bomb or packaged IEDs appears in Appendix Q.

c. Limit access to the executive office area strictly.

d. LIMIT PUBLICITY ABOUT THE EXECUTIVE TO A BARE MINIMUM; keep official biographies short; provide minimal information that would reveal executives personal interests and hobbies, and consider using outdated photographs if a publicity photograph is absolutely essential.

e. Avoid working alone late at night and on days when the remainder of the staff is absent.

f. If late night work is necessary, work in conference rooms or internal offices where observation from the outside of the building is not possible. Notify security officers that you will be working late and ask that they look in periodically. Executives should enter and exit several offices, turning lights on and off before going to their own offices to disguise the purpose of their activities to outside observers.

g. Avoid placing of office furnishings directly in front of exterior windows.

2. Official Business Away From The Office

The following suggestions reinforce efforts by executives to maintain the high level of security provided in the home or office environment while on official business outside these locations.

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 a darkened exterior.

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

3. Local Official and Unofficial Travel

a. General Practices

(1) Vary your daily pattern as much as possible. Leave and return at different times.

(2) Consider escorts to and from work, or travel with a neighbor.

(3) Establish a simple duress procedure between executives and drivers. Any oral or visual signal will suffice (i.e., something that the executive or driver says or does only if something is amiss).

(4) When using a taxi service, vary the company. Ensure that the identification photo on the license matches the driver. If uneasy for any reason, simply take another taxi.

(5) When attending social functions, go with others, if possible.

(6) 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).

(7) Do not leave personal items exposed in the car; e.g., uniform items, service issued maps, official briefcases, etc.

(8) Use the same precautions when you drive a privately owned vehicle (POV).

b. Security Practices While Driving

(1) Keep car doors locked. Do not open windows more than a few inches.

(2) Never overload a vehicle, and all persons should wear seat belts.

(3) Always park vehicles in parking areas that are either locked or watched and never park overnight on the street. Before entering vehicles, check for signs of tampering.

(4) Keep the trunk locked.

(5) Where feasible, drive in the inner lanes to keep from being forced to the curb.

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

(7) Avoid driving close behind other vehicles, especially service trucks, and be aware of activities and road conditions two to three blocks ahead.

(8) Beware of minor accidents that could block traffic in suspect areas; especially crossroads because they are preferred areas for terrorist or criminal activities as crossroads offer escape advantages.

(9) Actions to take if attacked:

[redacted]

4. Interurban, National, and International Travel Security Practices and Procedures

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 as to your itinerary and subsequent changes. However, clearly and emphatically restrict this information to those having a need to know.

5. Home Security Practices and Procedures

a. 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.

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

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

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

e. Investigate household staff (especially temporary staff).

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

g. Note and report suspicious persons.

h. Strictly control house keys.

i. Place car in a locked garage.

j. Be alert for the unusual; e.g., the movement of furniture or the placing of unusual wires.

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

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

m. Test your duress alarm if available. Make certain the members of your family understand how they work as well as the importance of their use.

n. Cooperate with law enforcement personnel and abide by their security recommendations concerning your home's security.

6. Security at Social and Recreational Activities

The risk of terrorist incidents is always present for high-risk personnel or personnel assigned to high-risk billets. Life must go on nevertheless. The following measures are intended to permit executives to continue living as close to a normal life as possible while still remaining mindful of the risks to their security.

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, etc.

E. COMBATTING TERRORISM TRAINING FOR EXECUTIVES

1. High-Risk Billets and/or High-Risk Personnel

a. [redacted]

2. Travelers to High and/or Potential Physical Threat Risk Areas

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. [redacted] During this one-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 combatting terrorism measures (vehicle, personal, airline, and physical security), and hostage survival.

b. [redacted] These are one-week courses offering personnel instruction in cultural, political and/or 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, NC.

F. PROTECTIVE SECURITY DETAILS

1. General Discussion

a. Each Service can provide protective service teams for key senior military officers, DoD civilians, other U.S. Government officials or foreign dignitaries requiring personal protection.

b. Assignment of Protective Security Details (PSDs) to Service members is made by each Service Secretary upon recommendations of their counterintelligence and/or law enforcement investigation staffs. PSDs are assigned to DoD personnel who meet requirements established by Service regulations.

2. General Security Concept

[redacted]

3. Maintenance of Low Profiles

a. Protective Security Details are trained in the art of maintaining low profiles. [redacted]

b. Toward that end, PSDs will strive to keep travel routes and means of transportation to be used by the protected person from being publicized. If this cannot be accomplished, the PSD may suggest editorial changes to the itinerary scheduled for release

to limit details of planned travel from public disclosure. For example, routes to and from announced appointments usually need not be revealed.

4. PSD Mission Duties

a. During the course of a PSD mission, members of the PSD may be asked to perform several different security functions. [redacted]

b. The attitude of the protected person is critical to the success of the PSD mission. Protectees do have a right and a responsibility to make their wishes known with respect to their personal security; they also have an obligation to listen carefully to the head of the PSD who is trained and highly qualified to assist the protectee in making reasonable judgments about manageable risks. PSD members understand their function is inherently intrusive, and that protectees can easily resent the loss of privacy that accompanies the protection offered. On the other hand, PSDs have jobs to do, not merely to protect executives, but to help safeguard mission critical assets--senior military and civilian leaders.

c. One of the most demanding functions placed on PSDs is to limit the ability of individuals to circulate and approach the protectee. [redacted]

d. DoD personnel who are provided PSDs and must conduct official business or hold social engagements in large rooms can take several steps to minimize the disruptions to such functions as may occur as a result of good security practices. [redacted]

e. Protective Services Detail members are highly trained security specialists. While in the company of protectees, they will be accommodating and helpful. [redacted]

G. EXECUTIVE PROTECTION SYSTEM INTEGRATION

1. This chapter has focused on supplemental security measures used to address terrorist threats to senior High-Risk Personnel within the Department of Defense.

2. Various methods and measures have been discussed that provide increments of security over and above the base level of security provided to all DoD personnel assigned to an installation, a facility, an activity, or a unit. In making decisions to allocate protective resources to enhance the security of senior officers and senior DoD officials, it is essential to bear in mind such measures must be applied systematically.

3. Additional security measures implemented to protect high-risk persons in the office environment must be carried over to official functions conducted outside the office. The security measures must also be extended to the protected persons' private lives, and depending upon the nature of the threat, the lives of their dependents as well.

4. The converse is equally true [redacted] in view of the total costs of security measured in dollars, time, inconvenience to protected persons, their staffs, colleagues, and families, it may be prudent to radically alter living and working arrangements than to try to augment security in a piecemeal manner. For example, it might be prudent to house high-risk personnel within a DoD installation rather than to try to secure a detached, private residence at substantial distance from the operations base of a response force.

5. The key to successful executive protection is to ensure the level of protection afforded, by physical security measures, operational procedures in the office and at home, and protective security details, is constant. The level of protection must be matched to the threat, and must be sustainable.

6. Executives have a special responsibility to set a personal example of combatting terrorism awareness, of attention to personal, family, office, information and operations security concerns, and of combatting terrorism security measures implementation. By doing so, they make their colleagues and subordinates more aware, more conscious of their security environment, and less likely to be victimized by terrorist attacks.

CHAPTER 14

HOSTAGE SURVIVAL

A. INTRODUCTION

1. Despite implementation of a DoD-wide combatting terrorism policy and program, DoD personnel may still become kidnap hostage victims. This chapter provides techniques helpful to hostage and kidnap victims in surviving their ordeal with dignity and self respect. Kidnappings and hostage-taking affect family members as well as the victim. This chapter discusses several measures families may wish to implement to help them through their ordeal.

2. All DoD personnel, both military and civilian, have special obligations as representatives of the U.S. Government and as professionals in the field of military affairs and international security, to conduct themselves in captivity in accordance with domestic and international rules, laws, and policies. This chapter concludes with a discussion of DoD policies on behavior during peacetime detention.

B. HOSTAGE SURVIVAL

Several specific measures can be implemented in the event that DoD-affiliated personnel become the victim of a kidnapping or hostage-taking episode. While preventive measures taken may have postponed an incident, eventually it may occur. If so, the question then occurs: now what should be done?

1. Measures to Be Taken During Capture

a. During the initial moment of capture, the victim must make an instant decision—[redacted]

b. [redacted]

c. The specific circumstances of a kidnapping or hostage seizure may dictate the answer to these questions with no additional analysis being required on the part of the

potential victim. [redacted] k. The situation is primed for violence. Therefore, follow these steps:

(1) Resist panic; remain calm; MAKE NO SUDDEN MOVEMENTS.

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

(3) [redacted] assure your captors of your intention to cooperate, especially during the abduction phase.

(4) ANTICIPATE ISOLATION AND TERRORIST EFFORTS TO CONFUSE YOU.

[redacted]

(6) Try to prepare yourself mentally for the situation ahead as much as possible. Stay mentally active.

e. After the initial shock of capture wears off, both the kidnappers and the victims stabilize their emotions and begin to plan for the future. The terrorists may divulge information about themselves, their organization, their goals and objectives. They may share their demands, and they may even begin to discuss roles and responsibilities the victim or victims will have in the future.

f. Those taken hostage also should begin to make an emotional transition from being a "victim" to being a "survivor." The following actions help in this process:

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

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

(3) Carefully consider the requirements for and consequences of escape.

2. Surviving Detention

a. Being held hostage is one of the most stressful and difficult circumstances conceivable. Several factors make this situation especially difficult for many victims.

b. First, there are often few or no relationships between actions of the victims and their hostage status. Unlike prisoners of war who are captured and incarcerated as a consequence of their participation in a war, hostages are almost always innocent victims of

circumstance, at least in their own thinking. Hostages have a difficult time imagining or understanding why anyone would want to kidnap them or hold them hostage.

c. Second, kidnappings and hostage-taking events occur as ugly surprises, totally disrupting plans and activities for an unknown period of time. Surprise is often very stressful; for those individuals who take special pride in making and fulfilling commitments, such events can be emotionally shattering. These individuals are easily rattled when thrown off schedule or when their daily, weekly, or monthly plans are upset. Being kidnapped is the ultimate surprise party--no one knows in advance (except the kidnappers, and even they might not have planned for so many "guests") and no one knows when or how the episode will end. For victims, but especially those who are especially schedule conscious, the stress level can be life-threatening in and by itself.

d. Third, kidnap victims and hostages are usually isolated from all outside contact. While they may have access to radios and televisions, they are never allowed to call their families, friends, or colleagues. Even if seized in large groups, victims are often separated and held individually or in small groups. In some circumstances, separation from the group can compound anxiety and fear, especially if the victims are separated from their children, elderly parents, or spouses.

e. Fourth, and perhaps most important, victims must come to grips with a whole host of intangibles and unknowns. Once the trauma of initial capture has subsided and the victims have adjusted to the total loss of freedom and being placed in a position of complete dependence on their captors, other uncertainties begin to manifest themselves in the victims' behavior and demeanor. Victims wonder who knows of their predicaments, what is being done to bring the episode to a close, who will take care of "things" in their absence, what is going to happen next, and perhaps most importantly, when is this episode going to end?

f. Kidnappers will frequently undertake certain actions to increase the degree to which victims become dependent upon them. Victims can expect to be stripped of wristwatches, calendars, and even eyeglasses. These actions are all part of a concerted plan by terrorists to exacerbate the psychological hazards associated with being kidnapped or taken hostage: claustrophobia, loss of sense of time, and isolation from society.

g. Victims of kidnappings and hostage situations report they were often placed in dark, confined surroundings for prolonged periods. The victim must be able to compensate feelings of depression, adjust to living alone, and offset the demoralizing realization that human contacts they may have for the foreseeable future are likely to be quite hostile.

h. To maintain a sense of order, personal dignity, and personal functionality, the following measures should be implemented by each kidnap victim or hostage:

(1) Try to prepare yourself mentally for the situation ahead as much as possible. Stay mentally active.

It is difficult to avoid speculation on what lies ahead, but victims of kidnapping and long-term hostages seemed to handle periods of captivity by building elaborate plans for their future upon release. Americans held hostage in Lebanon during

the 1980s, for example, taught each other collegiate-level courses from memory, designed plans for a dairy farm to the smallest detail, played chess on a self-made board with self-crafted pieces, and studied one another's religion.

(2) Be a role model.

If the victim remains calm during captivity, it is easier for terrorists also to remain calm. If you treat yourself, your fellow hostages, and your captors with respect, you can often expect similar treatment from your captors.

(3) Be extremely courteous and polite to the terrorists.

Polite and courteous behavior extended towards captors emphasizes the nonbelligerent attitude of victims towards captors. In so doing, such behavior conveys information that reinforces earlier and continuing messages that the victim is not an immediate threat to their welfare or security.

(4) Try to build human relationships.

Identify those captors with whom you can communicate and attempt to establish a relationship with one or more of them. Do not debate or argue, but try to discuss neutral issues.

(5) Talk in a normal voice.

Avoid whispering when talking to other hostages, or raising your voice when talking to a terrorist. Whispering suggests conspiratorial behavior, plots of escapes, and the possibility that victims might turn on captors. Whispering among hostages can be perceived as quite threatening to terrorists and result in further emotional or physical harassment of hostages or worse. Similarly, loud conversations with terrorists can be interpreted as an indication of dangerous, bellicose, and threatening behavior by hostages. Such an interpretation might result in further deterioration of conditions for hostages.

(6) Read anything you can find to keep your mind active.

While the library available to kidnapping victims may be quite limited, reading is still an excellent activity to keep one's mind active while maintaining vigilance, offering no overt acts of opposition, but no overt acts of cooperation with captors either.

(7) Eat whatever food is offered to you to maintain your strength.

Kidnap victims rarely gain weight during their captivity. However, eating enough to maintain body weight and sustain proper functioning of the immune system is important. If kidnap victims lose too much weight by not eating available rations, they can become seriously ill. In so doing, they may develop medical conditions which exceed the medical resources and skill of the kidnappers and their external sources of assistance, if any.

(8) Exercise daily.

Prisoners of war and long-term hostages emphasize the importance of maintaining as fit physical condition as possible. Exercise not only strengthens the physical durability of the victim, it gives added mental strength as well. Exercise and good

physical conditioning also increase resistance to disease which may be a by-product of dietary changes or inadequate food, poor living conditions, and general emotional deprivation associated with victim status.

(9) Establish a slow, methodical routine for every task.

It is important that hostages and kidnap victims develop routine behavior. Such routines are helpful in many ways. First, routine behavior helps to reassure guards that the hostages pose no immediate threat to their welfare. Having survived the trauma of initial capture, hostages and kidnap victims need to avoid provoking their captors into physical violence against them. Second, routine behavior helps to pass time on the one hand, and maintain a sense of time, space, and purpose on the other. Third, routines help ensure the health and safety of victims if their conditions degrade over time.

(10) Obey terrorist orders or commands.

Victims of kidnappings or hostage-taking are often put into very dangerous, onerous, humiliating situations. Under such circumstances, victims should obey terrorist orders or commands. Obedience to orders or commands need not be swift, cheerful, or overtly enthusiastic, but it should be sufficient to maintain a balanced relationship between the hostages and their captors.

(11) Be alert always for signs or signals from outside for rescue efforts.

(a) One of the hallmarks of the DoD Combatting Terrorism Program is the well-trained DoD member or dependent who remains sensitive to his or her security environment at all times. Even in captivity, victims must try to remain alert for changes in the environment, to expect the unexpected.

(b) Listen for unusual sounds that seem out of place or inconsistent with usual activities. Such sounds might include helicopter blades beating in the air, high performance aircraft overhead, diesel engine sounds in the neighboring street. Watch for unexplained changes in guard behavior, unexplained increases or decreases in civilian traffic observable from one's place of detention, or other signs of unusual activity on the part of the terrorists.

(c) There are also some discrete measures victims of kidnappings and hostage-taking should refrain from taking because such measures generally increase the risk of physical violence to the victim without increasing opportunities for escape.

(12) Do not aggravate your abductors.

Terrorists oftentimes have low thresholds for dissent and argument. When aggravated, they can become abusive and violent. [redacted]

Given the emotionally charged atmosphere surrounding a kidnapping or hostage situation, discussions of politics and religion are likely to be even more emotionally charged than normal. Under the stressful conditions of a terrorist kidnapping or hostage situation, find other topics to discuss with the terrorists, at least until some degree of mutual respect has been established. Even then, try to steer conversations away from topics which arouse strong emotions in other victims or the terrorists.

(14) Do not complain, act belligerently, or be uncooperative when dealing with the terrorist or other hostages.

(15) DO NOT LET YOUR BODY LANGUAGE SEND UNINTENDED MESSAGES OF HOSTILITY AND ANTIPATHY TO THE TERRORISTS.

When many people speak, they talk not only with their voices but with their bodies. The way people tilt their heads, move their hands, and hold their bodies are often important cues about emotions and future actions. Placing hands just above each hip and leaning forward while speaking is often interpreted as defiant or aggressive speech, regardless of the words and tone of voice used. Turning away from a speaker is often interpreted as an insult or an act of hostility. Victims must become sensitive not only to what they say, but also how others might hear and view such conversations.

(16) Do not refuse favors offered by the terrorists if doing so will aggravate them or cause further harm to the health and safety of all hostages [redacted]

This includes offers of food, beverage, tobacco, etc. Such gestures may indicate nothing at all; they might indicate an interest in building a relationship which can later be used to win release or bring an end to the episode.

(17) Do not hesitate to answer questions about yourself.

During informal conversations with terrorists and captors, victims can sometimes develop human relationships by conversing with their captors and responding to personal questions that do not require discussion of the victims' positions, responsibilities, purposes of travel, except if your position, post, or purpose of travel poses an additional threat to the terrorists or to their ideologies.

(18) Do not worry about your family.

One of the advantages of being a DoD employee is being part of a large organization with substantial resources on call to provide support to families in crisis. In the event that DoD personnel are involved in a kidnapping or hostage-taking episode, their families are notified and kept informed of the situation. In the event DoD personnel had not completed some of the preparations suggested above with regard to wills, powers of attorney, and other legal matters, DoD personnel and their dependents will be assisted, either by DoD activities, Service activities, or other relief organizations. The Department of Defense does not knowingly abandon families of DoD personnel or dependents caught up in a hostage or kidnapping situation.

3. Conduct During Interrogation

Depending upon the personality of terrorists holding the victims hostage, the purpose of seizing hostages, and the prominence or position of the hostages, the terrorists may elect to interrogate victims. DoD personnel should be guided by the following principles in responding to questions posed during such interrogations:

a. Be prepared to explain all information in your luggage and around your seat at the time of capture.

b. Take a simple position that you feel comfortable with, and stick to it.

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

d. KEEP YOUR TEMPER UNDER CONTROL AND BE POLITE.

e. GIVE SHORT ANSWERS, TALK ABOUT NON-ESSENTIAL THINGS.

f. Do not be lulled by a friendly approach.

g. If required to make a public statement, identify your statement as being made in response to the demands of your captors.

h. Retain a sense of pride and faith in yourself, your government, and your religion.

4. Release

Episodes of kidnapping and hostage-taking do end, and often with no loss of life or physical injury to the victims. The psychological casualties suffered by kidnapping victims are difficult to assess, as are the casualties incurred by victims families, friends, and colleagues. Nevertheless, hostage and kidnapping episodes can end as a result of fatigue on the part of the terrorists, negotiations, or terrorism counteraction. The manner by which an episode comes to an end will have considerable bearing on measures that are most appropriate; since victims cannot predict the outcome of a hostage situation beforehand, the following measures to aid hostages at the end of an episode should be reviewed and implemented as appropriate:

a. Rescue

(1) Do not run, because the terrorists may shoot you. Even if you can, do not pick up a gun to assist rescue forces. You will probably be handcuffed, searched, and possibly gagged and/or blindfolded. As a common procedure for rescue forces, this must be done until everyone is positively identified.

(2) In the event an armed rescue effort is mounted, victims should be alert to their surroundings and be prepared to follow instructions of rescuers. The following specific measures should be implemented at the first indication of a rescue attempt:

(a) DROP TO THE FLOOR AND REMAIN STILL.

During the rescue attempt, both the hostage and the rescue force are in extreme danger. If the facility confining victims is breached by rescue forces, drop to the floor immediately, and lie as flat as possible.

(b) AVOID SUDDEN MOVEMENT OR MOTION.

Rescue forces are trained to assume that terrorists will (a) resist rescue efforts or (b) will attempt to flee in a rescue attempt is undertaken. The trained response of such forces to any movement is to shoot first, ask questions later.

(c) WAIT FOR INSTRUCTIONS.

After order has been restored by rescue forces, there may be some moments when the victims may be handled roughly or ordered up against the wall. Victims may be handcuffed, searched, and even gagged until the rescue forces have positively identified all persons. This procedure is common to special response teams and hostage rescue teams and is employed for their safety as well as the safety of hostages upon release.

b. Voluntary or Negotiated Release and Episode Termination

(1) Many kidnappings and hostage-taking episodes end as the result of successful negotiations between the kidnappers and law enforcement authorities or because the kidnappers and/or hostage-takers exhaust their sources of supply and wish to terminate the episode without additional risk of injury to themselves or anyone else. While these endings to hostage situations are less dramatic than those brought to conclusion as a result of forcible rescues, the termination of the episode has much the same effect on hostages and kidnap victims.

(2) The following discussion applies to all victims, regardless of the manner by which the episode was brought to an end.

(a) Be prepared to face the media.

Terrorist events have become media events, even if the terrorists and the families of kidnapping or hostage situations would prefer otherwise. As survivors of difficult ordeals, the victims will be encouraged to speak out on their experiences. Just as the terrorists stripped away virtually all privacy and dignity during the victims' captivity, so too will some members of the press seek out answers to the most demeaning, humiliating, or private questions conceivable. Many victims want to share their stories, but are shocked, angered, and humiliated by their treatment at the hands of the press. Therefore, victims need to recognize that press interviews can be very difficult; many survivors of terrorist incidents return to normal life more easily by minimizing their interaction with the press. Many are simply ill-prepared for interviews.

[redacted]

2 [redacted]

3 A good general response to all press inquiries is to note the simple joys of freedom and that given a choice between being free and being a hostage, being free is far superior.

(c) Understand that feelings of guilt and a closeness to your captors are normal psychological results of a hostage experience. (See Appendix U.)

1 The reentry of a terrorist incident survivor is a difficult experience. Several problems must be overcome. First, former hostages must reacquaint themselves with the world in general and their little piece of the world in particular. It does not matter how long hostages may have been held, the fact that they were in circumstances on which they were totally dependent on the largess of others has a profound impact. Virtually everything changes for hostages upon their release, and it takes some time for them to adjust to the world.

2 Hostages also experience a wide range of emotions, exaggerated in all dimensions if the survivors were part of a larger contingent in which there were some casualties and deaths. Survivors typically must confront several questions:

Why me? Why did I become a victim and not some other person?

3 Where casualties or deaths occurred and the survivor was not killed or severely injured, the question is often inverted.

Why not me? Why was I allowed to live while others were chosen to die?

4 Often there is anger directed at the U.S. Government or the Department of Defense.

Why did you allow this to happen to me? Why did you not rescue me sooner? Why did you let me suffer?

5 These are difficult questions to answer, and survivors and their families may benefit from psychological support and social services in the aftermath of surviving a terrorist incident. Chaplain, medical and law enforcement victim assistance offices located on DoD installations can provide assistance to DoD personnel and their dependents; the U.S. Embassy staff can also provide assistance to DoD personnel and their dependents assigned to embassies.

C. THE ROLE OF THE FAMILY

DoD personnel can help their families deal with the trauma of kidnapping and hostage-taking by preparing them for what might happen. Such preparations include

implementation of the security measures noted in earlier chapters as well as the formulation of specific family security contingency plans.

1. Family Contingency Plans

a. Every family should develop its own system of communicating duress.

Notes from parents to children should include a code phrase, word, or set of alphanumeric characters that can be understood by the children as authenticating the message. Telephone conversations should begin or end with similar codes so that parents and children know whether or not the discussion is voluntary or is occurring under duress.

b. All family members should assemble a personal history and/or information sheet, preferably in their own handwriting, which can be used as an aid to law enforcement and intelligence officials in the event of an incident.

(1) This sheet should contain information items identified in Figure 14-1.

• Name	• Prescription for eyeglasses, if used
• Nickname	• Chronic illnesses
• Place and date of birth	• Special medicines and instructions for their use
• Address of principal residence and telephone number	• Pharmacies regularly used
• Address of secondary residence and telephone number	• Vehicles (types and license)
• Precise physical description (e.g., height, weight, scars, tattoos prostheses, dentures, etc.)	• School (type, class, address, names of teachers)
• Other identifying characteristics (e.g., birthmarks, physical handicaps, etc.)	• Recent information on educational qualifications, specializations, hobbies, etc.
	• Information about friends residing in diverse localities, including their telephone numbers

Figure 14-1. Personal History and/or Information Sheet

(2) The preparation of a brief family member oral history on a standard cassette recording might also be a helpful item to include in every DoD family's combatting terrorism and security plan. Reading aloud the information written down on the family member personal history/information sheet will provide a sample of the family member's voice. This sample can be used to help identify voices on recordings mailed to the authorities or media outlets in the event of a kidnapping.

c. Family legal documents including wills and powers of attorney should be updated at least annually; keep copies at home and the originals in a secure place.

Discuss with your family what they should do in the event of your abduction. Make a packet containing instructions, money, airline tickets, credit cards, insurance policies, and the name of whom to contact for survivor assistance. Be sure to discuss what should be done if one of the parents is kidnapped by terrorists. The family should resolve the following issues: the continuation of education for the children; if and where the family might relocate as a result of the kidnapping; and the disposition of family property. Holding these discussions and undertaking these preparations will ease worries about family matters during captivity in the event you are taken hostage or are kidnapped.

2. Family Crisis Response

a. The family almost always faces the first impact of a kidnapping alone. If the kidnapping happens at home, family members are often anxious witnesses to the crime; if the kidnapping occurs outside home, the family usually learns of the situation via telephone call. After requesting aid from the installation security office, the intelligence activities, the unit security office, and the local police, family members should take no further action. They should wait at home to provide assistance to crime scene investigators and specially trained law enforcement personnel skilled in kidnapping and/or hostage release negotiations.

b. Kidnap negotiations require specific preparation and professionalism. They should be entrusted to trained persons who can form a task force. This force should include an authoritative representative of the family. The task force should manage every aspect of the case and should delegate one member and a substitute to negotiate directly with the kidnappers.

c. Concurrently with the creation of the task force, the family should seek help from chaplains or others skilled in stress management Remaining calm under extraordinarily difficult circumstances is critical to the successful resolution of a kidnapping and hostage-taking episode. Finally, one must remember that everything, even this period of anguish, comes to an end. Whatever the outcome, the kidnap victim's family must know they did everything humanly possible to be reunited with their loved one.

D. DoD CODE OF CONDUCT

1. The Code of Conduct (Figure 14-2) as promulgated by Executive Order 10631, (reference gg)) and as amended by Executive Order 12017, (reference (hh)) outlines basic responsibilities and obligations of members of the U.S. Armed Forces. All members of the Armed Forces are expected to measure up to the standards embodied in the Code of Conduct. Although designed for prisoner of war situations, the spirit and intent of the Code of Conduct is applicable to Service members subjected to other hostile detention. Service members should conduct themselves in a manner that shall avoid discrediting themselves and their country.

2. The Code of Conduct does not formally apply to civilian employees of the Department of Defense. As representatives of the U.S. Government, however, they are expected to conduct themselves in a manner consistent with the spirit and intent of the Code of Conduct.

CODE OF CONDUCT

ARTICLE I. I AM AN AMERICAN, FIGHTING IN THE FORCES WHICH GUARD MY COUNTRY AND OUR WAY OF LIFE. I AM PREPARED TO GIVE MY LIFE IN THEIR DEFENSE.

ARTICLE II. I WILL NEVER SURRENDER OF MY OWN FREE WILL. IF IN COMMAND, I WILL NEVER SURRENDER THE MEMBERS OF MY COMMAND WHILE THEY STILL HAVE THE MEANS TO RESIST.

ARTICLE III. IF I AM CAPTURED I WILL CONTINUE TO RESIST BY ALL MEANS AVAILABLE. I WILL MAKE EVERY EFFORT TO ESCAPE AND AID OTHERS TO ESCAPE. I WILL ACCEPT NEITHER PAROLE NOR SPECIAL FAVORS FROM THE ENEMY.

ARTICLE IV. IF I BECOME A PRISONER OF WAR, I WILL KEEP FAITH WITH MY FELLOW PRISONERS. I WILL GIVE NO INFORMATION OR TAKE PART IN ANY ACTION WHICH MIGHT BE HARMFUL TO MY COMRADES. IF I AM SENIOR, I WILL TAKE COMMAND. IF NOT, I WILL OBEY THE LAWFUL ORDERS OF THOSE APPOINTED OVER ME AND WILL BACK THEM UP IN EVERY WAY.

ARTICLE V. WHEN QUESTIONED, SHOULD I BECOME A PRISONER OF WAR, I AM REQUIRED TO GIVE NAME, RANK, SERVICE NUMBER, AND DATE OF BIRTH. I WILL EVADE ANSWERING FURTHER QUESTIONS TO THE UTMOST OF MY ABILITY. I WILL MAKE NO ORAL OR WRITTEN STATEMENTS DISLOYAL TO MY COUNTRY AND ITS ALLIES OR HARMFUL TO THEIR CAUSE.

ARTICLE VI. I WILL NEVER FORGET THAT I AM AN AMERICAN, FIGHTING FOR FREEDOM, RESPONSIBLE FOR MY ACTIONS, AND DEDICATED TO THE PRINCIPLES WHICH MADE MY COUNTRY FREE. I WILL TRUST IN MY GOD AND IN THE UNITED STATES OF AMERICA.

Figure 14-2. Code of Conduct

3. DoD Directive 1300.7 (reference (ii)) prescribes three levels of training in the content and application of the Code of Conduct:

Level A: All Members of the Armed Forces.

Level B: Personnel whose military role entails moderate risk of capture.

Level C: Personnel whose roles entail a relatively high risk of capture or make them vulnerable to greater-than-average exploitation by a captor.

4. Appendix W contains detailed education objectives associated with each Article in the Code of Conduct. Level B training with particular emphasis on conduct during periods of confinement or detention by terrorists is recommended for the following DoD military and civilian personnel:

a. Defense attaches and their staffs.

b. Individuals assigned to High-Risk Billets.

c. Members of Military Assistance Advisory Groups assigned to countries assessed as Threat Levels CRITICAL, HIGH, or MEDIUM.

d. Members of Mobile Training Teams assigned to countries assessed as Threat Levels CRITICAL, HIGH, or MEDIUM.

e. Civilian employees of the Department of Defense assigned to countries assessed as Threat Levels CRITICAL, HIGH, or MEDIUM.

f. DoD Personnel assigned to units with responsibility for Personal Security Detachments or counterterrorism policy implementation.

5. The Department of the Air Force and the Department of the Army have several excellent films and video tapes that can be used in conjunction with this Handbook to improve understanding and application of the Code of Conduct by DoD personnel and their dependents to terrorist hostage and kidnapping situations.

6. Specific guidance for DoD personnel in implementing the Code of Conduct in terrorist captivity situations is as follows:

1. If assigned in, or traveling through, areas of known terrorist activity, U.S. military personnel shall exercise prudent antiterrorism measures to reduce their vulnerability to capture. During the process of capture and initial internment, they should remain calm and courteous, since most casualties among hostages occur during this phase.

2. Surviving in some terrorist detentions may depend on hostages conveying a personal dignity and apparent sincerity to the captors. Hostages may discuss nonsubstantive topics such as sports, family, and clothing, to convey to the terrorists the captive's personal dignity and human qualities. They shall make every effort to avoid embarrassing the United States and the host government. The purpose of that dialogue is for the hostage to become a "person" in the captor's eyes, rather than a mere symbol of his or her ideological hatred. Such a dialogue also should strengthen the hostage's determination to survive and resist. A hostage also may listen actively to the terrorist's feeling about his or her cause to support the hostage's desire to be a "person" to the terrorist. However, he or she should never pander, praise, participate, or debate the terrorist's cause with him or her.

3. U.S. military personnel held hostage by terrorists should accept release unless doing so requires them to compromise their honor or cause damage the the U.S. Government or its allies. U.S. military personnel must keep faith with their fellow hostages and conduct themselves according to the guidelines of this enclosure. Hostages and kidnap victims who consider escape to be their only hope are authorized to make such attempts. The hostage must weigh carefully the unique circumstances of the terrorist situation and all aspects of a decision to attempt escape.

E. HOSTAGE SURVIVAL SUMMARY

1. Although the DoD Components have implemented the DoD Combatting Terrorism Program, there is always a possibility that a DoD-affiliated person may be taken hostage or kidnapped. This chapter has presented specific steps to be taken immediately to ensure survival as a hostage. In addition, implementation of the measures described in this chapter will allow hostages to survive with dignity. Preservation of dignity, a sense of self-worth, and a sense that behavior during the period of confinement was honorable is critical to the long-term mental and physical health of the victim. Implementation of measures by DoD dependents is essential so that family members can provide support to hostages during and after a terrorist episode. Family members, too, must be prepared so that they, too, can retain a sense that their behavior during the crisis was honorable and helpful.

2. Terrorist episodes do end. Implementation of hostage survival measures outlined in this chapter is the foundation upon which life after the conclusion of kidnapping and/or hostage will be built.

CHAPTER 15

TERRORISM CRISIS MANAGEMENT PLANNING AND EXECUTION

A. INTRODUCTION

1. Chapter 1 introduced the DoD Combatting Terrorism Program concept as having both a preventive and reactive phase. Chapters 5 through 14 have dealt with many elements of prevention. The DoD Combatting Terrorism Program concept builds on a foundation of terrorist threat analysis and the preparation of an integrated threat estimate. The integrated threat estimate examines the interactions among the following elements:

a. Terrorist threat (provided by the intelligence community);

b. Risk of terrorist attack (provided by the DoD Component military and civilian staff at each echelon);

c. Vulnerability of DoD Components to terrorist attack (provided by the DoD component military and civilian staff at each echelon); and

d. Assessment of asset criticality to DoD missions and functions (provided by DoD component military and civilian staff at each echelon).

2. On the basis of the Integrated Terrorist Threat Estimate, military commanders and civilian managers as appropriate develop and implement a plan to reduce the likelihood of terrorist attack (terrorism prevention) and mitigate its effects should it occur. Preventive measures include terrorism awareness, education, and training; physical security enhancements at the installation, facility, and DoD personnel residence level (if necessary); and personal protective measures including education, training, and even classroom or residential instruction for DoD-affiliated personnel and their dependents.

3. Notwithstanding efforts to prevent terrorist incidents at DoD facilities or involving DoD-affiliated personnel, military commanders and civilian managers must also include the development of a terrorism crisis management plan to cover such contingencies when preventive efforts do not succeed. The purpose of this chapter is to review elements of a terrorism crisis management plan and examine implementation of the plan in the event of a terrorist attack on DoD-affiliated persons or DoD facilities.

B. TERRORIST INCIDENT CRISIS MANAGEMENT PLANNING

The establishment of a mechanism to respond to a terrorist incident is an essential element of the DoD Combatting Terrorism 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. Developing a Terrorist Incident Crisis Management Plan will probably draw on plans for other emergency situations which may arise on or near a DoD installation. In some instances, planning for disaster assistance, emergency evacuation of an installation or facility because of a hazardous materials incident, or criminal incidents such as bank robber and/or hostage-barricade will provide a good emergency planning and/or incident management planning baseline. The following elements enter into the preparation of a terrorist incident crisis management plan:

1. Intelligence

Crisis management plans should consciously allow for the gathering of information before, during, and after an incident. This is vital, both to the tailoring of preventive measures and for implementation of crisis management operations. The intelligence collection plan should note restrictions on collection and storage of information, properly segregating intelligence, counterintelligence, and law enforcement information. The plan should include identification of persons responsible for liaison and coordination of information regarding the threat of terrorism among local, State, Federal, and host-government authorities.

2. Integrated Terrorist Threat Estimate

a. The terrorist incident crisis management plan should identify terrorist threat groups thought to pose problems in the near, mid-, and long term. The plan should indicate whether or not these groups are operating adjacent to the installation or facility, or represent threats to units or personnel deploying from the installation to other locations.

b. As part of the integrated terrorist threat estimate, issues of risk, vulnerability, and criticality should be addressed. The integrated threat estimate should identify those types of terrorist weapons which might pose the greatest risk to DoD assets on the facility. It should assess the ability of the facility to maintain mission capability in the event of a terrorist attack, identifying recovery and reconstitution of assets available within the installation, from adjacent DoD installations or facilities, from nearby host-government facilities, and from the local economy. The integrated terrorist threat estimate should also identify which assets are critical to which missions supported by the installation and personnel assigned to it. It should also identify critical assets.

3. Security Countermeasures

a. The terrorist incident crisis management plan should identify elements from the DoD Threat Condition System (THREATCONs) appropriate for employment as part of its terrorist incident crisis management execution. The THREATCON System is discussed in greater detail in Chapter 17.

b. The plan should also identify a variety of security countermeasures that might be employed in response to an incident, storage locations of dedicated security countermeasures equipment, and the usual availability of expedient security equipment needed to implement the plan. For example, first aid kits, traffic control flares, traffic control cones, and tactical police radios are usually stored in law enforcement vehicles, gate

houses, and security checkpoints just inside the main entrance to an installation. Portable floodlights, traffic barricades, and auxiliary power generators that might be necessary to contain or resolve in incident are usually stored in a civil engineering or facilities maintenance yard.

4. Operations Security

The terrorist incident crisis management plan should address the various mechanisms by which terrorists can collect intelligence regarding activities or personnel at an installation or facility. The plan should identify specific operations security measures to be taken to offset as many collection techniques as possible.

5. Personnel Security

The plan should outline affirmative steps that should be taken to provide additional protection to critical DoD assets assigned to an installation or facility in response to terrorist threats, the risk of attack on those assets, and the vulnerability of missions and capabilities to the loss of such assets. DoD personnel who are "mission-critical" should be made aware of the terrorist threat in general and their importance to missions in particular; additional educational and training requirements for such personnel should be addressed by the plan.

6. Physical Security

The terrorist incident crisis management plan should be closely incorporated with overall installation and facility physical security plans. The plan should be coordinated with all military construction plans as early as possible to determine whether or not additional antiterrorism measures should be included in the design and construction and/or modification of existing or new facilities. The plan should also review facility intrusion detection systems, their usual mode of operation, maintenance schedules and history, and planned upgrades in the face of identified threats.

7. Security Structure

The plan should identify key DoD, local, State, Federal, and host-government (if any) agencies, offices, or departments that should be contacted in the event of an emergency. In addition, the plan should identify points of contact with the Staff Judge Advocate or General Counsel office as appropriate. The plan should specify points of contact among military, civilian, Federal, and host-nation law enforcement organizations for routine sharing of information, routine joint security activities, joint training and exercises, and joint or combined responses to incidents as appropriate. The plan should include copies of all law enforcement, fire services, and public health mutual aid agreements between the installation or facility and other local, state or federal agencies.

8. Operations Center Training

a. The terrorist incident crisis management plan should identify an emergency operations center that will be activated in response to an emergency or terrorist incident. The plan should include an inventory of communications, computing, and intelligence information collection and dissemination capabilities within the center. The plan should also note the location of the media center to be established in the event of an incident. The plan should note further the location of a dedicated crisis intelligence staff facility.

b. The plan should also discuss training and exercises to be completed by the emergency operations center staff as part of the terrorist incident crisis management process. Training goals and objectives should be identified, and plans to remedy problems uncovered in previous exercises should be presented.

9. Reaction Force Training

a. The terrorist incident crisis management plan should include a detailed assessment of response for training and readiness. The assessment should address the knowledge of laws and policies governing the use of force and use of deadly force in the protection of DoD assets. The plan should identify specific training requirements which all members of the response force should meet, as well as additional functional training.

b. For example, members of the reaction force; i.e., Special Reaction Team and/or Emergency Service Team (SRT/EST), hostage negotiators, protective services, drivers for high-risk personnel, installation and/or base and/or unit antiterrorism planners, and personnel responsible for the terrorist analysis input to the installation/base/unit threat analysis, cannot perform their mission without specialized training. In addition, appropriate members of the installation planning team should be trained in installation and facility physical security planning such as those offered by the U.S. Army Corps of Engineers and the U.S. Army Military Police School (USAMPS).

c. Where training has not been completed, the plan should identify resource and schedule requirements necessary and sufficient to complete such training.

10. General Observations

a. The terrorist incident crisis management plan should also address the following issues:

(1) Incident reporting requirements (e.g., logs, journals, after-action report).

(2) Appropriate management and support of news media coverage of an incident.

(3) Adequacy of communications within the installation or facility, between the installation and local law enforcement resources, and the adequacy of communications between the facility and the appropriate DoD component head.

(4) Potential requirement for foreign language and or hearing and/or speech interpreter.

(5) Identification of personnel with various foreign backgrounds to provide cultural intelligence on foreign subjects and victims, as well as to assist with any negotiation efforts.

(6) Explosive ordnance disposal (EOD) support.

(7) Purchase and/or use of civilian vehicles, supplies, food, etc., if needed (including use to satisfy a hostage demand).

(8) Payments to civilian employees for overtime if required.

(9) Messing, billeting, and transportation of civilian personnel.

b. Appendix X provides a checklist of issues to consider when developing or reviewing a terrorist incident crisis management plan. Appendix Y contains a sample terrorist incident crisis management plan format that may be used as an aid in the development of detailed plans outlined here.

C. INITIAL RESPONSE

1. Onset of a Terrorist Incident

a. The onset of a terrorist incident begins with the detection of an unlawful act of violence or threatened violence. Detection may result from routine surveillance performed by an installation or facility intrusion detection system, guard or security force, or aware DoD-affiliated persons. Once detection of a criminal act occurs, an initial assessment must be performed by the first responding security or law enforcement personnel. Four critical questions must be answered immediately.

[redacted]

DELETED

Figure 15-1. Initial Security Force Situation Assessment Criteria at Onset of Criminal or Terrorist Incident

c. [redacted]

2. Initial Response Force

a. [redacted]

b. [redacted]

c. [redacted]

3. Installation and/or Base Commander

The installation and/or base commander, depending upon established standard and/or standing operating procedures (SOPs), activates the installation's 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 and the U.S. Embassy, as required.

4. The Operations Center

The operational command, coordination, and control center (Operations Center) serves as the command post at a predetermined location. [redacted]

[redacted]

5. Confirmation

a. Since jurisdiction depends on whether the crime is a terrorist incident, it is important for the response force to 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.

b. The initial or specialized response forces may be required to provide only outer perimeter security or be prepared to manage all aspects of an event. [redacted] These installation and/or base response forces must therefore always be prepared for the most resource-demanding contingency. This level of readiness requires considerable sustainment training.

D. FOLLOW-ON 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.

1. Phase I: Locally Available Resources

a. Phase I is the commitment of locally available resources. [redacted]

b. [redacted]

2. Phase II: Augmentation of Initial Response Force

Phase II is the augmentation of the initial response force [redacted]

[redacted]

3. Phase III: Commitment of Specialized Counterterrorist Resources

[redacted]

4. Response Sequence

a. A typical response sequence to a terrorist incident for which DoD personnel remain responsible for containment and resolution is shown in Figure 15-2.

b. Figure 15-2 addresses the straightforward case within the United States, its territories, and its possessions where DoD components perform all three phases of terrorist incident crisis management--initial response, containment, and crisis resolution. The process outlined here applies to those instances overseas where SOFAs permit DoD components to manage terrorist crises on their own authority. The following section addresses those situations in which host governments or the FBI assume responsibility for managing the containment and resolution phases of a terrorist incident.

E. TERRORIST INCIDENT RESPONSE: SHARED AUTHORITIES AND JURISDICTIONS

a. As noted in Chapter 4 above, it is customary and usual for military commanders and civilian managers to assume responsibility for initial response, containment, and resolution of criminal incidents that occur on DoD facilities within the United States, its territories, and its possessions. T[redacted]

b. DoD installation military commanders and civilian managers have responsibility and authority for making an initial response and containing and resolving criminal incidents occurring within their installation. [redacted]

DELETED

Figure 15-2. DoD Management of Terrorist Incident From Initial Response Through Resolution Phases of Crisis

F. SPECIAL CONSIDERATIONS

The following special considerations apply in implementing crisis management.

1. Establishing Communications

[redacted] communications personnel must be able to respond to changing needs during the incident and be able to maintain, over a prolonged period, the communications channels included in the antiterrorism plan.

2. Evidence

Although the primary goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, etc., are important in achieving a successful prosecution. Maintaining the continuous chain of custody on evidence obtained during an incident requires documenting the location, control, and possession of the evidence from the time custody is established until presenting the evidence in court. Failure to maintain the chain can result in exclusion of the evidence. Types of evidence for which the chain must be established include:

a. Photographs taken during the incident.

b. Physical evidence, including any item(s) used by the terrorists.

c. Tape recordings of conversations between terrorists and hostage negotiators.

d. Reports prepared by the military police who initially responded to the incident scene.

e. Eyewitness testimony.

f. Demand notes or other written messages prepared by the terrorists.

3. Disposition of Apprehended Personnel

Apprehended military personnel must be handled according to Service regulations and applicable installation SOPs. In the U.S., civilian detainees must be released to the FBI or U.S. Federal Marshals for disposition. In foreign incidents, civilian detainees will be processed according to the SOFA with that particular country. The Staff Judge Advocate (SJA) should be consulted prior to releasing any individual to host-nation authorities.

4. Reports

Reporting to higher headquarters is an important element in any special threat or terrorist situation. Each Service and command 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 seven working days after termination of the event. This should include all staff journals and other documentation to include detailed information concerning disposition of evidence and captured individuals. The SJA and law enforcement personnel should ensure this report is in sufficient detail to meet prosecution requirements.

5. Public Affairs

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

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

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

c. Support DoD public affairs strategy on releasing information pertaining to antiterrorism plans, operations, or forces involved in antiterrorist operations.

(1) [redacted]

(2) When U.S. military antiterrorist forces are employed, the Department of Defense provides a spokesman for dealing only with antiterrorist military operational matters. On military installations, the Department of Defense may delegate the public affairs responsibility to a designated DoD representative.

(3) The DoS coordinates public affairs during terrorist incidents overseas. The DoS may delegate the public affairs responsibility to a designated DoD representative.

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

(5) When the operations center is activated, it should include the activities of the Public Affairs Office (PAO) and media center. The media center should be located in a separate location away from the operations center. The PAO will prepare media releases and conduct briefings at the media center during the incident. The PAO will use information obtained from participating operations center activities. Information released by the PAO will be 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, providing them thorough briefings, maintains DoD credibility and preserves freedom of information. Appendix AA provides additional guidance.

6. 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 to record every action that occurred during the incident.

7. After-Action Reporting

a. 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 determine the

effectiveness of the antiterrorism plan. All personnel involved in the antiterrorism operation should be debriefed and the debriefings recorded in accordance with Service OSD Agency requirements pursuant to DoD 0-2000.12 (reference (a)). This information will be used to develop lessons learned and after-action reports. It is the responsibility of the military installation commander or the civilian manager of a DoD agency activity to ensure all required after-action reports are prepared and subsequently reviewed with representatives of the Staff Judge Advocate's and/or General Counsel's office as appropriate.

b. The after-action report should be prepared in a format that is compatible with the Joint Universal Lessons Learned System (JULLS) operated for the Chairman of the Joint Chiefs of Staff.[1] A sample format appears as Figure 15-3.

Joint Universal Lessons Learned System (JULLS)
JULLS Report Format

JULLS Number	Unique 10 Digit Number, Point of Contact, Phone #	
Exercise/Operation	Name	
Keywords	Quick Database Searches	
Title	Title of Individual Lesson Learned	
Discussion	Detailed Narrative	
Lessons Learned	How to Succeed; Problems Encountered; Solutions Implemented	
	Information Other Commanders Can Use!	
Recommended Actions	Suggested Changes in Procedures, Organization, Equipment	
Comments	Recommended Disposition	
Field Codes	Subject:	e.g., personnel, logistics, doctrine, etc.
	Interoperability:	planning, training, organization, etc.
	Echelon:	joint staff, major command, field unit, etc.

JULLS is operated by the Joint Center for Lessons Learned
Joint Staff, J-7 Evaluation and Analysis Division
in accordance with MCM-86-90 dated 12 June 1990

Figure 15-3. Sample JULLS Report Format

c. It is also important to capture information on terrorist events that may have been averted due at least in part to the successful implementation of antiterrorism measures. Hence, all DoD activities should report on incidents which appear to have been averted as a result of or at least are correlated in time and in place with antiterrorism measures put into effect. Following the JULLS format, the reports should include information on the threat,

---

1 The Joint Universal Lessons Learned System and its use by DoD Components is prescribed in Joint Chiefs of Staff Policy Memorandum 53, "Military Capability Reporting," March 28, 1991. Operation of the JULLS is exempt from the requirements of DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986 (reference (jj) pursuant to the waiver provided in paragraph E.4.b).

its estimated capability, its estimated intentions, its history, a description of measures adopted upon receipt of warning information, and an assessment of the results of antiterrorism measures.

G. TERRORIST INCIDENT CRISIS MANAGEMENT SUMMARY

1. The purpose of this Handbook is to provide information necessary and sufficient to reduce the risk of terrorist attack on DoD-affiliated personnel, facilities, materiel, and assets, and mitigate the effects of such attacks should they occur. This chapter has emphasized the importance of planning, preparing, and training installation, facility, and unit security personnel to respond to criminal incidents. Such incidents may or may not be politically motivated, and may therefore be, or not be, terrorist in nature. The intent of the perpetrator(s) at the initial onset of an incident may be ambiguous at best; the jeopardy or potential danger to DoD assets will be much clearer.

2. Notwithstanding the apparent motivation of perpetrators of criminal acts on DoD installations, in DoD facilities, or against DoD personnel, the incident must be joined, contained, and resolved. [redacted]

3. There are two different sets of special concerns related to crisis management planning as the result of terrorist acts. The first is the specific security problem for civilian managers and military commanders posed by bomb threats. This is addressed in Chapter 16. The second is the challenge of maintaining an installation's day-to-day operations and routines at an advanced level of preparedness directed by the DoD Terrorist Threat Condition (THREATCON) System. This subject is discussed in Chapter 17.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 16

BOMB THREAT AND BOMB RESPONSE PROCEDURES

A. INTRODUCTION

1. Terrorists have frequently used homemade explosive devices (Improvised Explosive Devices or IEDs) in carrying out their attacks against DoD personnel, facilities, and assets. These are ideal terrorist weapons. They are made at relatively low cost; the components of many IEDs are common items which can be obtained from many sources and are difficult to trace. IEDs can be large or small, and can be designed so that they are transported to the site of attack in components for last-minute assembly. [redacted]

2. [redacted]

3. [redacted]

B. DISCOVERING BOMBS

1. One can ask the question: "Where have terrorists placed bombs in the past and where should we look for them?" There is no easy answer. Figure 16-1 lists a few obvious locations that should be examined; terrorists using bombs as their weapons of choice can be very creative in designing and placing their weapons; the list is illustrative, not exhaustive.

2. Bombs can be found anywhere people can place them. Without becoming paranoid and seeing a bomb under every rock and behind every tree, the practical answer is: "Where they can be easily placed without the bomber being caught."

C. DAMAGE AND CASUALTY MECHANISMS

1. IEDs and other explosive devices inflict casualties in a variety of ways. Figure 16-2 summaries the mechanisms by which explosive devices cause casualties.

DELETED

Figure 16-2. Damage and Casualty Mechanisms from Bombs and IEDs

[redacted] As a general rule, the further away from a bomb, the safer the intended or collateral targets are. Blast effects, fragmentation injuries, and injuries resulting from flying debris diminish greatly as the distance between a bomb and possible targets increase. The amount of material in the device, the type of explosive material, the manner in which the device is constructed, and the location or container in which it is placed all have a bearing on the specific destructive potential for each IED.

3. There are, however, four general rules to be followed:

a. Move as far away from a suspicious object as possible without being placed in further danger from other hazards (traffic, secondary sources of explosion such as POL storage in the event the device detonates, etc.)

b. Stay out of "line of sight" of object, thereby reducing hazard of injury as a consequence of direct fragmentation;

c. Keep away from glass windows or other materials which could become additional flying debris; and

d. Remain alert for additional or secondary explosive devices in the immediate area, especially if the existence of a bomb threat evacuation assembly area has been highly publicized.

4. [redacted]

5. Others have used a real or simulated device to force evacuation of a facility, only to detonate a much more substantial device in identified bomb threat evacuation assembly areas. Such attacks are especially harmful because the evacuation assembly areas often concentrate government or commercial office workers more densely than they are when dispersed throughout their usual workplaces.

D. RESPONDING TO BOMB AND/OR IMPROVISED EXPLOSIVE DEVICE THREATS

Appropriate responses to take when a suspected improvised explosive device (IED) is discovered are outlined below.

1. Telephonic Threat

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 Z provides advice on handling anonymous telephone calls.

2. Response to Telephonic Threat

a. Upon receiving an anonymous warning or threat, notify the Provost Marshal's Office (PMO), Security Police, Security Forces, or other law enforcement and/or security offices immediately. Local standard and/or standing operating procedures (SOPs) determine subsequent actions. Immediate action may include search without evacuation, movement of personnel within the establishment, partial evacuation, or total evacuation. Appendix A offers two approaches to the collection of information from a person reporting a bomb or uttering a threat.

b. Figure 16-3 provides some criteria to be used in evaluating a bomb threat.

[redacted]

Figure 16-3. Bomb Threat Evaluation and Facility Evacuation Criteria

c. The criteria outlined above are intended to be an aid to military commander and civilian management judgment, not a substitute for it. Each situation must be carefully assessed.

3. Searching for a Suspected IED

a. Figure 16-4 summarizes the types of searches may be employed when searching for a suspected improvised explosive device.

[redacted]

Figure 16-4. Searches in Response to Bomb and/or IED Threats

b. Searches can be undertaken in response to a telephonic threat or a report of an unidentified object on or near premises occupied by DoD personnel.

4. Search Procedures

a. Figure 16-5 outlines procedures that should be followed if a search for explosive devices must be conducted before qualified Explosive Ordnance Disposal (EOD) teams arrive. Such circumstances might arise in the event of a very short warning period. In other instances, a threat of a bomb against some facilities, if true, might necessitate evacuation of a very large area. In such circumstances, searching for the presence of an explosive device for the purpose of identifying its location, appearance, and possible operating characteristics may be warranted.

[redacted]

Figure 16-5. Expedient IED and/or Bomb Search Procedures

b. In general, personnel who have not been trained in IED search and identification techniques should refrain from undertaking searches for such devices. [redacted]. Depending upon the devices used to arm and trigger an IED, the search process could actually result in an explosion.

c. EOD teams are generally best prepared to conduct effective searches and identification of IEDs and explosives.

5. Search Organization

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 a search team leader who should report to the person controlling the search when each area has been cleared. [redacted]

6. 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.

7. Alarm System

The bomb threat alarm system should be easily distinguished from the fire alarm.

8. Assembly Areas

a. Assembly areas are preselected and well known to personnel. Establish a clearly defined procedure for the controlling, marshaling, and checking of personnel within the assembly area. If buildings or establishments are in a public area, coordinate assembly areas with local police. Assembly areas are selected using criteria illustrated in Figure 16-6.

[redacted]

Figure 16-6. Emergency Assembly Area Selection Criteria

b. As discussed below, efforts should be made to preserve location uncertainty for key personnel who evacuate a facility upon notice of an emergency.

9. Routes to Assembly Areas

[redacted] 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.

10. Personnel Evacuation Response

Upon hearing the alarm, personnel should lock up or secure all classified materials, 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. Opening the building will reduce internal damage as a consequence of blast effects and will mitigate to some degree the extent of debris flying out of or falling from the building should a detonation occur.

11. 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 initial control point (ICP) as the focal point for the PMO and for military police control.

E. 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.

F. INCIDENT CONTROL POINT (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 PMO or local police upon their arrival. Maintain the cordon until the PMO and/or Security Policy and/or Security Forces or local police have completed their examination or state that the cordon may stand down.

G. DISCOVERY OF A SUSPECTED IED

When a suspicious object has been found, its location, and general description should be reported immediately to the nearest law enforcement or supervisory person. Do not touch or move a suspicious object. Figure 16-7 summarizes steps to be taken following discovery of a suspicious object.

H. REACTION TO AN EXPLODED IED

1. Figure 16-8 summarizes action to be taken in the event that an explosive/ improvised explosive device detonates at a DoD facility.

2. Civilian management officials and subordinate military commanders continue to have important personal roles to fulfill during a bomb and/or IED attack on DoD personnel, facilities, and assets. These responsibilities are summarized below in Figure 16-9.

3. Execution of steps outlined in Figure 16-9 will provide substantial assistance to the crisis management team and give other personnel constructive, supportive actions to be taken to assist resolution of the crisis. Care must continue to be exercised, however, that

additional explosive devices are not concealed to be detonated during the midst of rescue operations. Such attacks add to the physical damage and emotional devastation of bomb and/or IED attacks.

[redacted]

Figure 16-7. Actions In Response to Discovery of a Suspicious Object

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 PMO and/or Security Police and/or Security Forces or local police if they are not yet on scene.

(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, etc., and corresponding personnel is maintained.

(6) Refer media inquiries to the Public Affairs Officer.

(7) Establish a separate Information Center to handle inquiries from concerned friends and relatives.

Explosion With Casualties

[redacted]

Figure 16-8. Actions Following Detonation of Explosive Device

Reporting

- All personnel should pass available information to the operations center
- Do not delay reports because of lack of information--report what you know. Do not take risks to obtain information.
- Include the following information in your report:
  - (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.

Emergency Assistance to Authorities

- Upon arrival, ensure PMO and/or Security Policy and/or Security Forces, and other emergency response units from local police, fires and rescue, and EOD are not impeded from reaching the ICP. Help maintain crowd control and emergency services access to the site.
- Evacuate through the doors and windows of buildings.
- [redacted]
- Locate, identify, and make witnesses available to investigative agency representatives when they arrive on scene. Witnesses include the person(s) who discovered the device, witnessed the explosion, or possesses detailed knowledge of the building or area.

Figure 16-9. Assistance to Crisis and/or Threat Management Team

I. TERRORISM AND BOMB AND/OR IED RESPONSE SUMMARY

Use of bombs and IEDs in the commission of terrorist attacks against DoD personnel, facilities, and assets is an all too common occurrence. The procedures outlined above are intended to help a DoD facility respond to an attack before an explosive device detonates. The procedures discussed are also intended to help mitigate the consequences of an attack in the event that efforts to find an explosive device and render it inoperable are not successful. Incurring the costs to DoD facilities and installations of detecting an explosive device and terminating a terrorist incident before the device can detonate are almost always preferable to exercising plans and options to respond to a detonation. Several of the security measures discussed in preceding chapters will help reduce the likelihood of a successful bomb and/or IED attack against DoD assets.

CHAPTER 17

DoD TERRORIST THREAT CONDITION SYSTEM

A. INTRODUCTION

1. As part of the Department of Defense's comprehensive approach to combatting terrorism, a common framework of protective measures against terrorist threats has been developed for implementation by all DoD Components. The purpose of this chapter is to expand on terrorist incident crisis management planning by describing the general framework of the DoD Terrorist Threat Condition System and its implementation among various DoD Components. Before doing so, however, it is important to differentiate three different concepts:

a. Terrorist Threat Level;

b. Terrorist Threat Condition System (THREATCONS); and

c. Defense Readiness Conditions (DEFCONS).

2. While there is a relationship among the three concepts underpinning these terms, it is not a linear one.

B. ENVIRONMENT AND FORCE READINESS DESCRIPTORS

Terrorist Threat Level, Terrorist Threat Condition System, and Defense Readiness Conditions are very different concepts. Although somewhat interrelated, the purposes these concepts serve are very different, and their specific use has vastly different ramifications for the DoD Components.

1. Terrorist Threat Levels

a. As noted in Chapter 5 above, Terrorist Threat Levels are one word descriptors which summarize the DoD-level intelligence analysis of the threat of terrorism to DoD personnel, facilities, materiel, and assets on a country-by-country basis. There are five Terrorist Threat Levels:

(1) Critical.

(2) High.

(3) Medium.

(4) Low.

(5) Negligible.

b. Using the six threat factors described in Chapter 5, intelligence analysts assign terrorist threat levels to individual countries based on assessments of information obtained from all sources. Figure 17-1 illustrates the application of these threat analysis factors to generate terrorist threat levels.

	Threat Analysis Factors				
THREAT LEVEL	Existence	Capability	History	Intentions	Targeting
CRITICAL	•	•	¤	¤	•
HIGH	•	•	•	•	
MEDIUM	•	•	•	¤	
LOW	•	•	¤		
NEGLIGIBLE	¤	¤			

• Factor must be present ¤ Factor may or may not be present

The factor, Security Environment, which assesses the ability of police, paramilitary, and military institutions to preserve social order, may be a mitigating factor. Countries which have effective internal security institutions may be assessed at a lower threat level on that basis.

Figure 17-1. Terrorist Threat Analysis Factors and Terrorist Threat Levels

2. Terrorist Threat Condition System

a. The Terrorist Threat Condition System (THREATCONs) describes the progressive level of protective measures implemented by all DoD components in response to terrorist threats in accordance with DoD Directive 0-2000.12 (reference (a)). The terminology, definitions, and specific recommended security measures are designed to ease inter-Service coordination and support of DoD Component combatting terrorism efforts.

b. There are five Terrorist Threat Condition (THREATCON) Levels. The circumstances under which and the purposes of each protective posture are as follows:

(1) **NORMAL.** Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.

(2) **ALPHA.** Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable.

(3) **BRAVO.** Applies when an increased and more predictable threat of terrorist activity exists.

(4) **CHARLIE.** Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent.

(5) **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 is likely. Normally, THREATCON DELTA is declared as a localized warning.

c. Declaration of THREATCONs is the prerogative of the military commander or the head of DoD Components. As a general rule, lower echelons within each DoD

Component should adopt terrorist threat measures consistent with the THREATCON declared by the CINCs, their subordinate component commanders, or the heads of the DoD Components.

d. Specific THREATCON measures appropriate for land installations, ships, and airfields and included in Appendix BB, DoD THREATCON System. Local commanders retain authority to implement terrorist threat measures (THREATCON measures) to defend against a greater than expected terrorist threat; local commanders should not implement measures less rigorous than those appropriate for declared THREATCON level for their particular facility. LOCAL COMMANDERS MAY ADOPT HIGHER THREATCON MEASURES THAN ORDERED BY CHAIN OF COMMAND IF LOCAL CONDITIONS WARRANT GREATER PROTECTION.

3. Defense Readiness State

Defense Readiness States or DEFCONs are mobilization and deployment states of the entire U.S. defense establishment including but not necessarily limited to DoD components, other U.S. Government agencies and departments assigned specific responsibilities to assist the Department of Defense during times of war, and elements of the Defense Industrial Base. DEFCONs refer to wartime postures. DEFCONs are declared by the National Command Authority.

4. Comparisons

a. Figure 17-2 offers a brief comparison and contrast among Terrorist Threat Level, Terrorist Threat Conditions, and Defense Readiness Conditions.

b. As Figure 17-2 makes clear, there is no direct correlation between threat information, (e.g., Intelligence Summaries, Warning Reports, and Spot Reports), and THREATCONs. Threat Level Declarations are probabilistic statements; they do not contain judgments with respect to timing of terrorist attacks. Terrorist Threat Level declarations ARE NOT warning reports. However, dissemination of Threat Level Declarations and supporting country-by-country threat analyses, coupled with the guidance provided below, assists commanders in making prudent THREATCON declarations.

c. DEFCONs rarely figure directly into the implementation of THREATCONs except that under some circumstances, accelerated DEFCON state may require implementation of high levels of THREATCONs. [redacted]

	Terrorist Threat Level	Terrorist Threat Conditions (THREATCON)	Defense Readiness Conditions (DEFCON)
Description	Description political environment surround DoD personnel, facilities, and assets or interests and the degree to which they are at risk of terrorist attack; used in in peacetime, crisis, and mobilization periods	A system of protective measures intended to aid in the consistent allocation of security resources by DoD components, facilitate inter-Service coordination, and enhance overall implementation of DoD combatting terrorism policies	A short-hand description of measures taken by U.S. forces to mobilize from peacetime to wartime postures. DEFCON system generally applies to General War Mobilization.
Declared By	Intelligence components or organizations	Military commanders at all echelons, heads of DoD Agencies; other DoD components	National Command Authorities
Implemented By	Not applicable	Lowest to highest echelons within DoD Components;	Combatant Commands and other DoD components as required; may be extended to other U.S. Government agencies and departments by Executive Order and declaration of National Emergency by the President, or declaration of War by the Congress
Results In	Further studies by DoD components with respect to a need to implement Combatting Terrorism Measures	Allocation of security resources in accordance with a schedule of protective measures based on terrorist threat, risk of terrorist attack vulnerability of DoD assets, and ability to accomplish assigned missions as a result of terrorist attack, and criticality of DoD asset(s) to be protected.	Mobilization of Active Forces; mobilization of Reserve Forces; forward deployment of combat units, combat service and combat service support units, mobilization of war reserve fleet; CRAF Air Cargo Fleet; and industrial base.

Figure 17-2. Functional Differences Among Terrorist Threat Level, Terrorist THREATCON System, and Defense Readiness States

d. Although there is no direct relationship between Terrorist Threat Level declarations and THREATCONs, it is clear that terrorist threat plays a large role in bringing about the declaration of THREATCONs. The relationship between Terrorist Threat Level and THREATCONs is explored below.

C. SELECTION OF THREATCONS

1. The DoD Combatting Terrorism Program relies heavily on the concept of an integrated threat assessment in which military commanders and civilian managers routinely and continually examine terrorist threat analyses prepared by the intelligence community as well as assessments of terrorist attack risk, the vulnerability of their missions to such attacks, and the criticality of DoD assets entrusted to them for safekeeping. DoD Directive O-2000.12 (reference (a)) reminds commanders:

A COMMANDER, AGENCY, OR ORGANIZATION DIRECTOR DETERMINES which THREATCON level is to be designated and which security measures are appropriate. Actions should be based on all information, and command liaison, AS TEMPERED BY BEST JUDGMENT AND KNOWLEDGE of the local situation.

2. Some of the concepts introduced in earlier chapters of this Handbook may be helpful assessment guides in declaring a terrorist threat level or in implementing terrorist threat response measures dictated by the selection of a THREATCON by higher commands.

3. Figure 17-3 suggests an analytical process to be carried out by each level military command and each installation management to recommend or to select an appropriate THREATCON level when the combination of factors discussed below exceeds the ability of the usual physical security system (barriers, surveillance and detection systems, security forces, and dedicated response forces) to provide the level of asset protection required by operational considerations, mission and functions, or DoD policy.

4. Figure 17-3 draws heavily from analysis presented in preceding chapters to illustrate the utilization of the Integrated Terrorist Threat Estimate. Selection of THREATCONs makes use of information and analyses used to assemble such estimates.

a. Integrated Terrorist Threat Estimate Elements

(1) Figure 17-4 illuminates the use of information and analysis performed in the process of preparing integrated Terrorist Threat Estimates at the unit or installation, the CINC and his subordinate component command, Service, and DoD levels in the process of assessing the need for and the selection of appropriate Terrorist Threat Conditions.

(2) Figure 17-4 reinforces earlier discussion in which it was asserted there is no direct relationship between Terrorist Threat Levels and Terrorist Threat Conditions. As the figure illustrates, Terrorist Threat Level declarations are only one input into a command or management decision to allocate supplemental security resources to the peacetime defense of an installation, facility, or DoD asset.

(3) Furthermore, the figure is incomplete to the extent that it suggests integrated terrorist threat estimates are static and insensitive to change. Just the opposite is true.

(4) Terrorist threat analysis inputs are updated frequently; each change in the history of capability of a terrorist threat group may have implications for the physical security threat it presents to an installation or facility. Use of new weapons, employment of weapons against new types of targets or in a new mode can have serious implications for the capability of an existing physical security system to withstand and defeat terrorist assault.

(5) Assessment of terrorist attack risk is an examination of DoD practices and procedures. These are subject to frequent change based in part on evolving roles, missions, and functions assigned to DoD installations and facilities, and the personalities

DELETED

Figure 17-3. General THREATCON Selection Process

DELETED

Figure 17-4. Integrated Terrorist Threat Estimate Elements and Selection of Terrorist Threat Conditions

and experiences of military commanders and civilian managers in solving operational problems. Changes in day-to-day operations require reassessment of terrorist attack risk, even if the basic nature of the terrorist threat to an installation or facility does not change.

(6) Similarly, changes in deployment of units or activities from one installation to another may radically alter assessments of risk, vulnerability, and DoD asset criticality.

(7) The basic or initial integrated terrorist threat estimate provides a nominal baseline from which deviations can be examined. It is the temporary increases or decreases in terrorist attack risk, terrorist attack vulnerability, and DoD asset criticality that must be examined carefully to ensure proper allocation of protective resources. These concerns are described as Situational Risks, Vulnerability, and Criticality in Figure 17-3 above.

b. Physical Security Protection Level

(1) [redacted]

(2) [redacted]

(3) [redacted]

(4) All DoD assets are not equally critical; even some critical assets are "critical" for altogether different reasons. Given limited security resources, selecting DoD assets for priority protection can be a difficult challenge. Guidance in reference (cc) coupled with an integrated terrorist threat estimate can help military commanders and civilian managers identify priority assets for additional protection in light of known terrorist threats.

c. Costs of THREATCON Implementation

(1) Implementation of Terrorist THREATCONs does not come without costs that can be measured and described both quantitatively and qualitatively.

(2) Figure 17-5 offers some illustrations of these costs associated with various THREATCON measures.

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Figure 17-5. Example of Quantitative and Qualitative THREATCON Costs

(3) [redacted] DoD Directive O-2000.12 makes the following observations with respect to THREATCONs ALPHA, BRAVO, and CHARLIE. [redacted]

THREATCON ALPHA: [redacted]

THREATCON BRAVO: [redacted]

THREATCON CHARLIE: [redacted]

(4) In view of the costs of THREATCONs on the one hand and the need to enhance security in the face of terrorist threat on the other, several DoD components have developed their own Random Antiterrorism Measures Program. This innovative approach

addresses trade-offs between security benefits of THREATCONs and financial and operational costs.

D. RANDOM ANTITERRORISM MEASURES

1. The underlying principles of Random Antiterrorism Measures (RAM) have already been introduced in preceding chapters. RAM efforts seek to deter terrorist attacks on DoD facilities and personnel by:

a. Varying routines.

b. Being sensitive to changes in the security atmosphere around DoD facilities and personnel.

2. The basic approach is to identify at any THREATCON a set of measures extracted from higher THREATCONs that can be employed to supplement the basic THREATCON measures already in place. This is illustrated by Figure 17-6.

3. At THREATCON Alpha, certain measures from higher THREATCONs are implemented in addition to THREATCON Measures 1-10. In the example illustrated, selected BRAVO, CHARLIE, and DELTA measures have been selected for implementation that convey an external impression of greater vigilance and awareness to the presence of observers outside the facility. Random searches of vehicles seeking to enter the installation, proliferation of foot patrols, removal of trashcans and waste receptacles around buildings imply that the security forces are aware of the possibility of an intrusion into the facility, or worse.

4. Implementation of RAM programs have three purposes. First, military commanders can use RAM as a tool to test which measures have higher costs to an installation or facility in terms of productivity than others. A RAM program can help identify those measures that security personnel and the installation infrastructure are more capable of sustaining and those that will be unduly stressful on human and materiel resources.

5. Second, RAM programs provide security forces with training and stimulation. This makes their job more challenging, but also more interesting and more exciting. By keeping the guard force interested and alert, RAM programs appear to increase security, even if they do so only by making the security forces more attentive to their regular assignments.

6. Third, RAM programs change the security atmosphere surrounding an installation. Such programs, when implemented in a truly random fashion, alter the external appearance or security "signature" of an installation to terrorists or their supporters who may be providing surveillance assistance. [redacted]

7. [redacted]

terrorists have introduced uncertainty in planning, organizing, training, and movement of DoD resources throughout the world.

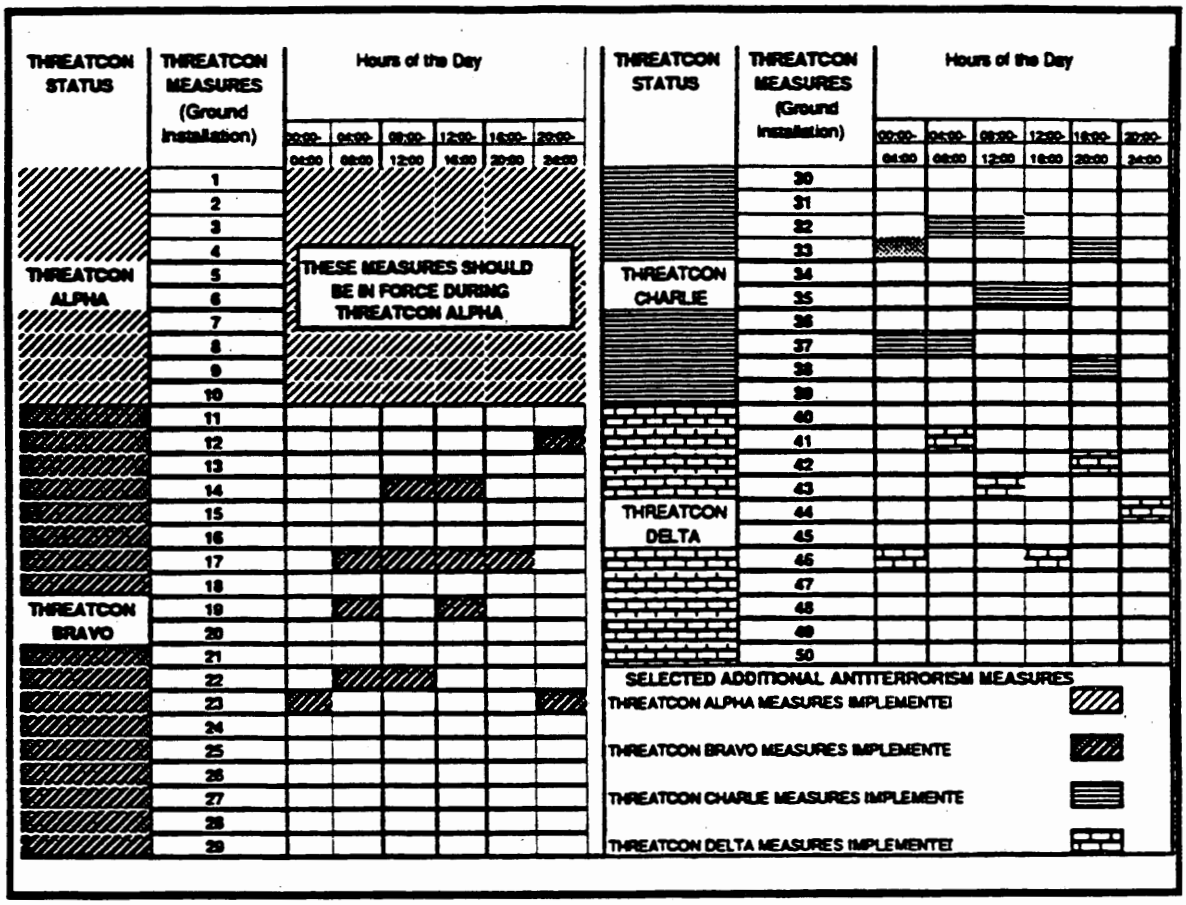


Figure 17-6. Illustration of Random Antiterrorism Measures Implementation

8. [redacted]

9. On the other hand, RAM programs offer military commanders an excellent alternative to full implementation of all THREATCON measures when Terrorist Threat Estimates suggest THREATCON ALPHA or THREATCON BRAVO may not be adequate protection in view of the risk, vulnerability, and criticality of DoD assets at the installation for the moment. Selected RAM measures extracted from THREATCONs CHARLIE and DELTA supplementing a THREATCON ALPHA or THREATCON BRAVO posture might be a more economical, sustainable response to a terrorist threat.

E. IMPLEMENTATION OF DoD THREATCONS

1. This chapter has focused on the differences among Terrorism Threat Levels, the DoD Terrorist Threat Condition (THREATCON) System, and the DoD and/or National

Command Authorities Defense Readiness Condition (DEFCON) System. All three concepts are descriptive terms which in shorthand notation describe considerable analysis (for Threat Levels) or allocation and expenditure of resources (THREATCONs and DEFCONs). There is no direct connection among any of these concepts.

2. Threat Level is an intelligence judgment about the likelihood of terrorist attacks on DoD personnel and facilities. It is not a warning. Threat levels do not allocate protective resources. Such decisions are properly in the domain of commanders, not the intelligence community.

3. THREATCONs are a series of protective measures whose implementation is elected by military commands and civilian managers of defense agencies where appropriate. THREATCONS are selected by assessing the terrorist threat, its capability to penetrate existing physical security systems at an installation, the risk of terrorist attack to which DoD facilities and personnel expose themselves, the ability of the installation or units to carry on with missions even if attacked, and the criticality to DoD missions of assets to be protected. [redacted]

4. DEFCONS refer to Defense Readiness Conditions and are changed only by direct order from the National Command Authorities.

5. This chapter concludes with an illustration of an innovative technique to the implementation of DoD combatting terrorism policies and programs not previously included in DoD issuances. The RAM implemented on the initiative of individual DoD installations are good examples of effective combatting terrorism measures not always included in DoD issuances. The RAM programs offer three clear benefits: a low-cost approach to testing the ability of individual installations or activities to implement DoD combatting terrorism measures; an excellent vehicle for training security personnel and keeping awareness of the threat of terrorism high at DoD installations; and a serious complication in the collection of intelligence against DoD installations in advance of terrorist attacks.

6. The next chapter of this Handbook turns to the application of DoD combatting terrorism measures to forces deployed for training or as part of expeditionary forces.

CHAPTER 18

COMBATTING TERRORISM PRACTICES FOR EXPEDITIONARY AND DEPLOYED FORCES

A. INTRODUCTION

1. The material presented in this chapter is most applicable to Service-unique situations when forces are deployed as part of training exercises under the control of a Service and not under the operational control of a CINC. The procedures described below are identical to those found in Joint Publication 3.07 (reference (kk)).

2. Combatting terrorism measures should be taken by military units and individual service members to protect themselves and ensure their ability to accomplish assigned missions during deployment and expeditionary operations. The installation, base, port, or unit combatting terrorism plan provides the mechanism to ensure readiness against terrorist attacks while the unit performs its mission during deployments. The degree of the protection required depends on the threat in a given location. Commanders must continually evaluate installation and/or base and/or port and/or unit security against the terrorist threat in order to evaluate security requirements effectively. This responsibility cannot be ignored.

B. 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 units performing security assistance, peacekeeping, mobile training teams, and other small unit activities can be derived from these measures.

1. Installations, Bases, Sites, and Non-Urban Facilities

Forces are frequently employed for security operations or other short-term, conventional, combat-related tasks. Easily defended locations are often rare in areas due to 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.

a. Estimate Situation

The commander and staff should complete a thorough estimate of the situation using mission, enemy, terrain, and troops-time and political planning factors in developing

a security assessment. The questions outlined in Figure 18-1 aid in developing an estimate of the terrorist situation.

DELETED

Figure 18-1. Estimating the Combatting Terrorism Situation for Deployed and Expeditionary Forces

b. Develop Plan

Defenses should include a combination of law enforcement and/or 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.

(1) Fortification Considerations

Figure 18-2 provides general guidance concerning fortification materials.

DELETED

[redacted]

Figure 18-2. Fortification Materials

(2) Obstacles

Obstacles slow down or stop vehicles and personnel approaching an area. [redacted]

(3) Local Security

Local security must be around-the-clock to provide observation, early warning and, if necessary, live fire capabilities. [redacted]

Figure 18-3 presents a list of equipment items which should be available to security police and/or security forces as part of installation antiterrorism programs, training activities, and intimidating shows of force intended to discourage outbreaks of violence against DoD facilities, equipment, personnel or other assets.

DELETED

Figure 18-3. Specialized Equipment for Local Security

(4) Establish Defense

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

(a) [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

2. Guard Duties

Guard duties are detailed in Service regulations and in local general and special orders. Heads of Defense Agencies should use the Service regulations for the Service or Agency providing law enforcement support to the Agency for detailed elaboration of guard duties. However, in a terrorist high-risk environment, special orders should address at a minimum:

a. Details of authorized passes; provide samples of passes.

b. Procedures for searching people and vehicles.

c. Response to approach by unauthorized personnel or hostile crowds.

d. [redacted]

e. [redacted].

f. [redacted]

g. [redacted]

h. [redacted]

3. **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 utilized. If road movement is required:

a. Avoid establishing a regular pattern.

b. Vary routes and timing.

c. Never travel in a single vehicle.

d. Avoid traveling at night or during periods of agitation; e.g., religious holidays, political holidays, etc.

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

f. Plan alternate routes and reactions to various threatening scenarios.

g. Plan communications requirements.

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

i. Provide adequate security.

j. Plan in advance for maintenance and/or evacuation.

4. **Vehicle Protection**

[redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

f. [redacted]

g. [redacted]

h. [redacted]

i. [redacted]

5. Convoys

a. 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 prior to 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 assets 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 40-mm machine guns are extremely effective. Overhead helicopters and AC-130 gunships can also be utilized as air escort 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 advanced 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 vehicles, and expected arrival of first and last vehicles at destination.

(g) Identify action upon arrival.

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

6. **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:

a. [redacted]

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

c. Ensure the railway is free of obstructions or explosives.

d. Patrol the railway area.

e. Place armed security personnel on duty throughout the train to include engine room and trail car.

f. Patrol and guard departure and arrival stations.

g. Use deception measures.

h. Provide air cover (AC-130, helicopters, etc.).

i. Maintain communications within the train and with outside agencies.

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

7. **Sea Movement**

[redacted] hostile coastlines are visible threats and high-risk targets. Crews of ships in harbors need to evaluate each new port and determine possible terrorist threats. Crew members must be aware of host-nation support and responsibilities while in port or anchored in foreign waters. The ship's captain is solely responsible for the ship and all those embarked. As a minimum, the captain:

a. Establishes methods of embarkation and/or debarkation and patrol activities for all personnel.

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

c. Coordinates above and below waterline responsibilities.

d. Establishes a weapons and/or ammunition policy and rules of engagement (ROE), appoints a reaction force; e.g., Security Alert Force (SAF), Backup Alert Force (BAF), Reserve Force (RF).

e. Drills all personnel involved.

8. 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 and while en route, and determine weapons and ammunition policies. Special considerations include the following topics:

a. 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.

b. 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 require close coordination. Maintain an open communications net between all elements until the aircraft is loaded and reestablish communications upon arrival.

c. 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.

d. [redacted]

9. Patrolling

Units outside the United States may be called upon to conduct patrols in urban or rural environments. Individuals or small groups assigned to various Defense agencies overseas may also be called upon to assist or advise host governments on security matters. 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. Patrols support police operations, expand the area of influence, gather information, help maintain order at clubs and restaurants, detain individuals as required, conduct hasty searches, and emplace hasty roadblocks. Patrols must understand the rules of engagement (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, observation posts (OPs), host nation assets and reaction forces provide additional support.

10. Roadblocks

a. There are two types of roadblocks: deliberate and hasty.

b. Deliberate roadblocks are permanent or semi-permanent roadblocks used on borders, outskirts of cities, or the edge of controlled areas. [redacted]

c. Use hasty roadblocks to spot check. [redacted] 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.

d. 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.

11. Observation Posts (OPs)

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 occupation and withdrawal of an OP by normal operations (e.g., house searches, roadblocks, patrols to leave people behind), flooding an area with patrols to disguise movement, using civilian vehicles and/or clothes, and using deception. Any compromise of an OP location should be reported immediately.

12. Civil Disturbances

a. 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.

b. Riot control aims to restore order with minimum use of force. [redacted]

[redacted]

13. 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. Refer to Chapter 16 for procedures to be followed in handling bomb situations.

14. Individual Protective Measures

Overseas deployments require implementation of individual protective measures. [redacted] 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.

C. TACTICAL FORCE PROTECTION

During unified, joint and combined operations U.S. units, bases, and contractor support personnel and facilities in the joint rear area (JRA) are still vulnerable to terrorist attacks. The same procedures identified in the preceding paragraphs and in preceding chapters of this handbook apply. Commanders will be advised by the Joint Rear Area Operations Commander (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 the Joint Chiefs of Staff, Joint Pub. 3-10, "Doctrine for Joint Rear Area Operations" (reference (ll).

D. SUMMARY

1. This chapter has illustrated the incorporation of combatting terrorism protective measures drawn from installation, facilities, and personal protection measures discussed earlier in this handbook into combatting terrorism plans and programs for military units as they are deployed for or as they become part of expeditionary forces. The fundamental principles of combatting terrorism remain unchanged:

   a. Avoid Routines.

   b. Maintain a Low Profile.

   c. Be Sensitive to Changes in the Security Atmosphere or Environment.

2. This Handbook has presented courses of action that apply these principles to individuals; the principles also apply to military units as well.

CHAPTER 19

SPECIAL CONSIDERATIONS

A. OVERVIEW

1. No discussion of efforts by the Department of Defense to combat terrorism would be complete without at least some discussion of two important DoD functions:

a. Public affairs.

b. Acquisition.

2. DoD combatting terrorism policies and programs depend heavily on DoD and Service public affairs officers for dissemination, interpretation, and feedback. The entire acquisition community, from RDT&E activities to procurement, to maintenance and logistics, must evaluate its activities to ensure DoD personnel, facilities, and materiel are not made victims of terrorist attack. The responsibility of acquisition executives and their representatives--contracting officers and contracting officers' technical representatives--for antiterrorism efforts do not end at the Department of Defense boundary.

3. In addition to these topics, there still remains one last element in the DoD Combatting Terrorism Program concept introduced in Chapter 1 to be discussed. This Handbook will therefore conclude with a brief discussion of the concept and methods of operations security as part of the DoD Combatting Terrorism Program.

B. ANTITERRORISM AND DoD PUBLIC AFFAIRS

1. General Public Affairs AT Responsibilities

a. All DoD activities strive to fulfill the DoD goal of providing as much information to the public about the DoD activities as possible, consistent with the requirements of operations security, technology security, and information security. DoD's approach to the provision of information on its combatting terrorism efforts is no different.[1]

---

1 Multiple DoD issuances govern the dissemination of information from DoD to the general public. Among those most relevant to antiterrorism related public affairs activities are the following:

DoD Directive 5230.9 (reference (mm));

DoD Directive 5410.1 (reference (nn)); and

DoD Directive 5105.35 (reference (oo)). (cont'd)

b. However, unlike many public affairs activities, the audience for DoD public information on antiterrorism efforts is composed of as many members of the DoD community as the general public at large. Indeed, DoD public affairs officers have a special, prominent role to play in the DoD Combatting Terrorism Program.

c. All DoD installations, facilities, organizations, and commands should have an ongoing program intended to reduce its risk and vulnerability to terrorist attack. A Public Affairs Annex should be developed in support of all Major Command and Unified or Specified Command Operations Plans. Installation commanders and heads of DoD agencies should develop an antiterrorism public affairs plan as well.

d. Detailed public affairs guidance, specific for dealing with incidents on DoD facilities is provided in Appendix BB.

2. Combatting Terrorism Public Affairs Plan

a. There are four objectives for the Combatting Terrorism Public Affairs Plan:

(1) Increase awareness of DoD-affiliated personnel and their dependents of the threat of terrorism and assist security, intelligence, counterintelligence, and law enforcement organizations by providing information about measures to reduce risk of terrorist attack;

(2) Maintain good communications with the surrounding communities. [redacted] Public affairs programs should also provide feedback about the community's attitude towards and understanding of the DoD Combatting Terrorism Program;

(3) Provide timely, accurate, and authoritative information on terrorist attacks to counter rumors or inaccurate news stories about terrorist accomplishments; and

(4) Provide authoritative information to news media representatives in the event of a terrorist incident, consistent with guidance provided by the on-scene U.S. Government official in charge, DoD policies, and specific guidance issued by the senior DoD officer responsible for DoD Components on scene.

In addition, the following DoD Directives address specific public affairs issues associated with nuclear weapons or incidents allegedly involving nuclear materials. The guidance on dissemination of information found in these directives may be helpful in dealing with other terrorist incidents of significant drama:

DoD Directive 3150.5 (reference (pp));

DoD Directive 5230.16 (reference (qq)); and

DoD Manual 5100.52-M (reference (rr)).

b. The news media may interview DoD officials, commanders, senior leaders, and knowledgeable individuals. DoD interviewees are allowed to discuss the general subject of antiterrorism as it pertains to their areas of responsibility.

c. The Office of the Assistant Secretary of Defense for Public Affairs (OASD(PA)) approves all requests for media coverage of antiterrorist training exercises on a case-by-case basis. OASD(PA) also approves in-house photos of antiterrorist training forwarded through PA channels before release.

d. In response to queries regarding a possible or actual terrorist threat at a particular base, installation, or activity, the PAO may acknowledge increased security generally. PAOs may comment more specifically on those security measures taken that can be readily observed. For example, the PAO may acknowledge increased gate guards or additional patrols, if obvious to the public. PAOs should, however, exercise care and prudent judgement in discussing these or other security measures which have been or will be implemented.

3. Planning Considerations

a. Public affairs planning for antiterrorist actions must include numerous considerations:

(1) The information needs of all audiences such as military personnel, DoD civilian employees, host-nation employees, their family members, news media, and local civilians.

(2) The current OSD public affairs policies regarding release of combatting terrorism information.

(3) The deterrent value of releasing information about security measures versus the possibility that releasing this information could benefit terrorists.

(4) The severity of the local terrorist threat and the tactics and techniques used.

(5) The identities of the terrorist leaders and other groups involved.

(6) The balance between releasing too little and too much information. [redacted]

b. No matter how detailed, complete, and aggressively promoted, the Department of Defense's combatting terrorism and antiterrorism education, training, and exercises may not prevent a terrorist attack. Such an attack, however, may be more difficult for the terrorists to launch and may result in fewer casualties.

4. Terrorist Incident Response: Public Affairs Role

a. Once a DoD installation, activity, organization, or senior person is attacked, the PAO participates in the response implementing the Crisis Management Plan discussed earlier in this Handbook.

b. The Public Affairs Incident Response Plan to support response to terrorist acts committed on DoD installations or against DoD personnel must be developed to support both the DoD Operations Plan and the needs of the media. It should include as much detail regarding news media and public affairs crisis operations as can be determined in advance. General considerations of how to handle issues with respect to the observing, filming, and reporting of a terrorist incident and its aftermath should be carefully considered. Among the key elements are:

(1) Identify the senior U.S. Government representatives and their agencies who will be responsible for managing an incident.

(2) Identify senior state, municipal, and local authorities (as well as host government representatives and their agencies, if overseas) who will be responsible for managing an incident.

(3) Identify the lead PAO organization which may assume responsibility for organizing and managing public affairs matters in an incident.

(4) Identify the PAO representative who will be assigned duty in the emergency operations center.

(5) Determine potential locations for the press center and the resources needed to quickly put it into operation.

(6) Establish controls to limit media access to the scene of the incident.

(7) Establish rules governing photography of the incident and interviews with personnel involved.

(8) Determine the frequency of press briefings.

(9) Determine the responsibilities and relationships of all agencies involved.

(10) Establish coordination of information for release.

c. Once the Public Affairs Incident Response Plan is developed, the PAO should coordinate it with installation, Service, DoD, other Federal, local, state, and host government staff elements who may be involved in its execution.

d. The Public Affairs Office should participate when combatting terrorism exercises are conducted. PA staff teaches all participants what to expect and how to react in a real-life situation. Exercises also provide the PAO an opportunity to solidify his position as part of the crisis management team and demonstrate how an effective PA operation can support the mission.

e. PAOs must know what their organizations or units will do in response to a terrorist incident. They must know the roles and responsibilities of the other involved governmental agencies and how these agencies interface. They must also know the circumstances under which territorial responsibilities transfer from one agency to another.

f. [redacted]

[redacted] The local PAO is the initial release authority. He and/or she will handle the situation as a criminal incident until it is determined to be a terrorist act.

g. [redacted] In such a case, that agency assumes the lead for PA activities, and the PAO will act in a support role. The primary Federal Agencies that may assume responsibility for resolving terrorist incidents are:

(1) [redacted];

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

h. [redacted] Although the local DoD Public Affairs Officer may be viewed as the spokesperson, the OASD(PA) is the sole spokesperson for DoD whenever such forces are deployed. OASD(PA) will provide guidance to the local PAO. Basic guidance covers the following situations.

a. [redacted]

b. [redacted]

c. [redacted]

[redacted]

d. The senior Service PAO will continue to serve as the release authority for information about the Service-specific involvement in the incident.

e. All information for release will be coordinated with all the agencies involved.

6. Incident Management: PAO Objectives

The major objectives of DoD Public Affairs Officers dealing with a terrorist incident and its immediate aftermath are as follows:

a. Identifying and reporting terrorist incidents as criminal acts unworthy of public support.

b. Protecting information concerning possible reactions of law enforcement agencies.

c. Providing accurate and timely information to the news media to minimize speculation and dispel the inevitable rumors that spread during any such situation.

d. Preventing the terrorists from using DoD assets to manipulate the media and achieve their goal of massive publicity.

e. Preventing members of the media from interfering with or influencing operations in response to the incident.

f. Preventing information about the preparation and deployment of Special Response Teams, Hostage Rescue Teams, or other DoD units being released through PA channels.

g. Ensuring, to the maximum extent possible, that all **official** information originates from a single source, thereby reducing the possibility of compromising key information and of releasing conflicting or inconsistent information.

7. PAO Role in DoD Combatting Terrorism Program

a. Public Affairs Officers can play a major role in the DoD Combatting Terrorism Program. They are educators, making audiences within and outside DoD aware of the threat of terrorism. They are communicators, explaining to DoD personnel, their dependents, and the communities in which DoD components are present, the measures taken to reduce their risk and vulnerability to terrorist attack. They are "pollsters," taking the pulse of the community and reporting back to the DoD components the concerns and

fears of the community generated by DoD presence and/or DoD activities in their communities and the risks of terrorist attack that may ensue.

b. The challenge facing PAOs from the terrorist threat is great. To succeed in their mission, PAOs must exercise constant vigilance and sensitivity to the needs of their audiences. [redacted] In making information available to the news media, PAOs must delicately balance the legitimate information requirements of their DoD and civilian audiences against the intelligence requirements of the terrorists. PAOs must constantly coordinate with other members of the installation, activity, organization, or command staff.

C. ACQUISITION AND DoD COMBATTING TERRORISM PROGRAMS

1. No part of DoD is immune from the risk of terrorist attack. The vulnerability of the entire DoD acquisition system, from RDT&E laboratories, to production facilities, to key transportation routes, to logistic bases and supply points, are all potential targets waiting to be struck by one terrorist group or another. Furthermore, from the perspective of many terrorists, there is little difference between installations or activities owned, operated, and manned by DoD civilian personnel, military personnel, or contractor personnel.

2. [redacted]

a. Key Assets Protection Program

(1) E.O. 12656 (reference (ss)) requires that each U.S. Government department and agency assess the vulnerability of facilities critical to the national defense. Not only must the program analyze facility vulnerability, it must develop plans to ensure the continued operation of critical facilities in time of national security emergency. The Federal Emergency Management Agency (FEMA) coordinates compliance by all Federal agencies, including the Department of Defense.

(2) DoD Directive 5160.54 (reference (bb)) implements the Executive Order within the Department of Defense. KAPP sets forth a planning process that results in the development of military plans to support civil law enforcement efforts to physically secure certain facilities identified as "Key Assets." Key Assets are industrial and infrastructure facilities that are not owned by the Department of Defense, but are essential for the Department of Defense in mobilizing, deploying and sustaining military forces in a crisis or war. [redacted] KAPP supplements, and does not diminish, DoD command responsibilities to protect DoD-owned facilities.

b. Key Asset List Nominations

[redacted]

[redacted] identifying "critical" or "essential" infrastructure is difficult. Acquisition executives and their designees should consult with their parent Services to determine whether or not contractors participating in their specific acquisition programs have had facilities listed on the Service Critical Industries List. After identifying key industrial facilities, it is then possible to determine the irreplaceable commercial and public infrastructures that support the key asset. These infrastructures, too, may require protection in addition to the key industrial asset.

(2) Acquisition and logistics executives in the Services and DoD Agencies, as well as their contracting officers and contracting officer's technical representatives, identify potential DoD Key Assets. Those nominations are forwarded through the heads of DoD components to the Commander-in-Chief, Forces Command (CINCFOR). CINCFOR coordinates KAPP as an Executive Agency for the Secretary of Defense.

(3) Other U.S. Government agencies may also nominate contractor facilities, public utilities, or other public assets for inclusion on the Key Assets List (KAL). Nominations may be made through FEMA in accordance with the DoD-FEMA MOU.

c. Key Asset Protection Plans

(1) Once a facility, utility, or other public asset has been placed on the Key Assets List, CINCFOR notifies the Army National Guard State Area Command (STARC) headquarters in each state of the presence of a DoD Key Asset. [redacted]

(2) A Physical Security Plan (KA-PSP) is prepared for each identified Key Asset. Each KA-PSP has two major parts supported by annexes as appropriate. The specific plans are classified and are not usually available to state Governors and their immediate civil staffs. The existence of KA-PSPs is not classified; the STARCs brief their state government counterparts to maintain awareness of the KAPP plans.

(3) Part I of the KA-PSP deals with protection requirements necessary for each installation. It discusses specialized equipment needs, security force size and composition, and security force training.

(4) Part II of the KA-PSP addresses specific remedies to security deficiencies to be undertaken if the PSP is implemented. The first section of Part II deals with expedient measures that can be taken at the direction of the Task Force Commander within the first 24 to 48 hours of arrival on scene to redress the most pressing security problems. The second section of Part II addresses more involved measures to be implemented by the Army Corps of Engineers or security contractor staff to implement a complete, physical security enhancement package.

(5) Key assets located adjacent to navigable waters may require the development and implementation of an annex to the Physical Security Plan prepared by the Coast Guard to address issues of waterside security.

(6) For purposes of physical security planning, Key Assets are divided into two classes:

a Simple Assets, consisting of small facilities, few buildings, covering six acres of land or less; and

b Complex Assets, consisting of large facilities, multiple buildings, and complex production paths.

(7) The STARC staffs undertake vulnerability analyses of DoD Key Assets in their respective states with the assistance of personnel from the Defense Investigative Service and the Army Corps of Engineers as needed. DIS and Army Corps of Engineers undertake assessment of Complex Assets; the STARCs tackle Simple Assets, obtaining Corps of Engineer review to ensure the completeness of vulnerability analysis scope.

(8) The primary focus of these vulnerability analyses is the potential harm to Key Assets that might result from wartime sabotage. However, these assessments apply to peacetime terrorist attacks against Key Assets. After all, the methods of attack, weapons of attack, and the degree of harm to the facility, its surrounding environment, and the ability of DoD to perform missions and execute assigned functions might be equal from the perspective of a Combatant Commander and his subordinate Service acquisition or logistics chain of command.

(9) The purpose of KAPP is to ensure continued operation of the Key Asset in the face of any threat. STARC-prepared physical security plans represent a major line of defense for DoD Key Assets in the event of an outbreak of domestic and/or international terrorism. Cooperation with private sector and state or local governments is essential in order to obtain access to facilities or adjacent areas to ensure proper physical protection of DoD Key Assets.

d. KAPP Crisis Response Capabilities

(1) KAPP planners benefit from close working relations among the CINCFOR, military intelligence, and FBI intelligence staffs. As a result, KAPP receives threat information and participates in DoD terrorist threat warning systems.

(2) KAPP war plans can be implemented only on the order of the President or the Secretary of Defense in time of a declared national security emergency or war. The general physical security assessments and judgments of consequences resulting from an attack on a Key Asset developed by each STARC are available to each Governor and his state's National Guard. This general information is provided to support state and local law enforcement agencies should a Governor elect to implement selected KAPP plans on his or her own authority. If authorized by the President, specific plans could hasten the use of federal forces to respond to a Governor's request for federal assistance. Such assistance could be provided under terms of the DoD-DoJ MOU on military assistance in support of efforts to control civil disturbances.

e. Antiterrorism Measures and DoD Industrial Security Practices

(1) DoD contracting officers (COs) and their technical representatives (COTRs) should review the risk of terrorist attack on contractor facilities, personnel, or

materiel. They should also assess the consequences for the Department of Defense of such attacks. They should also consider the criticality of contractor facilities, personnel, materiel, and supporting public and/or commercial infrastructure. If their assessment leads to the conclusion that a mission critical or mission essential facility, person, or materiel exists, then strong consideration should be given to nominating the facility to the DoD Key Assets List.

(2) In order to make more informed judgments, COs and COTRs are encouraged to discuss their concerns with the Service Acquisition Executive or his designee, as well as Service representatives responsible for preparation and maintenance of the Civil Industries List.

(3) Once COs or COTRs nominate industrial facilities to the DoD Key Assets List, they should meet with the contractors' management to discuss the implications of this nomination. [redacted]

(4) One of the benefits contractors receive as a result of their facilities being nominated to the DoD Key Assets List is a report or briefing describing the results of the physical security survey. Since the survey focuses predominantly on levels of threat that exceed the current environment, most of the recommendations will be targeted towards remedies to problems anticipated in that extreme, stressful environment. Some of the solutions identified may have relevance or application in the near term.

(5) Those DoD contractors performing work under terms of a DoD Industrial Security Agreement are required to develop emergency plans to ensure proper protection of all classified information, materiel, and equipment. Contracting Officers and their COTRs should work closely with the Defense Investigative Service to ensure that such plans are developed, tested, and refined. Those facilities which are Key Asset List nominee and performing DoD work under a DoD Industrial Security Agreement should be examined with special care.

f. Key Asset Protection Program and the DoD Combatting Terrorism Program

(1) The DoD Key Asset Protection Program was conceived to heighten awareness and build plans to protect the defense industrial base from enemy special operations forces and saboteurs during times of war. The highly integrated, specialized economy of the United States in general, and the DoD industrial base in particular, has increased the vulnerability of DoD to terrorist acts within the United States. Attacks on telephone networks, electric grids, highway, rail, and waterway facilities during a crisis could substantially limit the ability of DoD to move personnel and materiel. Attacks on DoD contractor facilities could substantially affect the ability of deployed forces to continue operations.

(2) KAPP therefore can play a vital role in preserving DoD's capabilities in the face of the terrorist threat. While KAPP is far from glamorous, it is a small but important facet in the DoD's efforts to protect our forces in peacetime. In doing so, KAPP helps ensure no matter what missions are assigned by the National Command Authorities, the Department of Defense can deploy and sustain operations for the duration of the mission.

D. OPERATIONS SECURITY AND DoD COMBATTING TERRORISM EFFORTS

1. [redacted]

2. [redacted]

3. [redacted]

4. Terrorists hold much of the initiative in their attacks on DoD personnel, facilities, and assets. In large measure, DoD assets are fixed targets; they operate within relatively predictable patterns described in terms of geography, time, and space. Specific targets among DoD assets are discernible. [redacted]

5. [redacted] This Handbook has therefore addressed specific measures designed to frustrate the collection of detailed intelligence necessary and sufficient to translate a general intention to attack American targets into specific acts against DoD assets. The key recommendations stressed throughout are the foundation of combatting terrorism OPSEC for DoD personnel:

a. Avoid routines.

b. Be sensitive to changes in the security atmosphere.

c. Be prepared for unexpected events.

6. This Handbook has identified a variety of measures that if implemented will help DoD-affiliated personnel avoid establishing routines. These measures range from practices at work, to practices in transit, to practices at home.

7. This Handbook has described indicators of potential terrorist violence in the atmosphere or environment around an installation.

8. This Handbook has outlined a wide variety of measures that can be taken to ensure the ability of individuals and the DoD Components to respond to unexpected events.

9. At the outset of Chapter 2, it was noted that terrorists in general, and the terrorist leadership cadre in particular, are not usually psychopaths, sociopaths, or "crazy." They are determined, highly motivated individuals prepared to employ force and violence as tools to achieve their goals and objectives. In this respect, they resemble adversary military forces.

10. [redacted]

CHAPTER 20

TERRORIST USE OF WEAPONS OF MASS DESTRUCTION (WMD)

A. PURPOSE

This chapter provides an overview of the potential use of weapons of mass destruction (WMD) by terrorists and broad guidance implementing DoDI 2000 STANDARDS 31, 32, and 33.

B. DEFINITIONS

1. Biological Agent: A microorganism that causes disease in personnel, animals, or plants, or causes the deterioration of material.

2. Chemical Agent: A chemical substance which is intended for use in military operations to kill, seriously injure, or incapacitate personnel through its physiological effects.

3. Nuclear Weapon: A complete weapon assembly in its intended ultimate configuration which is capable of producing the intended nuclear reaction and release of energy.

4. Radiological Material: Radioactive material usually found in research, industrial, or medical applications or radioactive waste from such operations.

5. Toxin Agent: A poison formed as a specific secretion product in the metabolism of a plant or animal organism as distinguished from an inorganic poison. Such poisons can also be manufactured by synthetic processes.

6. Weapons of Mass Destruction: Biological and chemical agents or material, plant and animal toxins, radiological material, and nuclear devices used as weapons against personnel, animals, plants, material, or facilities.

C. CHALLENGES

1. [redacted] Previous concerns regarding WMD use focused on battlefield employment against warned and protected military personnel. The threat has expanded in recent years as terrorist organizations have grown in sophistication and now have the ability to acquire and employ WMD. This growing threat now means units must plan for the possible use of WMD against peacetime forces and noncombatants. In 1995, President Clinton signed Presidential Decision Directive 39, U.S. Policy on Counterterrorism, underscoring the nations concern regarding possible terrorist use of WMD. In this document, the President states:

> The United States shall give the highest priority to developing effective capabilities to detect, prevent, defeat, and manage the consequences of nuclear, biological, or chemical (NBC) materials or weapons use by terrorists.

2. Several recent events have demonstrated the reality of terrorist acquisition and employment of all types of WMD. [redacted] The following examples highlight a few cases that serve to illustrate the growing concern over terrorist use of WMD:

a. **Biological Agents**:

(1) The only documented use of a biological agent in the US occurred in Oregon in 1984. Two followers of the Rajneesh Bagwhan produced and dispensed salmonella bacterium in the salad bars of local restaurants for the purpose of impacting the outcome of a local election. A total of 715 people were infected and required treatment; fortunately no deaths were caused as a result of the attack. Had a more lethal agent been employed, the consequence would have been much more severe. The attack occurred without any advance indicators of the capability or intent of the cult to use such tactics.

(2) In 1995, the FBI confiscated samples of plague bacteria from a white supremacist group. A member of the group posed as a researcher who requested and received three freeze dried samples of the plague from a commercial lab. The material was recovered by the FBI and the member was arrested and convicted.

b. **Toxins**:

(1) In 1992, the FBI arrested four members of the Patriots Council, an anti-government group based in Minnesota, for manufacturing the toxin "ricin" from castor beans. The group intended to use ricin to kill a Deputy US Marshall who had served them with papers for tax violations. The members were the first persons convicted under the Biological Weapons Antiterrorism Act of 1989.

(2) In 1995, the Canadian Customs Service detained a US citizen attempting to enter Canada from Alaska. The Canadians confiscated 130 grams of a white powder later confirmed to be ricin. The individual was suspected of being affiliated with white supremacist groups operating in Arkansas.

c. **Chemical Agents**:

(1) The 1993 World Trade Center bombing may also have been an unsuccessful chemical attack. Traces of sodium cyanide were found in the van containing 1200 pounds of explosives. The terrorist group responsible for the bombing was very interested in chemical and biological weapons and possessed several manuals describing their manufacture and use. They had also threatened the Philippine government with a chemical attack in an effort to secure the release of jailed members in that country.

(2) The 1995 Tokyo subway attack by the Aum Shinrikyo cult is the most well known example of a terrorist organization using WMD. Approximately ten liters of the non-persistent nerve agent Sarin were placed in vinyl bags on trains on three different subway lines and resulted in 12 fatalities and over 5000 casualties. An important aspect of this attack is the unplanned and unprotected response by first responder personnel. A total of 1,364 firefighters responded to the attack and 135 were among the injured after becoming exposed to the agent, either directly or indirectly.

d. **Radiological Material**:

(1) In 1987, Brazilian thieves took a package containing Cesium 137 and later abandoned the material. It took ten days to recover the radioactive material. Before the radioactive source could be found, a total of 244 victims were contaminated--resulting in 4 fatalities and 54 hospitalizations. These casualties were the result of inadvertent exposures. Had terrorists obtained the material and used it in a deliberate manner, the results would have been far more severe.

(2) In 1995, a Chechen insurgent leader threatened to turn Moscow into an eternal desert. The Chechen rebel planted a small amount of Cesium 137 in a container in a Moscow park. The material was recovered and would have posed a significant hazard if it would have dispersed with an explosive charge.

D. CONSIDERATIONS

1. **WMD Threat**. As the previous examples demonstrate, the use of WMD has grown in number and lethality in the past 15 years. Many different types of groups and organizations have determined that acquiring and using WMD may further their cause. Para-military groups, antigovernment organizations, political splinter groups, religious cults, and terrorist organizations have all attempted to use some type of WMD against US interests or those of our allies.

2. **WMD Planning Considerations**. Existing military doctrine addresses the use of NBC weapons and their effects on personnel and facilities. Planning factors for battlefield use of these weapons may have direct application when planning for terrorist use of WMD. A list of current publications that address NBC weapons, their effects, and planning factors is at References. Table 20-1 summarizes planning considerations in existing doctrinal publications on the use of nuclear, biological, and chemical weapons. Section H contains factors that address planning considerations for possible terrorist use of WMD.

[redacted]

Table 20-1. Doctrinal NBC Planning Considerations

3. **Chemical Agents**: The traditional categories of chemical agents includes: blister agents, nerve agents, blood agents, and choking/respiratory agents. These agents have been studied extensively and their physical properties, medical effects and treatment, and employment options are well documented in military doctrinal publications. It is important to remember that most military planning concerns large scale use of the weapons against troops in a tactical environment. [redacted] Table 20-2 lists some of the most common military chemical agents and their properties.

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 20-2. Examples of Chemical Agents

a. While much is known about these categories of chemical agents, terrorists are also capable of using a wide variety of industrial chemicals and non standard agents. [redacted] To minimize the uncertainty of these situations, a thorough assessment of the range of possible threat agents and potential vulnerabilities is essential.

b. For any type of chemical agent attack, procedures must be in place to allow for the rapid recognition and warning of the incident.. Unlike biological agents, chemical agent exposure generally results in the sudden onset of symptoms. Emergency response and medical personnel should be thoroughly trained in the recognition of symptoms and the treatment of agent casualties. Unless chemical agent detectors are in use prior to the attack, detection and identification of the agent will be done by first responders to the attack or while treating casualties at the scene.

4. **Biological Agents**: A major problem posed by biological weapons is the lag from employment to the time of detection. Most of the biological agents have an incubation period of one to seven days before the onset of symptoms. Potential agents such as anthrax, cholera, plague, tularemia, and viral hemorrhagic fevers (Ebola virus, Lassa fever, Yellow fever, etc.) have delayed symptoms following initial exposure. The lag from use until detection has the potential to allow for widespread contamination and the dispersion of affected personnel across a very large area. [redacted]

a. [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

b. Two key factors that help mitigate the effects of a potential biological agent attack are a comprehensive vaccination policy and the active medical support program. [redacted] it is important to involve medical personnel in assessing the threat from indigenous diseases and establishing an active preventive medicine program. In contrast to naturally occurring diseases in

which incidence of the disease increase slowly over a period of weeks or months, a deliberate biological attack will peak in a few days. Timely identification and communication of the attack is essential in treating and controlling the disease and limiting the effect on personnel.

c. Preventive medicine services will be in great demand upon the onset of an attack. [redacted] Preventive medicine specialists will be required to assist commanders with identifying safe food and water sources and in determining when to use treatment, immunization, and other preventive measures. Preventive medicine personnel must be continually aware of the biological threat in the areas in order to update their data base on diseases, potential vectors, and the susceptibility of troops to diseases.

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 20-3. Example Biological Agents

5. **Toxins**: These agents are a relatively new threat [redacted] As with biological agents, medical personnel must provide assistance in identifying and treating personnel that are exposed to toxin agents. Botulinum toxin and ricin are two types of agents that are in the toxin category. [redacted]

[redacted]

a. Toxins are defined as any toxic substance of natural origin produced by animal, plant, or microbe. They are non-volatile and tend to be more toxic than chemical agents. For example, botulinum toxin is 15,000 times more lethal than nerve agent GB. Their lack of volatility means that they would not be a persistent battlefield threat and would not likely be spread by secondary or person- to- person exposures.

b. For toxins, incapacitation, as well as lethality, must be considered. Several toxins cause significant illness at levels much lower than the level required for lethality and are militarily significant in their ability to incapacitate military force and civilian populations. [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 20-4. Possible Toxin Agents

6. **Radiological Materials**: [redacted] Nuclear research facilities, nuclear reactors, medical research and treatment centers, and construction engineering activities are all potential sources of radioactive material. [redacted] Equipment to detect radiation is available to most units. [redacted] Radiation, regardless of its intensity, has the potential to produce harmful effects on unprotected personnel. Effects may be the result of external exposure to a radioactive source or inhalation or ingestion of radioactive particles.

7. Recent events have forced a greater awareness of the vulnerability of US personnel and facilities to attack from terrorist elements, both in the US and abroad. The suddenness and severity of the attacks has reinforced the need to anticipate and plan for the threat and consequence of terrorist attacks against US personnel. The remainder of this chapter addresses the standards to assist in the analysis, planning, crisis management, and consequence management of the possible use of WMD by terrorist organizations.

E. Potential Threat of Terrorist Use of Weapons of Mass Destruction (Supports DoD Standard 30)

1. The potentially devastating effects of terrorist use of WMD mandates that organizations conduct a thorough analysis of the threat in their AOR. [redacted] The unique aspects of the terrorist threat to acquire and employ WMD should be considered as a distinct element of the overall threat assessment.

2. Combatant commanders should ensure an integrated collection and analysis program is established that draws detailed threat data from all available sources. The use of integrated terrorist threat estimates is discussed in Chapter 6, para 6E. Deployed forces should also establish close relationships with diplomatic missions and supporting country teams within their AOR; they are an excellent source of information on the political and psychological background of local terrorist organizations.

3. Collection plans should address the Essential Elements of Information (EEI) of the terrorist capability to acquire and use of WMD. EEI should be integrated into subordinate elements' collection plans and reviewed as new or evolving threats emerge. The plan should consider terrorist threats from commercial, industrial and medical source material as well as the traditional military nuclear, biological and chemical weapons and agents.

4. New or changing terrorist capability to acquire or employ WMD must be rapidly disseminated through command channels. Units should include procedures for immediate reporting of changing terrorist threats or actual use of WMD. Notification should be sent through chains of command, lines of authority, intelligence agencies and similar organizations. As appropriate, it must also be passed to diplomatic missions or local US authorities to assist them in their preparation and response for a potential incident.

F. Vulnerability Assessments for Terrorist Use of WMD (Supports DoD Standard #31)

1. Organizations will assess the vulnerability of installations, facilities, and personnel in their AOR to terrorist use of WMD. Vulnerability assessments will be based on the threat assessments derived from DoD Standard #30 and on the principles of vulnerability assessments discussed in Chapter 6, para 6C.

2. As a minimum, assessments should include information from intelligence, logistics, medical, physical security, facility engineering, meteorological, explosive ordnance disposal, and NBC staff elements. The entire range of potential terrorist WMD use should be considered when conducting assessments. As previously mentioned, threats from commercial chemical, biological, nuclear, and radiological sources should be included as well as traditional military agents. [redacted]

a. Individual protective clothing and equipment,

b. Collective protection equipment and facilities,

c. Medical response and emergency services capability,

d. Training of personnel,

e. Physical security and protective barriers,

f. Facility design and construction,

g. Early warning and detection,

h. Alarms and attack warning,

i. Threat Intelligence,

j. Sustainment operations and follow on support,

k. Preventive medicine and vaccination programs,

l. Storage of bulk hazardous material, and

m. Explosive ordnance disposal response capability/availability.

G. Mitigation of Terrorist Use of WMD (Supports DoD Standard #32)

1. Units will take appropriate measures to protect personnel and facilities and reduce their vulnerability to terrorist use of WMD. Mitigating the consequences of the actual terrorist use of a WMD is critical to reducing the loss of life and property. This includes actions taken prior to use as well as actions taken subsequent to the attack. Actions may be physical improvements such as installing an integrated large area siren and warning system, or procedural improvements such as exercising and validating the WMD emergency response annex or plan.

2. Commanders should develop a plan to address the threat a WMD and exercise the plan to determine effectiveness in mitigating the effects of an attack. In addition to providing crisis action and consequence management procedures, planning should include pre-attack measures and consideration for the collateral damage a WMD may have on adjacent facilities and surrounding communities. Plans should provide sufficient detail to permit organizations to rapidly recognize and respond to any terrorist event using WMD.

3. Chapter 15 contains detailed crisis planning and execution guidelines for dealing with a terrorist incident. In addition to the items contained in Table 20-1, the following contains additional planning considerations that should be included in addressing terrorist use of WMD:

a. **Commander's estimate of the potential for use of WMD**: This forms the basis for all facts and assumptions that drive the planning and preparation for any use of WMD by potential threat organizations. As such, the commander's estimate is the cornerstone of any successful program and must be reviewed frequently to incorporate any new or emerging threats.

b. **Type/number of threats**: Accurate identification of the WMD threats posed by terrorist organizations provide a mechanism to determine the resources needed to counter the threat and respond effectively if they are used. Planners should also factor in the magnitude and diversity of the threats throughout an AOR.

c. **Most likely/most vulnerable targets**: [redacted] identification of the most likely and vulnerable targets enables more detailed planning, which then drives responsible organizations to improve security measures. Further, responsible organizations can take measures to improve the security for these areas.

d. **Target Value Analysis**: Certain areas pose different challenges from those above due to their specific value to terrorists. These targets may not be mission related or of high military value, but their value to terrorists may be very high. [redacted] This analysis must be conducted by fusing all available sources of information on the terrorist organization.

e. **Coordination with local authorities**: Coordination with local authorities is essential when planning for terrorist WMD use. It is likely that an attack on either the DoD facility or the local civilian populace will affect both communities. [redacted] Thorough coordination between DoD organizations and local officials provides a means to improve the response time and offers the opportunity to share critical resources needed to mitigate the effects of an attack.

f. **Attack recognition and agent characterization**: [redacted] Agent identification will probably be done by first responders or medical personnel. Planning must address this potential vulnerability and incorporate procedures that minimize the delay from attack initiation until detection.

g. **Warning systems**: Because WMD attacks can cover large areas, timely warning can reduce the number of personnel who would otherwise be exposed to agent effects. A combination of outdoor warning sirens, telephonic notification, and broadcast announcements provide redundant warning systems that will reach a large portion of the population. Special consideration should be given to unique populations, such as the visually or hearing impaired, to ensure effective warning systems are in place to provide for their safety.

h. **Response levels**: Different agents require different responses. Plans should include details on the appropriate response for the agents identified in commander's assessment and the equipment needed to implement that level of response.

i. **Hazardous Material Response Teams**: Host nation, federal, state and local regulations have specific requirements for personnel responding to hazardous material and substances. Commanders must be aware of these requirements and emergency responders must have the equipment and training necessary to protect themselves, treat casualties and decontaminate the site. Planning should include adequate time and resources to ensure response teams have the appropriate equipment and level of training.

j. **Reporting procedures**: Because of the sensitivity of terrorist use of WMD, many agencies require formatted reports on the nature of the event. Plans should include pre-formatted templates for reporting requirements and message addresses and phone numbers for the agencies and commands that must be notified. [redacted] Brevity codes, established crisis action [redacted]res and predetermined local reporting requirements will all assist in the management of a crisis by providing timely and accurate information to the emergency operations center.

k. **Crisis action team responsibilities**: Emergency operations centers normally have only a small staff on duty and will require immediate augmentation when an attack occurs. Staff elements should be fully trained and prepared to implement the appropriate plan to reduce the effects of the WMD attack. It may be necessary to operate in protective equipment during the initial stages of the crisis. Training on the use of protective equipment and their specific duties as part of the emergency operations center staff should be regularly exercised to maintain proficiency in crisis action responsibilities.

l. **First responder responsibilities**: First responders will be called on to perform many critical functions during a WMD attack. [redacted] Careful planning and training is needed to address the special needs of these groups. The actions they take during the initial stages of an event will have a very important impact on the consequence management steps that follow.

m. **Medical support, treatment and transportation requirements**: As discussed earlier, pre- and post-attack medical planning is crucial. Prior coordination with host nation, state and local medical facilities is necessary to ensure medical plans include procedures to treat and care for contaminated or infected personnel. Medical teams require special training in the treatment and handling of contaminated casualties and remains. Medical facilities should have areas designated to treat and segregate contaminated patients. Preventive

medicine specialists and pathologists need to have a data base of naturally occurring diseases and procedures to quickly assess and identify suspicious illnesses and diseases. Antidotes and treatments for potential agents from commercial or industrial sources should be considered in the casualty management plan. Contaminated patient transport and contamination control measures should be incorporated into litter and ambulance operations.

n. **Evacuation routes and care centers**: There will always be a requirement to clear an area and provide orderly evacuation to safe areas when WMD is used. Evacuation routes, safe areas, and care centers should be identified during the planning process. Law enforcement and security personnel need to determine traffic control points to facilitate evacuation and prevent personnel from entering potentially contaminated areas. Copies of the routes and locations of care centers should be available to installation workers and residents.

o. **Public affairs**: The demand for information from the public and the media will be intense at the onset of an event. Public affairs planning should include background information on the potential agents and materials that pose a threat. Basic information on the properties, effects, treatment, duration, and decontamination of likely threat agents should be included in the public affairs reference materials brought to the emergency operations center and joint information center. Rapid and accurate information on the hazard during the early stages of an event will assist in protecting civilians from hazard and foster confidence in DoD's ability to safely manage the crisis.

p. **Crime scene procedures for agent material**: Terrorist use of any WMD material is a criminal act. Local plans should include procedures to control a crime scene in a contaminated environment and provide for the recovery of evidence that may be hazardous. For domestic events, the FBI will be responsible for investigating the criminal incident. Law enforcement and security plans should provide procedures to facilitate the transition of responsibility when the FBI arrives on site. Overseas facilities should include similar procedures that are required under host nation or status of forces agreements.

q. **Follow on assistance**: Any WMD event will generate the requirement for some form of external support or assistance. Plans should determine the type, amount and time frame for follow-on assistance. The logistics of managing a large contingent of external support organizations has the potential of overwhelming the ability of the local commander to control its effective employment.

r. **Hazard prediction**: When an event occurs, there is an immediate need to predict the size of the potential hazard zone. Reports from first responders will contain the location of the incident site; but the initial estimate of the hazard area should be made by emergency operations center personnel. Procedures should be incorporated into emergency operations centers that allow for a quick initial hazard prediction and methods for its rapid dissemination. Detailed predictions can be made when more information is provided on the agent type and dissemination means.

s. **Meteorological support**: As indicated above, hazard prediction must be done quickly. Current and reliable weather data is critical to providing accurate hazard predictions. Updated weather data should be routinely provided to emergency operations centers so that it is available at the onset of an event. Organizations providing data should be part of the planning process so they can develop weather products that support hazard prediction models or programs.

t. **Contamination control**: Containing and limiting the spread of contamination is essential in reducing the effects of a WMD attack. Procedures for personnel responding to the attack site should include methods that minimize their direct contact with contaminated material. [redacted] Access into the site should be through designated points and along designated routes.

u. **Decontamination and hot line operations**: Decontamination procedures should be developed using the resources locally available. Decontaminating exposed personnel, first responders, and site work teams requires the rapid establishment of a decontamination site. Plans should consider the requirement to maintain decontamination operations for extended periods and the potentially large personnel and logistics need generated to support this type of operation.

v. **Sampling and analysis**: Sampling will be required at the attack site and in the predicted hazard areas to establish the presence or absence of contamination. Plans should include procedures to determine sampling requirements and protocols for the collection of agent material. Analysis of samples may be done locally at the onset of an attack, but may be shipped off-site for confirmation or for detailed analysis if local facilities cannot identify the material.

w. **Monitoring operations**: Monitoring plans should include procedures to employ detection equipment to known or suspected hazard locations. Detection equipment intended for military tactical level employment

does not detect agent concentrations that are considered hazardous by the EPA and the Occupational Safety and Health Administration. Environmental and safety planners must be aware of the hazardous material exposure limits for civilian populations and understand the limitations of using military equipment to determine when areas are considered free of contamination.

x. **Reentry and remediation operations**: Preliminary planning should address the considerations for these operations. Reentry includes actions required to permit personnel to safely enter an area following an attack. Remediation includes actions to remove all contamination from the site and restore the environment to its original condition. Both of these processes can potentially take several days to weeks to complete. External support will probably be needed to ensure these tasks are properly accomplished.

4. Training programs should provide a comprehensive approach to meeting the needs identified in mitigation efforts. Actions required to reduce the vulnerability to attack and to respond as the result of a terrorist WMD incident involve many different tasks and levels of training. At a minimum, training programs should include individual, first responder, functional response team, and emergency operations center training.

H. Mitigation and Consequence Management Guidelines to Assist in Planning For Terrorist Use of WMD

1. Pre-deployment and garrison operations.

a. **Command, control, communications, computers, and intelligence (C4I):**

Review and update operational plans based on probable threats.

b. **Active defense:**

Gather intelligence on potential terrorist capability.
Identify essential elements of enemy information on terrorist capability.

c. **Detection and Identification:**

Gather meteorological data for area of operations.
Gather intelligence regarding terrorist WMD capabilities.
Conduct refresher training on all detection equipment.

Identify threats that require laboratory analysis for identification.
Develop specific identification techniques and acquire materials to conduct analysis.

d. **Hazard prediction, warning, and reporting:**

Conduct training for all personnel in the warning and reporting chain.
Exercise the warning and reporting system and communications nets.
Identify hazard prediction models and exercise procedures.

e. **Reconnaissance, survey, and monitoring:**

Develop sample collection, packaging, transportation, documentation, and analysis procedures.
Conduct training for reconnaissance and survey teams.
Identify laboratory locations to support agent identification.

f. **Individual Protection:**

Conduct training for individual defensive procedures and equipment use.
Issue individual equipment as appropriate.
Stockpile replacement items.

g. **Collective protection:**

Identify and quantify requirements.
Conduct operational checks of on-hand equipment.
Stockpile replacement items.

h. **Medical:**

Conduct medical threat analysis.
Provide medical input to medical force development planning.
Train in medical aspects of WMD defense.
Review medical logistics support.
Implement vaccination policy.
Review individual procedures for hygiene in a contaminated environment.
Review individual and collective procedures for general defense by

medical units against WMD.

i. **Contamination control:**

Identify assets and rehearse procedures.

j. **Logistics:**

Review planning factors for operations in contaminated environment.
Identify resources to support sustained operations in contaminated environment.

2. Pre-attack procedures.

a. **C4I:**

Pre-plan for WMD event.
Issue mission orders and directives.
Activate WMD reporting chain.
Order appropriate WMD protective actions and posture.
Enforce counter-surveillance measures.
Coordinate with local civilian or host nation governments.

b. **Active defense:**

Allocate resources to active defense mission.
Monitor terrorist offensive actions.
Disrupt terrorist planning cycle and C4I means.

c. **Detection and identification:**

Conduct routine background analysis and periodic monitoring.
Conduct refresher training for detector operators.
Position detectors.

d. **Warning and reporting:**

Conduct refresher training in WMD warning and reporting.
Initiate and maintain disease and non-battle injury reporting system.

e. **Reconnaissance, survey, and monitoring:**

Position assets.
Stockpile sample collection and transportation equipment.
Stockpile agent identification equipment.
Conduct routine sampling in accordance IAW the threat and detector capabilities.

f. **Individual protection:**

Implement unit standard operating procedures for WMD operations.
Adopt protective level appropriate to the threat.
Prepare to take additional protective measures when warned of possible or actual attack.

g. **Collective protection:**

Post sentries on entrance to collective protection shelters.
Adopt increasingly defensive posture in line with threat level.

h. **Medical:**

Provide medical input to Commander's estimate of the threat.
Review and promulgate medical treatment protocols.
Identify specialist medical teams.

i. **Contamination control:**

Identify water sources and decontamination solutions.
Position equipment and supplies.

j. **Logistics:**

Confirm availability of equipment and supplies for operations in a contaminated environment.
Identify host nation, federal, state, or local resources that may be available to augment unit assets.

3. **Actions during attack.**

a. **C4I:**

Transmit appropriate reports.
Synthesize attack information.
Notify local/host nation government.

b. **Active defense:**

Disrupt terrorist delivery systems.

c. **Detection and identification:**

Collect samples.
Coordinate and analyze intelligence, meteorological, medical, and detector system input.
Prepare and forward samples to lab for further analysis and identification.
Conduct downwind hazard analysis and disseminate predictions.

d. **Warning and reporting:**

Implement warning and reporting procedures.
Report and forward evidence of attack to command, medical and law enforcement authorities.
Make and disseminate alarm/protective action decisions.

e. **Reconnaissance, survey and monitoring:**

Implement collection and survey plans.
Collect any aerosol, environmental, plant/animal, and medical samples.
Report results of field surveys and monitoring efforts.

f. **Individual protection:**

Implement appropriate protection for personnel.
Implement evacuation plans for non-essential personnel and civilians.
Provide resupply of expended items and contaminated equipment.

g. **Collective protection:**

Activate collective protection shelters for key assets.
Maintain strict control over access to collective protection shelters.

h. **Medical:**

Initiate treatment of contaminated casualties.
Confirm detection system results.
Characterize agents.
Monitor outbreaks.
Maintain integrity of medical collective protection.

i. **Contamination control:**

Determine extent of attack location.
Control access to site and establish designated routes to and from the area.
Have first responders attempt to provide hasty decon of the known hazard area.
Implement decontamination plan.

j. **Logistics:**

Issue replacement items.
Replace expended supplies and contaminated items.

4. Post-attack actions.

a. **C4I:**

Assess result of terrorist attack.
Assess terrorist intention for any further attacks.
Ensure continued operation of WMD warning and reporting system.
Update threat based on latest attack information.
Order implementation of specific post-attack control measures.
Identify resource and capability shortfalls.

b. **Active defense:**

Target any residual capability.

Execute appropriate military response.

c. **Detection and identification:**

Relocate detectors to any predicted agent locations.
Continue sampling and monitoring until agent levels are below permissible exposure levels.

d. **Warning and reporting:**

Disseminate decisions on protection, hazard avoidance, and countermeasures.
Collect and forward casualty and disease reports.
Continue to report unexplained illnesses or agent symptoms.

e. **Reconnaissance, survey and monitoring:**

Identify contaminated areas for environmental remediation.
Continue to collect samples to verify initial results.
Provide agent samples to law enforcement authorities.

f. **Individual protection:**

Initiate controlled down dressing for protected personnel.
Redistribute supplies of individual equipment.

g. **Collective protection:**

Decontaminate as necessary.
Replace filters.

h. **Medical:**

Implement strict field hygiene measures.
Review treatment protocols and agent symptoms.
Characterize outbreaks.
Deploy specialist teams.
Institute quarantine as necessary.
Document and treat casualties.
Analyze and distribute medical intelligence.
Ensure medical protective measures for follow-on support is complete.

Ensure safety of food and water supplies.

i. **Contamination Control:**

Restrict movements of personnel and equipment into the hazard zone.
Establish multiple sites to speed the decontamination of personnel as appropriate.

j. **Logistics:**

Replenish contingency stocks.
Reissue decontaminated equipment.
Review accuracy of planning factors.

I. SPECIFIC WMD REFERENCES

1. Department of Defense: "Handbook of DoD Assets and Capabilities for Response to a Nuclear, Biological, or Chemical Incident"

2. Joint: Joint Publication 3-11, "Joint Doctrine for Nuclear, Biological and Chemical (NBC) Defense"

3. Multi-Service:

a. FM 3-6 / AFM 105-7 / FMFM 7-11H "Field Behavior of Chemical Agents"

b. FM 3-10-1 / NWP 18-1 AFM 355-4 / FMFM 7-11 "Chemical Weapons Employment"

c. FM 8-285 / NAVMED P-541 / AFM 160-11 / "Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries"

4. Army:

a. FM 3-3, "Chemical and Biological Contamination Avoidance"

b. FM3-3-1, "Nuclear Defense"

c. FM 3-4, "NBC Protection"

d. FM 3-5, "NBC Decontamination"

e. FM 3-7, "NBC Handbook"

f. FM 3-100, "NBC Defense, Chemical Warfare, and Smoke and Flame Operations"

g. FM 8-10, "Health Service Support in a Theater of Operations"

h. FM 8-10-7, "Health Service Support in a Nuclear, Biological, and Chemical Environment"

5. Navy

a. NSTM, Chapter 070, "Shipboard Radiological Defense"

b. NSTM, Chapter 470, "Shipboard BW/CW Defense and Countermeasures"

c. NBC, "Warfare Defense Ashore"

6. Marine

a. MCWP 3-37.2, "NBC Protection"

b. MCWP 3-37.3, "NBC Decontamination"

c. MCWP 3-37, "MAGTF NBC Defense"

d. MCWP 3-37.2A, "Chemical and Biological Contamination Avoidance"

e. MCWP 3-37.2B, "Nuclear Contamination Avoidance"

f. MCWP 3-37.4, "NBC Reconnaissance"

7. Air Force

a. AFR 355-1, "Disaster Preparedness and Planning Operations"

b. AFR 355-3, "Air Force Personnel Shelter Programs"

c. AFR 355-8, "Mission Oriented Protective Posture"

J. WEAPONS OF MASS DESTRUCTION CHAPTER SUMMARY

1. [redacted] The range of potential agents and weapons includes previously known military sources and unconventional attacks using materials from industrial and medical sources.

2. Existing doctrine provides useful information that assists in planning for defense against possible use of WMD by terrorists, [redacted] units must expand their planning process and actively seek information on terrorist intent and capabilities in their AOR.

3. [redacted] thorough planning by supporting staffs is essential in identifying procedures and resources necessary for detection, warning, and response to terrorist use of WMD. It is especially important for medical support staffs to be integrated into the planning process to establish medical support considerations for planning and conducting operations to mitigate the effect of WMD use.

APPENDIX A

SELECTED TERRORIST INCIDENTS AGAINST DoD-AFFILIATED PERSONNEL AND INSTALLATIONS IN PUERTO RICO AND ABROAD, 1972-1991

INTRODUCTION

The following summary of selected terrorist incidents against DoD-affiliated personnel and installations was prepared from previously published Department of Defense, Department of State, and FBI summaries of domestic and international terrorist incidents. This summary is provided to illustrate the wide variety of attacks to which DoD-affiliated personnel and facilities may be subjected.

Date (Year-Month-Day)	Event
72-05	Red Army Faction members carried out 6 separate bombing attacks in which 1 was killed and 13 were injured at a U.S. officers' club in Frankfurt; 3 were killed and 5 wounded in a blast at the U.S. Army European Command Headquarters in Heidelberg.
74-04	Members of the New People's Army of the Philippines Communist Party murdered three U.S. Naval personnel near Subic Bay Naval Base.
75-06	Members of the Popular Struggle Front kidnapped a U.S. Army colonel in Beirut and turned him over to the Popular Front for the Liberation of Palestine General Command after food was delivered to Palestinian refugee camps in Beirut.
75-11	Members of the Greek terrorist group, Revolutionary Popular Struggle (ELA), fire-bombed the U.S. Air Force Commissary in Athens.
76-06	Revolutionary Cells members were credited with a bomb attack on U.S. Army V Corps Headquarters in Frankfurt, Germany, in which 16 personnel were injured.
76-12	Members of the terrorist group, Revolutionary Cells, were blamed for a bomb attack on the U.S. Air Force Officers' Club at Rhein Main Air Base. Seven personnel were injured in the blast.
78-01	A U.S. Air Force truck was bombed in Istanbul, Turkey.
78-01-09	Cars belonging to two U.S. Navy personnel were firebombed in Nea Makri, Greece.
78-01-25	During an ambush of a U.S. Air Force truck, an airman was wounded in the vicinity of Izmir, Turkey.
78-02-14	Approximately 200 armed urban guerrillas attacked the U.S. Embassy and held U.S. Ambassador William B. Sullivan and 101 members of the Embassy staff for more than 2 hours in Tehran, Iran.
78-02-18	Car belonging to a school teacher at the DoD Dependent School was firebombed in Athens, Greece.
78-04-16	A DoD communications facility was fired upon in the vicinity of Pirinclik, Turkey.
78-05-31	A bomb explosion damaged the U.S. Air Force transient family quarters in Ankara, Turkey.
78-05-31	A bomb explosion damaged a U.S. Army hotel in Wiesbaden, Germany.
78-09-16	A man hurled two Molotov cocktails in front of the U.S. Marine Corps Headquarters at Camp Butler, Okinawa, Japan. The devices failed to detonate.
78-09-16	A machine gun attack was made at dawn on the U.S. Embassy by the Popular Liberation Forces in San Salvador, El Salvador.

Date (Year-Month-Day)	Event
78-10-15	A U.S. Air Force depot was attacked by machine-gun fire and robbed of weapons in Izmir, Turkey.
78-11-30	The apartment of a U.S. military member was bombed, resulting in the wounding of two personnel in Tehran, Iran.
78-12-30	U.S. Army Team House was robbed and burned in Mashad, Iran.
79-01-28	A U.S. Air Force officer was shot and wounded as he was returning to his home in Tehran, Iran.
79-01-30	NATO's Allied Forces Southern Command compound was firebombed in Naples, Italy.
79-0[illegible]	Unknown people poured kerosene on the rear portion of a U.S. Army officer's Jeep Wagoneer parked in front of his residence and set it on fire in Tehran, Iran.
79-02-20	Unidentified individuals fired from a passing car at the Izmir apartment of a U.S. serviceman attached to the Southeast NATO Headquarters in Izmir, Turkey.
79-02-28	Two U.S. Navy shore patrol vehicles were firebombed in Naples, Italy.
79-03-12	U.S. Air Force motor pool, the APO building, and the military exchange office were damaged by an explosion and firebombing in Izmir, Turkey.
79-04-12	Three masked men firing pistols from a stolen automobile killed a U.S. serviceman and wounded another before speeding off down a side street. The leftist Turkish People's Liberation, after spending 8 years underground, claimed credit for the attack in Izmir, Turkey.
79-05-01	A bomb exploded at the Marine Security Guard Residence in Bogota, Colombia. Damage was extreme. Four U.S. Marines and two Colombians were injured.
79-05-11	A U.S. Army soldier was killed and two others were wounded by a machinegun attack at a bus stop in Istanbul, Turkey.
79-06-25	RAF members attempted to assassinate General Alexander Haig, Supreme Allied Commander, NATO, with a bomb concealed under a bridge in Obourg, Belgium. The bomb exploded between General Haig's car and an escort vehicle. Two guards were wounded in the attack.
79-07-25	Police raided a First of October Group of Anti-Fascist Resistance (GRAPO) safehouse and found plans to kidnap or kill a high-ranking U.S. Air Force officer in the Royal Oaks Military Housing Community in Madrid, Spain.
79-09-16	A U.S. Army soldier was wounded by an explosion at an Army barracks in West Berlin, Germany.
79-10-30	About 300 leftists employing small arms attempted to take over the U.S. Embassy located in San Salvador, El Salvador. Two U.S. Marine Guards were slightly wounded.
79-11-24	A Puerto Rican terrorist group claimed credit for a night bombing at two Chicago, Illinois, military recruiting offices and the Naval Armory. No injuries were reported.
79-12-03	Two sailors were killed and 10 others injured when a U.S. Navy school bus carrying 13 enlisted men and 5 enlisted women was ambushed by Puerto Rican terrorists at 6:45 a.m. in the vicinity of Sabana Seca, Puerto Rico.
79-12-14	A U.S. Army soldier and three DoD contractors were shot to death in an ambush near their suburban Istanbul, Turkey homes as they were arriving home from work at the Cakmakli Military Base at 5:40 p.m.
80-02-11	A U.S. Army officer's car was damaged by arson near Vicenz, Italy.
80-03	Members of the terrorist group, Macheteros, fired on a U.S. Navy bus in Puerto Rico, killing two.
80-03-12	A Puerto Rican Popular Army terrorist shot at a government car carrying three Army ROTC instructors in San Juan, Puerto Rico. Minor injuries were sustained.

Date (Year-Month-Day)	Event
80-04-16	Three Turkish terrorists shot and killed a U.S. Navy chief petty officer and a Turkish friend as they left the petty officer's apartment to get into his vehicle in Istanbul, Turkey.
80-05-31	The NATO Rod and Gun Club was damaged by an explosion in Izmir, Turkey. No injuries were reported. The Revolutionary Way claimed responsibility.
80-07-31	Unidentified terrorists fire-bombed the first floor apartment of an Air Force staff sergeant. Two bombs were thrown. The second one struck the sergeant, causing second and third-degree burns. The attack took place in Izmir, Turkey.
80-09-26	Five U.S. Air Force members were among 213 persons injured by a bomb detonated at the Oktoberfest festival in Munich, Germany.
80-10-04	Two U.S. Naval personnel were among ten persons injured by bombs that exploded at six hotels and a theater in Manila, Philippines.
80-11-07	A pipe bomb, thrown over the perimeter fence, exploded on the roof of a civil engineering building at a U.S. military base in Ankara, Turkey. No injuries were reported.
80-11-15	A U.S. Air Force member was killed while another escaped injury in a terrorist attack at a U.S. Air Force facility in the vicinity of Adana, Turkey.
80-11-22	Two firebombs were thrown into a U.S. Army compound causing minor damage in Esslingen, Germany.
81-01	Terrorists belonging to Macheteros destroyed eight aircraft and damaged two others in a carefully executed multiple bombing attack on the Puerto Rican Air National Guard airfield. Damage was estimated to be $40 million.
81-02-02	Two incendiary devices were discovered inside two LOH-58 helicopters at the U.S. Army Airfield near Beudingen, West Germany.
81-03-15	Three U.S. Marines were wounded in a rocket attack on an embassy vehicle in San Jose, Costa Rica.
81-03-25	Puerto Rican National Guard soldier was wounded in an assassination attempt in Ponce, Puerto Rico.
81-04-12	A U.S. military train on the Bremen-Hannover, West Germany, line was halted by a cable that had been placed over the rail electrification wiring.
81-04-25	A U.S. Air Force member was wounded by a lone gunman near the Incirlik, Turkey, Air Base.
81-06-17	A bomb at the NATO Arms Depot in Wahrendahl, West Germany (17 miles southwest of Hanover), exploded and caused approximately $130,000 damage to a facility under construction. No injuries were reported.
81-08	Red Army Faction members bombed the U.S. Air Force headquarters in Ramstein, Germany, injuring 18 Americans and 2 Germans.
81-08-08	Two, and possibility four, men armed with automatic weapons opened fire on a U.S. Air Force pickup truck, but none of the truck's occupants was injured. The attack took place in the vicinity of Malatya City, Turkey.
81-08-31	A large car bomb exploded in the parking lot at U.S. Air Force Europe Headquarters, Ramstein Air Base, West Germany, injuring twenty people, including two senior U.S. Air Force officers.
81-09-01	Arsonists destroyed seven automobiles belonging to U.S. military personnel in an American housing complex in Wiesbaden, West Germany. No injuries occurred.
81-09-15	Red Army Faction members credited with an attack on U.S. Army European Commanding General Kroessen's car with two RPG-7 grenades. The General and his wife were slightly injured.

Date (Year-Month-Day)	Event
81-09-23	Members of the terrorist group, Lorenzo Zelaya Popular Revolutionary Forces (FPR-LZ), ambushed five members of a U.S. Mobile Training Team; they also exploded a time bomb on the second floor of the Honduran National Assembly building.
81-10-06	Egyptian soldiers assassinated Egyptian President Anwar Sadat as he was observing a parade outside Cairo, Egypt. Three U.S. military officers observing the parade were wounded.
81-10-21	Two unidentified persons, challenged by military police in the vicinity of military housing, opened fire on the MPs with a hand gun. The MPs returned fire and the individuals fled. No one was wounded.
81-11-27	A military policeman was shot and wounded at Fort Buchanan near San Juan, Puerto Rico.
81-12-07	Unidentified attackers threw a bomb through the window of the U.S. Army unit commander's office near Kassel, West Germany. Only the detonator of the bomb (a fire extinguisher packed with explosives) exploded and injured two soldiers.
81-12-17	Red Brigades members kidnapped U.S. Army Brigadier General James Dozier from his home in Verona, Italy. He was held for 42 days until freed in a rescue operation by Italian counterterrorist forces.
82-01-18	Terrorists belonging to the Lebanese Armed Revolutionary Faction (LARF) murdered Assistant U.S. Army Attache, LTC Charles Ray, while he stood on a Paris sidewalk.
82-04-17	An assistant U.S. Army attache was wounded by small arms fire as she drove in the vicinity of the Beirut, Lebanon, port area.
82-05	Macheteros terrorists killed one sailor and wounded three others in an ambush outside a San Juan nightclub.
82-05-16	One U.S. sailor was killed and three were wounded in an ambush by the Macheteros in the vicinity of San Juan, Puerto Rico.
82-05-21	A bomb exploded at Hellenikon Airbase, Greece, damaging the dairy plant inside the base. No injuries were reported.
82-06-01	Revolutionary Cells members were blamed for a bicycle bomb delivered to a U.S. Army communications center in Frankfurt. The bomb was detonated, but no casualties were reported.
82-07-02	A bomb exploded between two vans used by a computer data processing unit of the U.S. Army, but no injuries were reported. Revolutionary Cells claimed responsibility for the bombing, which took place in Frankfurt, West Germany.
82-08-12	A small bomb exploded in a U.S. military housing area in Frankfurt, West Germany, damaging a car. No injuries were reported.
82-10-09	A device exploded under a van belonging to a U.S. Army soldier, destroying it and causing minor damage to four other vehicles and windows in an adjacent building in Frankfurt, West Germany.
82-10-19	An incendiary device damaged two cars in the U.S. military leased housing area in Frankfurt, West Germany.
82-10-31	A bomb exploded in the Dulles Housing Area in Giessen, West Germany. The bomb, which had been placed under a vehicle in the parking lot, damaged approximately 15 vehicles and shattered windows in adjoining apartment buildings. There were no injuries.
82-12-13	A fire extinguisher-type bomb attached to the car of a U.S. Army soldier exploded outside of Butzbach, West Germany. The soldier received second and third degree burns and internal injuries.

Date (Year-Month-Day)	Event
82-12-14	A U.S. Army soldier entered his car and discovered a fire extinguisher-type bomb behind the driver's seat in the vicinity of Fechenheim, West Germany. The device, which contained approximately 4 lb of explosives connected to a pressure fuse, did not detonate.
82-12-15	A U.S. Army officer was injured on entering his car near Cambrat Fritsch Kaserne, near Darmstadt, West Germany, when he detonated a bomb.
82-12-28	A van assigned to U.S. NATO forces was set on fire while it was parked on the street in Ostia, Italy.
83-04	Hizballah members committed a suicide car bomb attack on the U.S. Embassy in Beirut. The operation was acknowledged by Islamic Jihad. Forty-nine persons were killed and 120 were wounded.
83-10	Suicidal terrorists drove two trucks carrying explosives into the U.S. and French military barracks in Beirut. 241 U.S. Marines and 46 French military personnel were killed. Islamic Jihad claimed responsibility.
83-11	Terrorists belonging to 17 November assassinated Navy Captain George Tsantes and his driver in Athens, Greece.
84-02	Red Brigades claimed responsibility for the assassination of Leamon Hunt, Director General, Multinational Force and Observers, responsible for monitoring the peace accord between Egypt and Israel.
84-06	Revolutionary Cells was identified as the organization responsible for the bombing of a NATO fuel pipeline near Lorch in Baden-Wurttemberg.
84-12	Combatant Communist Cells terrorists claim credit for simultaneous bombings along NATO fuel pipeline, forcing temporary shutdown in operations.
84-12	Members of the Popular Forces 25 April (FP-25) claim credit for a four-round mortar attack on NATO's Iberian Atlantic Command Headquarters near Lisbon. A car and several buildings were damaged in the attack.
84-12	A U.S. military office building was bombed in Duesseldorf. Members of the Terrorist Group, Revolutionary Cells, were thought to be responsible.
85-01	Combatant Communist Cells members claim responsibility for bombing at NATO support facility in suburban Brussels in which two American military policemen were injured.
85-01	Terrorists belonging to the Popular Forces 25 April (FP-25) fired three mortar rounds at NATO ships anchored in Lisbon harbor. None were hit.
85-01	Red Army Faction Members firebombed the U.S. airfield at Heidelberg.
85-06	Hizballah terrorists hijacked TWA flight 847 en route to Athens from Beirut. U.S. Navy diver, Petty Officer Robert Stethem, was murdered by the hijackers. 39 U.S. citizens were held hostage in Beirut for 17 days.
85-08	Red Army Faction claimed responsibility for a car bomb detonated at Rhein Main Air Base. The bomb killed two and injured 17. In addition, the terrorists killed an off-duty U.S. serviceman the night before the attack and used his military identification to gain access to the base.
85-11	Macheteros claimed responsibility for an attack on a U.S. Army recruiting officer in an ambush while he was on his way to work.
86-04	Red Army Faction was credited with a bomb attack on the NATO fuel pipeline near Vollersode.
86-05	Red Army Faction was blamed for an attack on a U.S. military fuel pumping station. In addition to the damage to the pumping station, the bomb destroyed two fuel trucks and initiated a fire that consumed more than 1000 gallons of fuel.

Date (Year-Month-Day)	Event
86-10	Explosives were discovered at several military and military-related facilities throughout Puerto Rico.
86-11	Macheteros members were believed responsible for a bomb discovered in the National Guard Building in Old San Juan, Puerto Rico.
86-12	Macheteros terrorists were believed to be responsible for a bomb that destroyed a vehicle in the National Guard Center at Yauco, Puerto Rico.
87-09	Members of the Greek terrorist group, Revolutionary Popular Struggle (ELA), firebombed the U.S. Air Force Commissary in Athens.
87-10	Terrorists belonging to the New People's Army (NPA) murdered two American servicemen, an American retiree, and a Filipino bystander outside Clark Air Base in the Philippines.
88-02	Hizballah members kidnapped United Nations Military Observer Lt. Col. Richard Higgins, USMC. In July, 1989, Higgins videotaped remains were aired; his remains were returned to the United States in 1991.
88-04	Japanese Red Army members were held responsible for a bomb that was placed in front of the U.S. servicemen's club in Naples, Italy. The bomb blast killed five people, including a U.S. servicewoman. Two JRA members were the main suspects in the bombing that coincided with the anniversary of the U.S. raid on Libya in 1986.
89-02-19	A bus carrying U.S. military personnel near Comayagua, Honduras, was hit by a bomb blast, injuring three U.S. military and two Honduran civilians. The Morazanist Patriotic Front (FPM) claimed responsibility.
89-06-19	An improvised explosive device detonated early in the morning at the Puerto Rico Army National Guard Recruitment Center, in Bayamon. The explosive device had been placed in the front doorjamb. The blast caused damaged to the exterior of the building, shattering a plate glass window and door. No injuries or loss of life occurred. EPB-Macheteros claimed responsibility.
89-09-26	The New People's Army killed two U.S. civilian Department of Defense contractors in their vehicle north of Clark Air Base, apparently timed to coincide with the arrival of the U.S. Vice President in Manila, Philippines.
89-10-22	Revolutionary Popular Struggle firebombed three cars belonging to U.S. Air Force personnel in Athens, Greece. The next day, an incendiary device was found under another airman's car.
90-02	The anticapitalist Antiestablishment Struggle Organization claimed responsibility for the firebombing of a U.S. Air Force vehicle in Patras, Greece.
90-03-02	An unidentified assailant threw a grenade into the My Place nightclub in Panama City, Panama. One U.S. soldier was killed; several others were injured. An eyewitness reported that the suspect shouted "Viva Noriega" before throwing the device and then escaping in a nearby vehicle. Responsibility for the attack was claimed by two previously unknown groups, The Organization for the Liberation of Panama and the M-20. Both groups were believed to be comprised of Noriega loyalists.
90-03-31	A bus carrying 28 off-duty U.S. Air Force personnel was attacked by unidentified gunmen in the vicinity of Amarteca, Honduras. Seven airmen were wounded in the ambush, two of whom required hospitalization in Tegucigalpa. The troops, who were assigned to Soto Cano Air Base, were attacked as they returned from a recreational outing at the port city of Tela. Responsibility for the attack was later claimed by the Morazanist Front for the Liberation of Honduras (FMLH).
90-05-13	The New People's Army, the military wing of the Community party of the Philippines was responsible for the slaying of two U.S. airmen near Clark Air Base and may have been responsible for the assassination of a Marine sergeant earlier in the month.

Date (Year-Month-Day)	Event
90-05-27	On May 27, 1990, an unknown number of individuals cut through a chain-link fence surrounding the Puerto Rican Army National Guard (PRANG) compound at Mayaguez, Puerto Rico. They set fire to two PRANG trucks, which resulted in the destruction of one vehicle and considerable damage to the other. No claims of responsibility were made.
90-08	Radicals threw more than 50 firebombs at the rear door of a U.S. Army office in Seoul, causing minor damage.
90-10-18	Six U.S. crewmen from the U.S.S. Saratoga were attacked by 12-14 students from the Technical University who were armed with sticks and clubs. One crewman was reported injured. The only identifiable word spoken by the attackers was "Saratoga." According to press reports, the attackers burned a cardboard American flag and shouted "damn American imperialism."
90-11-03	At 11:50 p.m., a bomb went off outside a restaurant in Vina Del Mar, Chile, injuring eight people including 3 personnel from the U.S.S. Abraham Lincoln. Responsibility for the incident was claimed by the Manuel Rodriguez Patriotic Front (FPMR).
90-11-10	At approximately 6 p.m., five to six youths threw two bottles at a Turkish bus transporting U.S. naval personnel from the Guzelbache dock to Izmir, Turkey. At the time of the attack, the aircraft carrier U.S.S. Kennedy and the cruiser U.S.S. Gates were in port. The following day, leaflets were found in the parking lot of an apartment building occupied primarily by U.S. military personnel, as well as on the windshield of some 10 cars (with foreign civilian license plates) parked in the lot. The leaflets read: "Yankee go home, condemn American Imperialism," and were signed by a heretofore unknown group called Socialist Youth.
91-01-02	Two U.S. crewmen, Lt. Col. David Pickett and crew chief PFC Earnest Dawson, were executed after their helicopter was downed by Farabundo Marti National Liberation Front (FMLN) militants in Canton San Francisco, El Salvador. A third American, Chief Warrant Officer Daniel Scott, died of injuries he received when the helicopter was shot down.
91-01-04	FMLN guerrillas fired upon a team of American military personnel in Canton San Francisco, El Salvador, who were investigating the deaths of the three U.S. airmen lost in the January 2 downing of a U.S. aircraft.
91-01-13	An unknown individual poured flammable liquid on the rear of a car owned by a U.S. citizen at Incirlik Air Base, Adana, Turkey, and set it on fire.
91-01-20	A molotov cocktail was thrown onto the street of an American housing area in Osterholz-Scharmbeck, Germany. No damage or injuries occurred.
91-01-21	An incendiary device was placed inside the car of an American soldier in Luebberstedt, Germany. The car was parked in an American housing complex at the time. Only minor damage and no injuries occurred.
91-01-21	The U.S. Military Traffic Management Command Outpost (MTMC) in Istanbul, Turkey, was severely damaged following detonation of a bomb.
91-01-29	A bomb exploded outside the U.S. military's engineering warehouse in Izmir, Turkey, causing extensive damage to a number of cars, one of which belonged to a U.S. serviceman.
91-01-29	Unknown individuals poured flammable liquid on three vehicles owned by U.S. military personnel, in Ankara, Turkey, casing extensive damage to two of the three cars and minor damage to the third.
91-02-07	Dev Sol shot and killed a U.S. civilian contractor Bobbie Mozelle, as he was getting into his car to travel to work at Incirlik Air Base in Adana, Turkey.

Date (Year-Month-Day)	Event
91-02-16	Terrorist members of the Manuel Rodriguez Patriotic Front/Dissidents (FPMR/D) attacked an armored U.S. Embassy van with a light antitank weapon (LAW) and automatic weapons fire in Santiago, Chile. A. U.S. Embassy Marine security guard was injured by flying Plexiglass from the van.
91-02-21	A bomb exploded on the U.S.-Spanish pipeline near Cordoba, Spain. The pipeline supports U.S. Air Force operations at Moran Zarragoza and Torrejon Air Base. The explosion caused minor damage and no injuries.
91-02-23	Chukaku-ha attacked a U.S. Navy housing compound in Yokohama, Japan, with projectiles, causing minor damage.
91-02-27	Three cars belonging to American personnel assigned to San Vito Dei Normani Air Base near Brindisi, Italy, were set afire. The cars were parked in a residential area where many of the base personnel live. All the cars had U.S. Forces' registration license plates.
91-02-28	Two Dev Sol gunmen shot and wounded a U.S. Air Force officer as he entered his residence in Izmir, Turkey.
91-03-12	U.S. Air Force Sergeant Ronald Odell Stewart was killed by a remote control bomb detonated at the entrance of his apartment building in Athens, Greece. The Revolutionary Organization 17 November claimed the attack was in response to "the genocide of 13,000 Iraqis."
91-03-22	Three members of Dev Sol assassinated John Gandy, a U.S. civilian contractor, in his Istanbul, Turkey, office.
91-03-28	Three U.S. Marines were shot at and injured by an Arab individual while driving near Camp Three, Jubial, Saudi Arabia.
91-04-13	An estimated 100 students from nearby Dankuk University attempted to block the road in front of Hannam Viallage, a U.S. military residential compound, in Seoul, Korea. The students scattered anti-U.S. leaflets and threw firebombs before being dispersed by police.
91-04-25	About 50 radical students attacked the two-story U.S. Army Engineering Corps building in downtown Seoul, Korea.
91-05-04	A small group of students staged several random anti-U.S. attacks outside the Lotte Hotel in Seoul, South Korea, where a U.S. military group was holding a social gathering. Students used rocks to break windows of a U.S. military vehicle that was approaching the hotel, injuring the driver. Other U.S. military personnel were physically accosted. Two U.S. military buses waiting in the parking lots incurred broken windows during the disturbance.
91-05-17	An estimated 400 students threw firebombs toward Hannam Village, a U.S. military housing compound in downtown Seoul, Korea.
91-06-05	Six U.S. military instructors training Colombian marines on three Bost Whaler craft on the Magdalena and Sogomoso Rivers, Colombia, came under hostile fire.
91-06-18	An explosive device was discovered about 15 feet from the side of an apartment building in Lima, Peru, housing both the chief of the U.S. Embassy's Military Assistance Advisory Group (MAAG) and the MAAG's senior U.S. Army representative. The device consisted of five kilograms of anfo and 500 grams of dynamite.
91-10-28	U.S. Air Force Staff Sergeant Victor Marvick was killed and his wife was injured when a bomb placed underneath their pickup truck exploded near Ankara, Turkey.

Date (Year-Month-Day)	Event
91-12-06	Unknown individuals threw molotov cocktails at a building that houses U.S. military personnel and their families in Ansbach, Germany. Minor damage and no injuries occurred in the attack.
91-12-08	A privately owned vehicle of a U.S. Naval officer was set ablaze and destroyed during the early morning hours while parked at the officer's residence on the Yokosuka Naval Base, Japan.
91-10-28	Two car bombings killed a U.S. Air Force sergeant and severely wounded an Egyptian diplomat in Turkey. Turkish Islamic Jihad claimed responsibility.
91-10-29	A rocket struck the edge of the U.S. Embassy in Beirut, Lebanon. There were no injuries.
91-12-22	The remains of American hostage Col. William R. Higgins were recovered and flown back to the United States for burial at Quantico National Cemetery.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

DoD COMBATTING TERRORISM-RELATED ISSUANCES

A. GENERAL

[redacted] Most DoD issuances are supported by Service, DoD Agency, or CINC documents containing specific implementation measures appropriate for each DoD component or activity. The following table identifies key DoD issuances which direct, regulate, or provide supplementary guidance bearing on the organization, development, formulation, implementation, and oversight of activities comprising the DoD Combatting Terrorism Program.

B. TABLE NOTES

1. The following comments are intended to aid interpretation of the table.

2. Column 1, Prefix, identifies any administration control or security marking applied to the DoD document identified by *unclassified* title. The following scheme is used:

O Official Use Only
C Confidential
S Secret

3. Column 2, Number, identifies the DoD document. Numbers followed by (D) are DoD Directives; all other issuances are either DoD Instructions or DoD Publications.

4. Column 3, Subject, is self-evident.

5. Column 4, Date, is the publication date listed in the annual index to DoD issuances, DoD 5025.1-I (reference (uu)).

6. Column 5 lists the Office Symbol and commercial telephone number for DoD Action Officers assigned to each DoD issuance. The following Offices and their related Office Symbols are found in the Table B-1.

7. Column 6, AT Relevance, is a brief description of material included in the DoD issuance of potential interest to AT program participants.

[redacted]

Appendix B-1

8. The DoD issuances generally fall into six broad categories:

a. **DoD Personnel**, including directives bearing on the assignment, training, and support of individuals assigned to high-risk billets or potential high physical threat countries;

b. **International Policy**, including adherence to and training with respect to the international conventions governing the conduct of military institutions in war;

c. **Security**, including information security, physical security of DoD facilities, arms and ammunition of all categories, and DoD-related industrial infrastructure;

d. **Intelligence**, including limitations and procedures governing the collection, storage, and dissemination of information, especially on American persons in CONUS or abroad;

e. **Law Enforcement**, including use of military resources to assist in the enforcement of local, state, and federal statutes; use of selected investigative tools, initiation of criminal investigations, establishment of jurisdiction by the Department of Justice in certain criminal matters arising on DoD installations, and the use of force or deadly force by DoD security personnel; and

f. **Public Affairs**, including general responsibilities of CINCs for public affairs activities, specific public affairs guidance on selected topics, and support by DoD public affairs officers to news media representatives.

c. [redacted]

Pre-fix	Number	Subject	Date	Action Office & Phone	AT Relevance
	1030.1 (D)	Victim and Witness Assistance with Change 1	20 Aug 84	GC (703) 614-7676	Obligations of DoD to aid witnesses to and victims of criminal acts including acts of terrorism.
	1300.7 (D)	Training and Education Measures Necessary to Support the Code of Conduct with Change 1	23 Dec 88	FM&P (703) 697-3387	Training requirements and objectives for DoD personnel on behavior while confined by terrorists.
	1342.6 (D)	Department of Defense Dependents Schools (DODDS) with Changes 1-4	17 Oct 78	DA&M (703) 697-1142	Eligibility requirements to use DODDS, instructional standards, required teacher training.
	1400.5 (D)	DoD Policy for Civilian Personnel	21 Mar 83	FM&P (703) 697-5421	DoD expectations of civilian employees; DoD obligations to civilian employees
	1400.6 (D)	DoD Civilian Employees in Overseas Areas	15 Feb 80	FM&P (703) 695-2330	Assignment of DoD civilian personnel; potential impact on assignment to high risk billets or high risk areas.
O-	2000.12 (D)	DoD Combatting Terrorism Program	27 Aug 90	SO/LIC (703) 693-2898	Basic directive outlining DoD anti-terrorism policies and responsibilities.
O-	2000.12-H	Protection of DoD Personnel Against Terrorist Acts	Pending Revision	SO/LIC (703) 693-2899	Provides background material on steps to enhance the security of DoD personnel and dependents against terrorist threats.
	3025.1 (D)	Use of Military Resources During Peacetime Civil Emergencies Within the United States, Its Territories, and Possessions	23 May 80	USDP (703) 697-5454	Implementation of Posse Comitatus Statute; describes and limits use of military resources to aid local law enforcement activities.
	3025.12 (D)	Employment of MilitaryReources in the Event of Civil Disturbances (reprint)	19 Aug 71	USDP (703) 697-5454	Outlines uses and limits of military forces to protect DoD property and personnel in the event of civil disturbances
	3025.13 (D)	Employment of Department of Defense Resources in Support of the United States Secret Service	13 Sep 85	ES (703) 697-3133	Implementation of DoD-Secret Service MOU for protection of the President and other U.S. and/or foreign dignitaries in the U.S.

FOR OFFICIAL USE ONLY

Prefix	Number	Subject	Date	Action Office & Phone	AT Relevance
	3150.5 (D)	DoD Response to Improvised Nuclear Device (IND) Incidents	24 Mar 87	AE (703) 695-7936	Outlines DoD responses to nuclear terrorist incident
	3224.3 (D)	Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Procurement, Deployment and Support	17 Feb 89	USDA (703) 695-9536	Identifies DoD organizations involved in RDT&E, acquisition efforts related to physical security equipment used in AT programs.
S-	3315.1	Coordination and Reporting of Foreign Intelligence and Intelligence-Related Contacts and Arrangements (U)	23 Mar 84	C3I (703) 697-3959	Intelligence Policy
	4500.50	Overseas Areas Exempt From Prohibition on Shipment of Foreign-Made Privately-Owned Vehicles at Government expense with Change 1	28 Aug 86	FM&P (703) 693-1068	Policy relevant to use of indigenous vehicles by DoD personnel in high risk billets or potential high physical threat countries
C-	4500.51	DoD Non-tactical Armored Vehicle Policy (U)	4 May 87	SO/LIC (703) 693-2898	AT Policy.
C-	5030.43	Significant Military Exercises (U) with Changes 2 and 3	26 Mar 70	USDP (703) 614-4660	See document for details.
	5030.7	Coordination of Significant Litigation and Other Matters Involving the Department of Justice	22 Aug 88	GC (703) 695-3657	Coordination with DOJ on aftermath of terrorist incidents, prosecutions of perpetrators, and DoD support to DoJ.
	5100.52 (D)	DoD Response to an Accident or Significant Incident Involving Radioactive Materials	21 Dec 89	USDA (703) 695-7936	DoD response to terrorist incident in which radioactive materials are alleged or are actually involved; Public Affairs guidance included.
	5100.52-M	Nuclear Weapon Accident Response Procedures (NARP)	Sep 90	AE (703) 695-7936	Outlines specific procedures to be followed in the event of a nuclear weapon accident; procedures may be used in the event that a weapon is target of terrorist attack.
	5100.76 (D)	Physical Security Review Board with Change 1	10 Feb 81	C3I (703) 697-5568	Charter of DoD Physical Security Review Board; responsibilities for technology supportive of AT efforts outlined.

Prefix	Number	Subject	Date	Action Office & Phone	AT Relevance
	5100.77 (D)	DoD Law of War Program	10 Jul 79	GC (703) 697-9248	International legal protections for non-combatants outlined including non-combatants who may have committed civil crimes against American personnel.
	5100.76-M	Physical Security of Sensitive Conventional Arms, Ammunitions, and Explosives Changes 3 and 4	Feb 83	C3I (703) 697-5568	Provides specific techniques to harden weapons and ammunition storage facilities against attack; techniques have applications to other facilities and defense against terrorists.
	5100.78 (D)	United States Port Security Program	25 Aug 86	C3I (703) 697-7641	Functional requirements for AT capabilities in U.S. Ports used by the Department of Defense
	5105.35 (D)	Responsibilities of Unified and Specified Commands in Public Affairs Matters with Change 1	7 May 65	PA (703) 697-1254	Public Affairs responsibilities assigned to CINCs.
	5148.11 (D)	Assistant to the Secretary of Defense (Intelligence Oversight) with Changes 1 and 2	20 Jul 89	DA&M (703) 695-4281	Outlines intelligence oversight responsibilities including collection and reporting touching upon AT and related matters.
	5160.54 (D)	DoD Key Assets Protection Program (KAPP)	26 Jun 89	USDP (703) 697-5491	Directs use of DoD assets to plan protection for assets not owned by the Department of Defense but critical to the Department of Defense's operational and logistic requirements.
	5160.54-R	Industrial Facilities Protection Regulation Changes 1 and 2	Mar 77	USDP (703) 697-5454	Outlines requirements to protect industrial facilities of significance to DoD; provides measures to be used against variety of attacks .
	5200.1 (D)	DoD Information Security Program with Change 1	7 Jun 82	C3I (703) 695-2686	Basic classification guidance; establishes policy governing protection of national security information.
	5200.24 (D)	Interception of Wire and Oral Communications for Law Enforcement Purposes with Changes 1-3	3 Apr 78	C3I (703) 697-9586	Outlines circumstances under which electronic surveillance and telephone surveillance may be used in AT investigations.
	5200.27 (D)	Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense	7 Jan 80	IG (703) F14-8163	Outlines procedures under which collection of information on American citizens is authorized.

Prefix	Number	Subject	Date	Action Office & Phone	AT Relevance
	5200.8 (D)	Security of DoD Installations and Resources	25 Apr 91	C3I (703) 697-5568	Basic requirements for protection of DoD assets from all threats detailed .
	5200.8-R	Physical Security Program	May 91	C3I (703) 697-5568	Specifies Physical Security System approach to be used to protect DoD assets against wide range of physical threats; specifies protective systems for categories of DoD assets.
	5210.41 (D)	Security Policy for Protecting Nuclear Weapons	23 Sep 88	C3I (703) 697-5568	Specifies protection of nuclear weapons against all threats including terrorists
	5210.46 (D)	DoD Building Security for the Nabonal Capital Region	28 Jan 82	DA&M (703) 695-5052	Specifies procedures to be used to protect DoD assets in the National Capital Area.
	5210.56 (D)	Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties	25 Feb 92	C3I (703) 697-5568	Outlines circumstances under which force and deadly force may be used to defend DoD assets; outlines circumstances under which weapons may be carried aboard commercial aircraft.
	5210.63 (D)	Security of Nuclear Reactors and Special Nuclear Materials	6 Apr 90	C3I (703) 697-5568	Specifies protection for nuclear reactors and special nuclear materials against threats comparable to those presented by terrorists.
	5210.84	Security of DoD Personnel at U.S. Missions Abroad	22 Jan 92	C3I (703) 697-5568	Implements DoD-DOS Memorandum of Understanding on security services to be provided to DoD personnel assigned to or attached to U.S. missions overseas.
	5220.22	DoD Industrial Security Program	8 Dec 80	C3I (703) 695-5179	Outlines responsibilities of DoD contractors to protect DoD information & technology from a wide range of threats.
	5230.16 (D)	Nuclear Accident and Incident Public Affairs Guidance	7 Feb 83	PA (703) 693-6163	Discusses proper dissemination of information in the event of an incident involving nuclear weapons.
	5230.17	Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations	17 Feb 85	USDP (703) 695-0122	Establishes procedures under which classified information may be provided to friends and allies; important with respect to sharing of terrorist threat .

FOR OFFICIAL USE ONLY

Prefix	Number	Subject	Date	Action Office & Phone	AT Relevance
O-	5230.22	Security Controls on the Dissemination of Intelligence Information	12 Jul 88	C3I (703) 695-2686	Establishes limitations on the dissemination of intelligence information; can impact dissemination of terrorism threat information.
	5230.9 (D)	Clearance of DoD Information for Public Release with Change 1	2 Apr 82	PA (703) 697-4768	Specifies procedures by which information can be cleared for public dissemination; relevant to writing and discussion of AT programs in media.
	5240.1 (D)	DoD Intelligence Activities	25 Apr 88	C3I (703) 695-0822	Defines DoD components participating in intelligence community; allocates responsibilities for information collection and analysis, much of which is related to terrorism.
	5240.1-R	Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons	Dec 82	C3I (703) 695-0822	Outlines procedures to be followed with respect to balancing rights of Americans with requirements of national security.
	5240.10	DoD Counterintelligence Support to Unified and Specified Commands	18 May 90	C3I (703) 697-9586	Discusses DoD assistance to CINCs in counterintelligence threat briefings.
	5240.2 (D)	DoD Counterintelligence	6 Jun 83	C3I (703) 697-9639	Defines counterintelligence activities and assigns duties and responsibilities, many of which related to DoD AT efforts.
	5240.4	Reporting of Counterintelligence and Criminal Violations	22 Jun 87	C3I (703) 697-9639 IG (703) 614-8163	Describes steps that should be taken to report unauthorized and/or illegal counterintelligence activities.
	5240.6 (D)	Counterintelligence Awareness and Briefing Program, Reprint	26 Feb 86	C3I (703) 697-9639	Establishes requirements for counter-intelligence briefing and defensive measures training for DoD personnel at risk from hostile intelligence services and their agents.
	5400.11 (D)	Department of Defense Privacy Program	9 Jun 82	DA&M (703) 614-3027	Outlines procedures to be used to safeguard private, personal information of DoD personnel.
	5400.11-R	Department of Defense Privacy Program	Aug 83	DA&M (703) 614-3027	Specifies procedures to be following regarding control and release of private information relating to DoD personnel and their dependents.

Prefix	Number	Subject	Date	Action Office & Phone	AT Relevance
	5400.7 (D)	DoD Freedom of Information Act Program	13 May 88	PA (703) 697-1180	Describes circumstances under which information may be withheld from the public following a FOIA request; outlines FOIA procedures.
	5400.7-R	DoD Freedom of Information Act Program Change 1	Oct 90	PA (703) 697-1180	Provides detailed guidance on processing of FOIA requests.
	5410.1 (D)	Release of Information Concerning Accidental Casualties Involving Military Personnel or Equipment	27 Sep 73	PA (703) 693-1076	Useful general guidance on dealing with casualty information matters resulting from terrorist incidents as if they were accidental injuries.
	5410.15	DoD Public Affairs Assistance to Non-Government, Non-Entertainment-Oriented Print and Electronic Media	28 Mar 89	PA (703) 695-0168	Provides guidance on support to be given news media during coverage of terrorist incidents, antiterrorism and counterterrorism training.
	5505.1 (D)	DoD Criminal Investigation Standards, Policies and Procedures	13 Feb 85	IG (703) 614-8163	Policies governing DoD criminal investigations including criminal acts committed against DoD personnel, facilities, or materiel by politically motivated perpetrators.
	5505.3	Initiation of Investigation by Military Criminal Investigative Organization	11 Jul 86	IG (703) 614-8163	Outlines circumstances underwhich DoD military investigative organizations initiate criminal investigations.
	5525.1 (D)	Status of Forces Polices and Information with Change 1	7 Aug 79	GC (703) 697-7215	Describes purpose and functions of Status of Forces Agreements and allocation of responsibilities under them.
	5525.5 (D)	DoD Cooperation with Civilian Law Enforcement Officials with Change 1	15 Jan 86	DEP&S (703) 693-1920 FM&P (703) 697-3387	Detailed discussion of DoD support to law enforcement under Posse Comitatus statute.
	5525.7 (D)	Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes	22 Jan 85	CG (703) 693-0270 IG (703) 614-8163	Outlines basis & procedures for dividing jurisdiction between the Department of Justice and the Department of Defense for investigation and prosecution of crimes, some of which may be committed by terrorists.

APPENDIX C

PHYSICAL SECURITY EVALUATION GUIDE

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

FOR OFFICIAL USE ONLY

315

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

Appendix C-3

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>
INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<PHYSICAL SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

SECTION IV - ADDITIONAL INFORMATION

Use this section to add pertinent information for your particular installation or activity.

Attach additional copies of this continuation page, as necessary.

1. TITLE / SUBJECT / ACTIVITY / FUNCTIONAL AREA, ETC.	2. PROJECT OFFICE / OFFICER	3. DATE *(YYMMDD)*

NO.	ITEM *(Assign a number to each item.)*			

APPENDIX D

PHYSICAL SECURITY MEASURES FOR DoD FACILITIES AND INSTALLATIONS ADJACENT TO BODIES OF WATER

A. INTRODUCTION

1. DoD facilities and installations located adjacent to bodies of water, such as ports, airfields, R&D facilities, and training areas face all of the terrorist threats as landlocked facilities or installations. In addition, they must be defended against waterside assault.

2. Measures discussed in this appendix are intended to address the following types of terrorist threats and potential consequences.

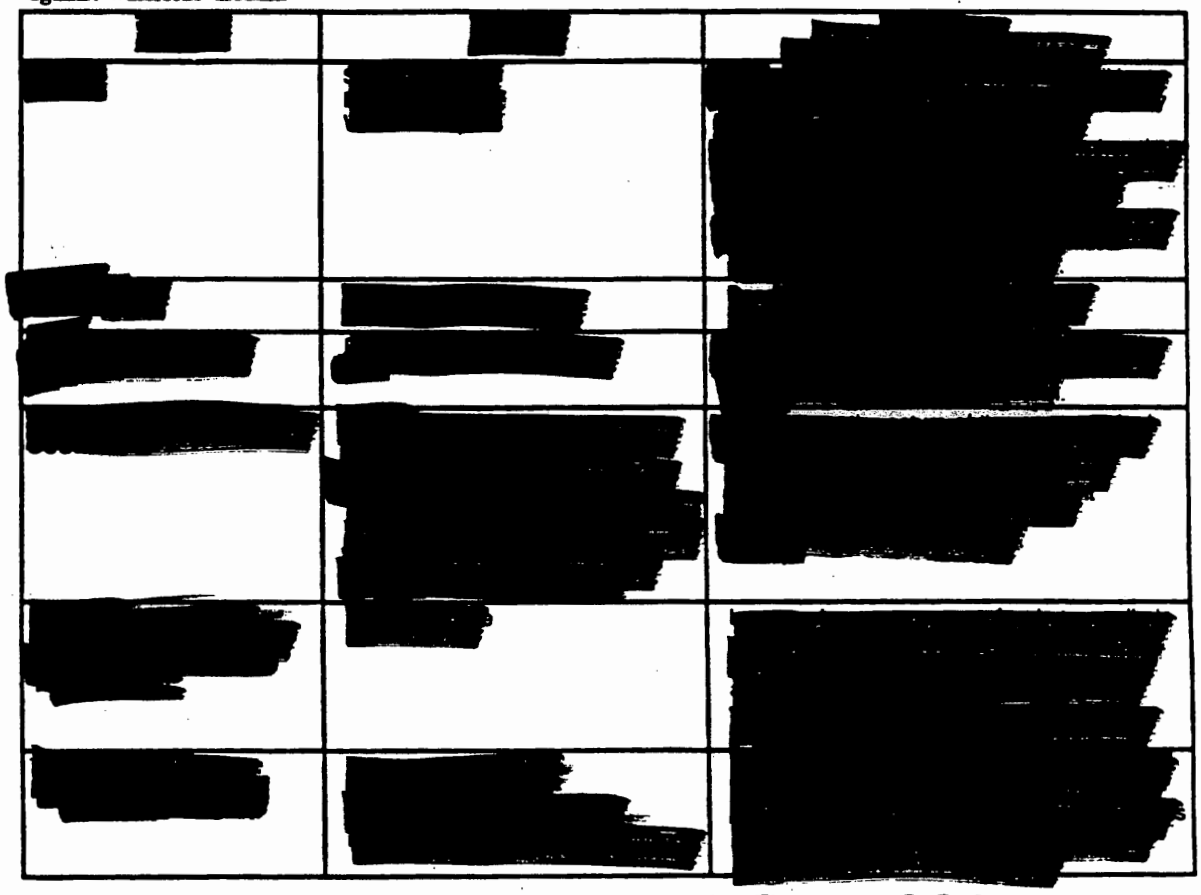


Figure Appendix D-1: Waterborne Terrorist Threats to DoD Assets

3. The Appendix presents material in a manner similar to Chapters VII through IX, building on the concept of a physical security system intended to protect a broad range of DoD assets, including those shown in Figure Appendix D-2: DoD Waterside Assets.

4. Terrorist attacks from the waterside of DoD facilities are not fundamentally different than terrorist attacks from the landside of such as an installation or facility. [redacted] In the following section the physical security system functions are reviewed, and some of the differences between waterborne and landside terrorist attacks are identified and discussed.

[redacted]

Figure Appendix D-2: DoD Waterside Assets

B. SECURITY SYSTEM FUNCTIONS

1. Security system functions performed in the protection of a landlocked DoD installation or facility must also be performed when the installation has an interface with a body of water or is itself surrounded by water. Threat detection, classification and identification, response, delay, and incident resolution must be performed.

2. The medium of water presents unique challenges and some opportunities for the physical security system. [redacted] some surveillance systems that do not work particularly well at landlocked installations can be applied with good success on the waterside of DoD installations, facilities, or assets afloat.

4. Figure Appendix D-3 below identifies some of the special concerns related to security system functions and each of the threats identified above.

In the sections that follow, the discussion will identify waterside physical security system components, the integration of the components into a physical security system, and the operation of the physical security system in response to various threats identified above.

C. WATERSIDE PHYSICAL SECURITY SYSTEM COMPONENTS

1. Barriers

a. Barriers on the waterside of a DoD installation, facility, or asset afloat perform many basic functions performed on land: establish boundary; isolate activity and discourage visitors; and impede passage by boat or swimmer.

b. [redacted] Some intrusion detection devices can be mounted on fixed installations that extend into the water such as wharfs or piers or navigation aid platforms.

c. [redacted] These problems are discussed below.

2. Boundaries

a. Several devices can be used to establish boundaries separating the DoD installation, facility, or asset from the surrounding or bordering waters. Among the devices that can be used to establish a boundary are the following:

(1) Buoys or floats.

(2) Nets.

(3) Anchored or pile mounted navigation aids and signalling devices.

(4) Log booms.

(5) Barges.

(6) Gig-boats, whale boats, and other small work boats at anchor.

(7) Roving patrols by security boats.

b. Once established, boundaries can be used to provide areas of operation for floating security patrols as well as Contact and Escort services and Tactical Reaction activities.

c. It must be emphasized that rules of navigation allow for inadvertent and innocent penetration of certain types of barriers, as may occur with small craft engine failure, sailboats, and in some waters, "weekend" sailors whose enthusiasm for water sports exceeds their navigational and operational skills. [redacted]

DELETED

Appendix Figure D-3. Physical Security System Functions and Special Challenges Applied to Waterborne Threats

3. **Isolate Activity and Restrict Access**

a. Some of the barriers noted in C.1.a above can be used to restrict waterside access to DoD installations. [redacted] Barges can be used to create a physical barrier of considerable penetration resistance to small craft. The barges should be secured bow to stern with the lead and aft barges being secured to the pier or shoreside mooring point. The primary purpose for deploying a barrier of this type is to absorb a large portion of the blast from an explosive laden vessel that managed to elude initial defenses.

b. Use of patrol boats is probably the most effective means of isolating a DoD activity and discouraging uninvited visits from benign or curious intruders. [redacted]

4. **Impede Passage**

a. Several of the barriers described above can be used to slow or impede access to DoD facilities by boats or swimmers. [redacted] such devices should be emplaced only after exhaustive consultations with appropriate legal authorities.

b. Again, patrol activity by Contact and Escort boats or Tactical Reaction Boats can be a very effective

5. **Surveillance and/or Intrusion Detection Systems**

a. There are a number of surveillance systems that are appropriate for use in connection with waterside security A partial list is found in Figure Appendix D-4 below.

b. As suggested by this figure, there is a substantial difference in surveillance of waterside activities during the day and during the night. During hours of darkness, a substantial reduction in surface activity occurs. As a result, nighttime surveillance of waterside activity can rely on active measures such as radar with comparatively good success in locating and partially identifying potential problems.

6. **Classification and/or Identification**

a. As in the case of landside security systems, once a potential intruder has been detected, it must be classified and identified in order to ensure that proper security measures are undertaken. Waterside security measures respond to the detection of threat by trying to gain more information. [redacted]

b. There may be many benign reasons to account for the presence of a swimmer or vessel in an area which is not usually open for such intrusions. Lost sailors and swimmers, mechanical failure, curiosity seekers, currents, tides, winds, etc., can be as much responsible for a barrier penetration as hostile intent. Being able to classify detected targets quickly in terms of hostilility and/or benignancy is critically important.

7. **Response**

a. **Establishment of Security Zones**

(1) Waterside security is enforced by the establishment of at least two zones of activity. [redacted]

(2) [redacted] security forces will stop and challenge intruders, taking all actions necessary to stop a potential threat.

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Appendix Figure D-4: Waterside Surveillance Sensors

(3) [redacted]

Security forces should endeavor to prevent the entry of hostile craft or vessels into this zone; local defenses may be engaged if hostile craft or vessels enter this zone. Techniques described below may be used to disrupt swimmer attacks within this zone.

b. Response Forces Generally

(1) Three types of waterborne security forces are employed to maintain perimeter security and enforce security zone restrictions. [redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

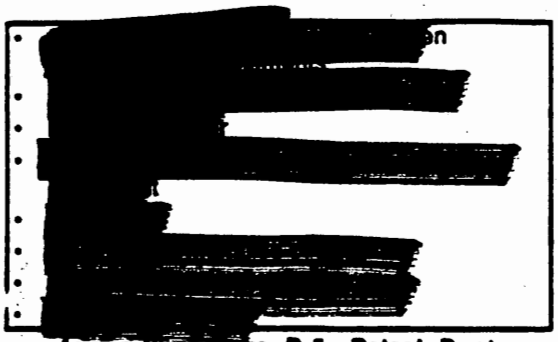
[redacted]

(5) [redacted]

(6) It is also recommended that a shore patrol force equipped with vehicles, communications equipment, and personal protection equipment be deployed to patrol the land-water interface.

(7) It is essential that command, control, and communications systems used by waterside security forces be fully integrated with landside security forces.

(8) Appendix Figure D-5 provides a list of equipment which should be provided to all boats performing supporting security forces:



Appendix Figure D-5: Patrol Boat Security Equipment

(9) [redacted]

(10) The primary source of small boat communication is, of course, the VHF-FM radio. If available, secure communications should be used. If not available, authentication tables must be used to avoid compromise. Also, when working with DoD forces, additional or alternate communication equipment must be shared to provide a compatible means of communication between forces. A single primary tactical frequency should be designated for small boat security operations. This frequency should not be one routinely used by non-operation forces in the area.

(11) No boardings should be conducted by patrolling small boats or any other vessels [redacted] If a boarding becomes necessary, it should be conducted by the contact and/or escort vessels, if employed, local or state law enforcement officers, or by designated boarding teams transported to the scene by a standby vessel. In all cases, the boarding should take place outside the security zone at a secure location.

D. SECURITY SYSTEM COMPONENT INTEGRATION

1. Patrol Techniques

a. Resource Allocation

(1) Designate Sectors

Divide the water approaches to the asset into sectors utilizing sector boundary lines that converge at the asset. Each sector should be lettered.

(2) Number Of Sectors Required

[redacted] The number of sectors within the Security Zone need not necessarily coincide exactly with those in the RZ. It may vary accordingly with the number of small boats available for patrol.

(3) Patrol Areas

[redacted]

(4) Patrol Boat Designations

(a) [redacted]

(b) [redacted] for patrolling a security zone are as follows:

b. One-Boat Security Zone

(1) [redacted] This position allows maximum visibility for observing the established security zone and for warning local vessel traffic.

(a) Intercept Procedures

[redacted]

(b) Maneuvering

[redacted]

c. Two-Boat Security Zone

[redacted]

d. Moving Security Zone

[redacted] Additional security vessels may [redacted] the threat indicates a need.

(1) Position

[redacted]

(2) Duties

[redacted]

e. Security Zone Enforcement At Anchorage

The tactics previously discussed in these paragraphs may be adapted for 360-deg coverage of assets at anchorage. In heightened threat environments, tactics discussed may also be adapted for 360-deg coverage.

f. Defensive Boat Tactics

(1) Defensive boat tactics provide a response mechanism for actively intercepting and neutralizing an identified, incoming hostile threat. This section will provide guidance on how small boats can be used to protect a designated asset. The asset can be a ship, pier, waterfront facility, or any area or object vital to national security that requires protection from a waterborne threat. These tactics were developed for use primarily in a Low-Intensity Conflict (LIC) environment. However, the tactics may be used at any level of THREATCON in support of security zone enforcement by modifying the use of force and Rules of Engagement (ROE) to meet the current threat.

(2) Security operations in a hostile environment without declared war require extraordinary measures to separate friend (or neutral) from foe. In a CONUS LIC environment, the DoD components as well as other U.S. Government agencies and departments participating in security operations must continually maintain a law enforcement posture that recognizes the constitutional rights and privileges of the citizenry to use the waterways of the nation.

(3) Peacetime and/or wartime security operations against an adversary, once identified, are the easiest part of the equation. The following tactics are designed to assist friendly forces in determining friend from foe:

(4) The first level of response with this tactical doctrine is to notify transiting vessels of the security zone and to determine their intentions. Nonaggressors will simply be escorted out of the area. The utilization of these tactics in security zone enforcement will ensure that a system will be in place to effectively respond to a wide range of threats. Without them, the DoD and other U.S. Government security forces and the protected asset may suffer unnecessary casualties with devastating consequences.

2. Boat Intrusion Response

Boats will respond to an intrusion into the security zone, as follows:

a. [redacted]

(2) Screen Vessel Tactics

[redacted]

(3) Screen Vessel Movements

(a) [redacted] Never allow the potential [redacted] clear line of progression to the asset; this is another method of screening out the innocent boater and a further step in the identification of the intruder vessel as having hostile intent.

(b) The obvious actions of a fully marked and identified U.S. Coast Guard boat or similar host-nation vessel if overseas with blue light, weapons at the ready, and siren and/or loudhailer and/or radio calls in the blocking of an incoming vessel's trackline is a positive indication of Coast Guard/host nation enforcement or interdiction action. [redacted]

b. TRB Response To Intrusion

(1) Initial Reaction

While the screen vessel is maneuvering, [redacted] if necessary and approved by the command center. If any degree of doubt exists as to the status of the intruder, he can be kept under observation of the TRB and fired upon if hostile intent is confirmed. Keep in mind that at this point the potential aggressor has been well screened and been given ample warning. If the screen vessel must break off, hostile intent by the inbound vessel is likely.

(2) TRB Response Techniques

[redacted]

(a) TRB Aspect

The aspect that the TRB assumes in relation to the incoming vessel will vary depending upon the type of small boat used (i.e., head on for small utility boat, broadside for larger utility boat or patrol boat.). [redacted]

(b) TRB Movements

Once in position, the TRB should come dead in the water (DIW) and maneuver only to maintain a position between the incoming vessel and the asset. This is simplified by the fact that larger course changes by the incoming vessel can be compensated for by relatively small movements along the zone boundary. [redacted]

c. Command TRB Response

[redacted] other Command TRB functions as may become necessary.

d. Night Operations

(1) Night operations vary from daylight operations [redacted]

[redacted]

controlled by a central command radar system; e.g., ship's radar.

(2) [redacted] Observation posts should be employed along the shoreline at strategic locations to prevent aggressors from making contact along the shoreline. All screen vessels should be equipped with parachute illumination flares for use during hostile activity to illuminate aggressors. Night vision devices should also be used to assist in visually acquiring incoming vessels.

3. Swimmer Deterrence and Countermeasures

The threat to vessels, waterfront facilities, port complexes, bridges, and other assets in the maritime environment from hostile swimmers is a viable one. [redacted] (LIC) operations without the use of complex hardware. [redacted]

a. General Swimmer Capabilities

The nominal speed for a swimmer, depending on distance and equipment carried, is one knot. Even a minor current will cause the swim-mer to limit his attack direction. Swimmers will take advantage of currents to reach their targets. This should be taken into consideration when orienting a defense. However, if intelligence indicates that hostiles are sophisticated enough to have swimmer delivery vehicles or swimmer propulsion units, a 360-degree defense (including under pier areas) should be maintained.

b. Swimmer Countermeasures

Security patrols in support of swimmer defense should be conducted as follows:

(1) Shoreside Patrols

The alert port security patrol is an important element in defending against a swimmer attack. Properly equipped, the port security patrol offers the most sophisticated detection, classification, and neutralization capability yet developed. They can operate in daylight or darkness, are capable of kill or capture (depending on the Rules of Engagement) and can alert others to a swimmer threat. [redacted]. Port security personnel should patrol in darkened areas, shielded from artificial lighting and as far forward in the area of threat as possible to eliminate background noise and other detection obstructions. When applicable and available, binoculars, night vision devices, and/or thermal imagers should be utilized to assist in detection. Anything that appears to be moving toward the protected asset should be treated as a possible attack. Drifting debris is often used to camouflage a swimmer or mine and should be investigated immediately.

(2) Waterside Patrols

(a) [redacted] The random presence of a vessel with turning screws and an alert crew is a respectable deterrent to unsophisticated divers. If the threat is high and believed to be from accomplished divers, [redacted]

(b) [redacted] should patrol likely launch points for both surface craft and all-terrain vehicles delivering hostile swimmers. The random presence of a vessel with turning screws and an alert crew is a respectable deterrent to unsophisticated divers. If the threat is high and believed to be from accomplished divers, [redacted] within CONUS use of drag lines for swimmer defense may only be authorized by the area or district commander.

(3) Pier, Hull, and In-water Structure Inspections

(a) [redacted] However, if they are not available, many local and state police agencies have similar capabilities. Throughout the vessel's port stay and established security zone, the pier area and the ship's hull should be inspected periodically by both landside personnel and Coast Guard waterside patrols.

(b) Other structures that may be at risk of terrorist attack such as navigation aids, bridges, utility cable towers, tunnels, etc., should also be inspected for underwater explosive devices on a periodic basis. Frequency of inspections should be increased on the basis of reported threats.

(4) Use Of Concussion Grenades

[redacted] However, they are to be used [redacted] qualified personnel in high threat areas only. [redacted] Although the kill range is not large, the random use of concussion grenades in several locations around the protected asset will force most swimmers out of the area. Care must be taken to ensure that a recognizable time pattern is not established. [redacted]

(5) Additional Measures

If the protected asset is a ship, or if a ship is moored near the protected asset, turning the ship's screw, maintaining sea suction, and shifting the rudder on a random basis can be an effective deterrence. However, these methods are generally effective only against unsophisticated swimmers. Establishing lighting around the protected asset that does not interfere with the security personnel's vision or give away their positions or movements is effective in locating surface swimmers and "bubble trails" from "open circuit" SCUBA divers. Portable lighting, search and/or spot lights, and illumination flares should be available for emergency responses. Periodic activation of the ship's sonar can be an effective deterrent through delivery of its high pitched "ping."

E. SUMMARY

This appendix outlines some measures that can be taken to protect DoD installations and facilities against waterside assault by terrorists. The measures outlined above are a subset of measures developed primarily by the U.S. Coast Guard, which has lead agency responsibility for protection of DoD assets in U.S. ports. Additional information and technical assistance can be obtained from that agency.

Enclosure 1 is an evaluation guide that can be used to assess the waterside security of DoD installations and facilities including but not limited to ports, facilities with an active land and/or water interface, and facilities that have navigation aids or support activities afloat in adjacent waters.

Enclosure: Waterside Security Evaluation Guide

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

<<WATERSIDE SECURITY EVALUATION GUIDE>>

INSTRUCTIONS AND FORM DELETED

PART M - ADDITIONAL INFORMATION

Use this section to add pertinent information for your particular installation or activity.

Attach additional copies of this continuation page, as necessary.

1. TITLE / SUBJECT / ACTIVITY / FUNCTIONAL AREA, ETC.	2. PROJECT OFFICE / OFFICER	3. DATE *(YYMMDD)*

NO.	ITEM *(Assign a number to each item.)*			

DD Form 2638, JAN 93

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

LOCK SECURITY

A. GENERAL

The first line of defense in any security system is locks or locking devices. 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.

B. ENTRYWAY SAFETY FACTORS

1. Windows

a. [redacted] A window's only security value is 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 due to the noise made by its shattering and potential injury to themselves. The following techniques can be used to upgrade window security.

b. [redacted] Key-operated locks are also available, but they pose a safety hazard in the event the window is needed for escape in an emergency.

c. Other methods of window security include the installation of steel bars, mesh, or grillwork.

2. Doors

a. 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, and rail (panel) wood doors, and metal doors.

b. 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.

c. [redacted] However, breaking through a door is not the most common method in defeating a door system.

d. A far more significant hazard is a door that fits loosely to the frame, thereby allowing it to be pried or forced open. Most wooden door frames have solid wood, 3/4 inch to 1 inch in depth. Beyond this, there is usually a 4-inch to 6-inch gap of air between the frame and the first stud. This construction provides very little resistance to forced entry.

(1) [redacted]

(2) [redacted]

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

(4) [redacted] 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 is to weld the pins to the hinge. This method is effective, 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. [redacted]

(5) [redacted] 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 provides 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. [redacted]

3. Locking Mechanisms

a. Cylindrical locks (key-in-knob locks) are the most widely used lock 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.

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

c. [redacted] 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.

d. 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 assures the knob turns freely from the inside to permit rapid exit in case of emergency.

e. Cylinder dead bolt locks are rapidly becoming the most popular auxiliary lock. 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 are under attack as a safety hazard where rapid escape is essential; e.g., in the case of fire, and are prohibited by many municipal codes because fire officials are concerned that the need to find a key delays escape in an emergency.

4. Lock Selection Guidelines

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

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

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

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

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

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

(1) [redacted]

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

(3) [redacted]

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

g. Use rim locks to provide additional protection.

h. Lock all vulnerable windows and doors at night.

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

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

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

l. Fill hollow metal door frames behind the striker plate with cement to prevent forcing the frame.

m. Restrict home and office keys.

n. Restrict distribution and duplication of keys.

o. Keep spare keys in a locked drawer or filing cabinet.

p. Incorporate heavy-duty, double-cylinder door locks on office entrance doors if fire and safety regulations permit.

5. Legal Protection for DoD Locks

a. In response to requests by the Department of Defense, Congress adopted section 1090 of the "National Defense Authorization Act for Fiscal Years 1992 and 1993" (reference (uu)), making it to unlawful for any person to knowingly duplicate a key or keyway used in a DoD security lock. This provision applies to key and keyway holders, as well as locksmiths or other vendors of duplicate keys and keyways.

b. Punishment upon conviction for violation of this statute may include fine and imprisonment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

GENERAL GUIDANCE FOR INDIVIDUAL PROTECTIVE MEASURES

A. OVERCOME ROUTINES

1. Vary your route to and from work, and the time you arrive and leave.

2. Exercise on a varying schedule, utilizing different routes and distances. It is best not to exercise alone.

3. Avoid routines (time and location) for shopping, lunch, etc.

4. Do not divulge family or personal information to strangers.

5. Enter and exit buildings through different doors, if possible.

B. MAINTAIN A LOW PROFILE

1. DoD personnel, DoD contractors, and their dependents should dress and behave in public in a manner consistent with local customs. Items that are distinctively American should not be worn or displayed outside American compounds unless necessary to accomplish official business.

2. Examples of such items include:

a. Cowboy hats, cowboy boots, Western belt.

b. Clothing adorned with American flags or other national symbols (Statue of Liberty), city, or commercial logos.

c. Suitcases, backpacks, brief cases, attache cases, or shopping bags with stickers, decals, or other distinctively American symbols.

d. Tattoos, patches, military duffel bags, or military style clothing, with or with unit or American identification markings.

e. Show respect for local customs.

f. Shun publicity.

g. Do not flash large sums of money, expensive jewelry, or luxury items.

C. BE SENSITIVE TO, AND CHANGES IN, THE SECURITY ATMOSPHERE

1. Be alert for surveillance attempts, or suspicious persons or activities, and report them to the proper authorities.

2. Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.

3. Avoid public disputes or confrontations. Report any trouble to the proper authorities.

4. Do not unnecessarily divulge your home address, phone number, or family information.

D. BE PREPARED FOR UNEXPECTED EVENTS

1. Get into the habit of "checking in" to let friends and family know where you are or when to expect you.

2. Know how to use the local phone system. Always carry "telephone change."

3. Know the locations of civilian police, military police, government agencies, the U.S. Embassy, and other safe locations where you can find refuge or assistance.

4. Know certain key phrases in the local language.

Such phrases include "I need a policeman," "Take me to a doctor," "Where is the hospital?," and "Where is the police station?" If such phrases are difficult to learn or time is too short, have someone write them down on small file cards. A 3 × 5 card can contain several phrases written out phonetically that can be read to summon assistance; alternatively, then can be written down so that a person in need of assistance can merely show a card to someone competent in a local language, thereby summoning help.

5. Set up simple signal systems that can alert family members or associates that there is a danger. Do not share this information with anyone not involved in your signal system.

6. Carry identification showing your blood type and any special medical conditions. Keep a minimum of a one week supply of essential medication on hand at all times.

7. Keep your personal affairs in good order. Keep wills current, have powers of attorney drawn up, take measures to ensure family financial security, and develop a plan for family actions in the event you are taken hostage.

8. Do not carry sensitive or potentially embarrassing items.

APPENDIX G

OFFICE SECURITY TIPS

A. GENERAL PRACTICES

1. Establish and support an effective security program for the office.

2. Discourage use of office facilities to store objects of significant intrinsic value unless essential for the mission or function of the activity (such items include petty cash boxes, firearms, personal stereos, binoculars, negotiable securities, original artwork of potential commercial interest, etc.).

3. Ensure that all persons working in an office are trained to be alert for suspicious activities, persons or objects.

4. Arrange office interiors so that strange or foreign objects left in the room will be immediately recognized; e.g., remove obvious obstructions behind which or within which improvised explosive devices could be concealed, such as draperies, closed waste baskets, unsecured desks and filing cabinets, and planters.

5. Provide for security systems on exterior doors and windows.

6. Ensure that access control procedures are rigorously observed at all times for access to:

   a. The installation.

   b. Buildings within an installation.

   c. Restricted and/or exclusion areas with a building.

7. Use an identification badge system containing a photograph.

8. Locate desks in a way that persons entering the office or suite can be observed.

9. Identify offices by room number, color, or object name, and not by rank, title, or name of incumbent (room 545, the gold room, the Berlin room, the maple room, not the General's office, the Assistant Attache's office, or the S-2's office).

10. Do not use name plates on offices and parking places.

B. SPECIFIC OFFICE PROCEDURES

1. Telephone and Mail Procedures

a. Rank or title should not be used when answering telephones.

b. When taking telephone messages, do not reveal the whereabouts or activities of the person being sought unless the caller is personally known to the individual taking the message.

c. Collect telephone messages in unmarked folders; do not leave exposed for observers to identify caller names and phone numbers, persons called, and messages left.

d. Observe caution when opening mail. In particular, be on the lookout for letters or packages that might contain improvised explosive devices. A checklist to aid in letter bomb or packaged IEDs appears in Appendix Q.

2. General Working Procedures

a. Avoid carrying attache cases, brief cases, or other courier bags unless absolutely necessary.

b. Do not carry items that bear markings that identify the owner by rank or title, even within the office environment.

c. Avoid working alone late at night and on days when the remainder of the staff is absent.

d. If late night work is necessary, work in conference rooms or internal offices where observation from the outside of the building is not possible.

e. Office doors should be locked when vacant for any lengthy period, at night and on weekends.

f. Papers, correspondence, communications materials, and other documents should not be left unattended overnight.

g. Maintenance activity and janitorial services in key offices, production, maintenance or other areas installation areas should be performed under the supervision of security personnel.

h. Removal of property, materiel, or information stored on any media from the facility should be prohibited without proper written authorization.

i. Consider prohibiting the importation of property, materiel, or information stored on any media into the facility unless such items have been properly inspected.

j Offices not in use should be locked to prohibit unauthorized access or the storage of material that could be used to hide improvised explosive devices or intelligence collection devices.

k. Use of vehicles or vehicle markings that make it possible to readily identify the vehicle and its occupants as U.S. Government or DoD contractor personnel should be minimized.

l. All personnel should have access to some sort of duress alarm to annunciate and warn of terrorist attack.

m. Secretaries and guard posts should be equipped with covert duress alarms which can be used to alert backup forces, summon assistance, or otherwise alert critical personnel for the need to take special actions to avoid a terrorist incident.

n. Placement of office furnishings directly in front of exterior windows is to be avoided if at all possible.

APPENDIX H

TIPS FOR EXECUTIVE ASSISTANTS

A. INTRODUCTION

The following recommendations are suggested for the consideration of executive assistants, administrative assistants, and secretaries assigned to senior military officers or senior DoD officials who may be the target of terrorist attack. These measures may be valuable aids to preserving the security of the principal; in addition, adoption of these measures may assure assistants they are not likely to become collateral casualties in an attack on the principal for whom they work.

B. SECURITY TIPS

1. Request installation of physical barriers such as electromagnetically operated doors to separate offices of senior executives from other offices.

2. Request installation of a silent trouble alarm button, with a signal terminating in the Security Department or at another the secretary's desk some distance away to ensure that in the event of an emergency it will be possible for someone other than the executive to summon assistance.

3. Do not admit visitors into the executive area unless they have been positively screened in advance or are known from previous visits.

4. Unknown callers should not be informed of the the whereabouts of the executive, his or her home address, or telephone number.

5. A fire extinguisher, first-aid kit, and oxygen bottle should be stored in the office area.

6. When receiving a threatening call, including a bomb threat, extortion threat, or from a mentally disturbed individual, remain calm and listen carefully.

7. Do not accept packages from strangers until satisfied with the individual's identity and the nature of the parcel.

8. Travel itineraries for all personnel should be kept absolutely private. Distribution should be limited strictly to persons with a need to know.

9. Daily schedules for senior officers and civilian officials should be distributed on a limited basis and should contain only that information needed by each recipient.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I

GENERAL TRAVEL SECURITY TIPS

A. INTRODUCTION

Statistics indicate that terrorist actions are most often perpetrated against victims during periods of movement. Traveling from home to work and return provides the move vulnerable time for a potential victim. This vulnerability comes from a number of factors that decrease the risks to the terrorist. The victim can more easily be identified, can be taken by surprise, can be attacked under conditions most favorable to the terrorist when the victim tends to be isolated from known surroundings. The following tips are provided to decrease your vulnerability during travel.

B. VEHICLE TRAVEL TIPS

1. Vary the routes and the times that you frequently travel.
2. Use an inconspicuous vehicle that has no special identifying license plates or stickers.
3. Do a complete walk-around inspection of the vehicle before beginning travel.
4. Lock doors, gas tanks, and storage areas at all times.
5. Ensure that all keys are accounted for regularly.
6. Park in secured areas whenever possible.
7. Remain alert and "aware" at all times while driving.
8. Never pick up hitchhikers.
9. Know the locations of safehavens.

C. TRAVEL ARRANGEMENTS

1. If available, consider using military air or MAC military contract carriers.
2. Avoid travel through high threat areas, if possible.
3. Do not discuss military affiliations with strangers.
4. Consider using a tourist passport.
5. [redacted]

D. PRECAUTIONS WHILE FLYING

1. [redacted]
2. Travel in conservative civilian clothing.
3. Do not wear distinctive military clothing, such as military shoes, organizational shirts and/or jackets, or sunglasses.
4. Arrive at the airport early and watch for suspicious activity.
5. Do not linger near the ticket counters, security areas, or luggage check-in. Go directly to the secured boarding area.
6. Beware of unattended luggage.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J

PERSONAL VEHICLE SECURITY TIPS

A. INTRODUCTION

An extremely important aspect of personal security is the need for regular vehicle inspections. Many terrorist actions are accomplished by placing bombs in individual vehicles. This provides the terrorist less risk and increases the chance of "hitting" the appropriate target. The following are some relatively simply steps that every driver of every DoD Privately Operated Vehicle can take to reduce the likelihood of being hurt by a terrorist act centered around a personal automobile.

B. VEHICLE INSPECTION TIPS

1. EVERY TIME YOU USE YOUR AUTOMOBILE, YOU SHOULD MAKE A PRECAUTIONARY INSPECTION. Bomb emplacement by terrorists is often rudimentary or hastily done, thereby providing the opportunity for easy detection. MAKE A HABIT OF CHECKING THE VEHICLE AND THE SURROUNDING AREA BEFORE ENTERING AND STARTING THE VEHICLE.

a. Check interior of the vehicle for intruders or suspicious items.

b. Check electronic tamper device, if installed. A cheaper option is to use transparent tape on the hood, trunk, and doors to alert you to any tampering.

c. Check underneath the car and in the fender wells for any foreign objects, loose wires, etc.

d. Examine tires for stress marks and any evidence of tampering.

e. Check wheel lug nuts.

f. Check exterior for any fingerprints, smudges, or other signs of tampering.

2. YOU MAY CONSIDER THE FOLLOWING SUGGESTIONS IN AN EFFORT TO "HARDEN" YOUR VEHICLE:

a. Lock the hood with an additional lock and ensure that the factory latch is located inside.

b. Have oversized mirrors installed.

c. Utilize a locking gas cap.

d. Put two bolts through the exhaust pipe, perpendicular to one another. This prevents the insertion of explosive devices in the tail pipe.

e. Use steel-belted radial tires.

f. Install an intrusion alarm system and an extra battery.

g. In high-threat areas, it may be appropriate to:

(1) Install car armor.

(2) Have an interior escape latch on the trunk.

(3) Use fog lights.

(4) Install bullet-resistant glass.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX K

TIPS FOR DEFENSIVE FLYING

A. INTRODUCTION

Air travel, particularly through high risk airports or countries, poses security problems different from those of ground transportation. Here are some simple precautions that can reduce the hazards of a terrorist assault.

B. MAKING TRAVEL ARRANGEMENTS

1. ____ Use office symbols on orders or leave authorizations if the word description denotes a high or sensitive position.
2. ____ Get a threat briefing from the appropriate counter intelligence or security organization prior to travel to a high risk area.
3. ____ Use military air, USTRANSCOM, MAC military contract, or U.S. flag carriers.
4. ____ Avoid scheduling through high-risk areas; use foreign flag airlines and/or indirect routes to avoid high risk airports.
5. ____ Do not use rank or military address on tickets, travel documents, or hotel reservations.
6. ____ [redacted]
7. ____ [redacted]
8. ____ Seats at an emergency exit may provide an opportunity to escape.
9. ____ Avoid off-base hotels, use government quarters or "safe" hotels.

C. PERSONAL IDENTIFICATION

1. ____ Do not discuss your military affiliation with anyone.
2. ____ You must have proper identification to show airline and immigration officials.
3. ____ Consider use of a tourist passport, if you have one, with necessary visas, providing it is allowed by the country you are visiting.
4. ____ [redacted]
5. ____ If you must carry these documents on your person, select a hiding place on board the aircraft to "ditch" them in case of a hijacking.
6. ____ Do not carry classified documents unless they are ABSOLUTELY mission-essential.

D. LUGGAGE

1. ____ Use plain, civilian luggage; avoid military-looking bags, B-4 bags, duffel bags, etc.
2. ____ Remove all military patches, logos, or decals from your luggage and briefcase.
3. ____ Ensure luggage tags do not show your rank or military address.
4. ____ Do not carry official papers in your briefcase.

E. CLOTHING

1. ____ Travel in conservative civilian clothing when using commercial transportation or when traveling military airlift if you are to connect with a flight at a commercial terminal in a high-risk area.
2. ____ Do not wear distinct military items such as organizational shirts, caps, or military issue shoes or glasses.
3. ____ Do not wear U.S. identified items such as cowboy hats or boots, baseball caps, American logo T-shirts, jackets, or sweatshirts.
4. ____ Wear a long-sleeved shirt or bandage if you have a visible U.S. affiliated tattoo.

F. PRECAUTIONS AT THE AIRPORT

1. ____ Arrive early; watch for suspicious activity.
2. ____ Look for nervous passengers who maintain eye contact with others from a distance. Observe what people are carrying. Note behavior not consistent with that of others in the area.
3. ____ No matter where you are in the terminal, identify objects suitable for cover in the event of attack. Pillars, trash cans, luggage, large planters, counters, and furniture can provide protection.
4. ____ Do not linger near open public areas. Quickly transit insecure ticket counters, waiting rooms, commercial shops, and restaurants.
5. ____ Avoid processing with known target groups.
6. ____ Avoid secluded areas that provide concealment for attackers.
7. ____ Be aware of unattended baggage anywhere in the terminal.
8. ____ Observe the baggage claim area from a distance. Do not retrieve your bags until the crowd clears. Proceed to customs lines at the edge of the crowd.
9. ____ Report suspicious activity to airport security personnel.

APPENDIX L

GROUND TRANSPORTATION SECURITY TIPS

A. INTRODUCTION

Criminal and terrorist acts against individuals usually occur outside the home and after the individual's habits have been established. Typically, the most predictable habit is the route of travel from home to duty station or to commonly frequented local facilities.

B. VEHICLES

1. ____ Select a plain car, minimize the "rich American" look.
2. ____ Consider not using a government car that announces ownership.
3. ____ Safeguard keys.
4. ____ Auto maintenance:
   - a. ____ Keep vehicle in good repair. You do not want it to fail when you need it most.
   - b. ____ Keep gas tank at least 1/2 full at all times.
   - c. ____ Ensure tires have sufficient tread.

C. PARKING

1. ____ Park in well lighted areas.
2. ____ Always lock your car,even when it is outside your house.
3. ____ Do not leave it on the street overnight, if possible.
4. ____ Never get out without checking for suspicious persons. If in doubt, drive away.
5. ____ Leave only the ignition key with parking attendants.
6. ____ Do not allow entry to the trunk unless you are there to watch.
7. ____ Never leave garage doors open or unlocked.
8. ____ Use a remote garage door opener if available. Enter and exit your car in the security of the closed garage.

D. ON THE ROAD

1. ____ Before leaving buildings to get into your vehicle, check the surrounding area to determine if anything of a suspicious nature exists. Before leaving your vehicle, look around carefully to be confident you are not headed directly into a threatening situation.
2. ____ Before entering vehicles, check for suspicious objects on the seats. You may also look underneath the seats.
3. ____ Guard against the establishment of routines by varying times, routes, and modes of travel. Avoid late night travel.
4. ____ Travel with companions or in convoy when possible.
5. ____ Avoid isolated roads and dark alleys.
6. ____ Know locations of safehavens along routes of routine travel.
7. ____ Habitually ride with seatbelts buckled, doors locked, and windows closed.
8. ____ Do not allow your vehicle to be boxed in; maintain a minimum 8-foot interval between your vehicle and the vehicle in front; avoid the inner lanes.
9. ____ Be alert while driving or riding.
10. ____ Know how to react if surveillance is suspected or confirmed.
    - a. ____ Circle the block for confirmation of surveillance.
    - b. ____ Do not stop or take other actions that could lead to confrontation.
    - c. ____ Do not drive home.
    - d. ____ Get description of car and its occupants.
    - e. ____ Go to nearest safehaven. Report incident to the nearest DoD counterintelligence, security, or law enforcement organization.

[redacted]

a. ____ [redacted]

b. ____ [redacted]

c. ____ [redacted]

d. ____ [redacted]

e. ____ [redacted]

f. ____ [redacted]

g. ____ [redacted]

h. ____ [redacted]

12. ____ [redacted]

a. ____ [redacted]

b. ____ [redacted]

c. ____ [redacted]

d. ____ [redacted]

e. ____ [redacted]

f. ____ [redacted]

E. COMMERCIAL BUSES, TRAINS, AND TAXIS

1. ____ Vary mode of commercial transportation.
2. ____ Select busy stops.
3. ____ Do not always use the same taxi company.
4. ____ Do not let someone you do not know direct you to a specific cab.
5. ____ Ensure taxi is licensed, has safety equipment (seat belts at minimum).
6. ____ Ensure face of driver and picture on license are the same.
7. ____ Try to travel with a companion.
8. ____ If possible, specify the route you want taxi to follow.

APPENDIX M

SUPPLEMENTAL SECURITY CHECKLIST FOR DRIVING

A. INTRODUCTION

The following items are suggested procedures to be used in operating personal and government motor vehicles in areas where terrorist activity is a concern. While adhering to these practices will not necessarily prevent a terrorist incident, continual practice and attention to details demanded by the procedures below will enable many potential victims to escape to safety.

B. CHECKLIST

1. Keep the gasoline tank of your vehicle full or near full.
2. Keep the vehicle locked at all times. Do not park on the street at night. Vehicles in locked garages should also be kept locked. Use parking lots with attendants and where the vehicle can be kept locked. Lock unattended vehicles, no matter how short the time.
3. Check up and down the street before moving out of a house and/or building into your vehicle.
4. While approaching vehicle, check its outside for evidence of tampering. Look for wires, strings, or objects attached to or hanging from vehicle.
5. Do not touch any unusual items protruding from the vehicle. Immediately call for assistance; i.e., the Regional Security Officer (RSO).
6. Before entering the vehicle, check the floor (front and rear) to make certain the vehicle is not occupied.
7. As you drive away from the curb, be immediately alert for surveillance of your vehicle. Look for multiple vehicle surveil-lance, as most attacks on vehicles have included two or more vehicles.
8. Stay alert and be prepared to take evasive actions. Keep noise level within vehicle low. Eliminate loud playing of the radio or unnecessary conversation.
9. Keep the vehicle locked while driving and the windows closed. If open, keep them rolled to within two inches of the top. This practice prevents objects from being thrown into your vehicle.
10. [redacted]
11. If you encounter a road block manned by uniformed police or military personnel, you should stop and remain seated inside your vehicle. If asked for identification, roll the window down enough to pass your identification to the officer. Do not unlock the doors.
12. Avoid suspicious road blocks. Do not stop. Turn and go back, or turn a corner to leave the area as quickly as possible.
13. A good driver is constantly aware of possible routes of escape or evasion while behind the steering wheel.
14. In the event of a firefight between local authorities and terrorists, get down and stay low. Unless you are in the direct line of fire, it is suggested that you do not move. Experience has shown that oftentimes anything that moves gets shot.
15. [redacted]
    a. [redacted]
    b. [redacted]
16. If possible put another vehicle between yourself and your pursuers.

17. Speed as an evasive tactic is functional only to the point of gaining time to allow you to take other evasive action and to put distance between you and your pursuers. Excessive speed reduces your ability to take evasive action and increases your chances of a fatal crash.

a. [redacted]ns

(1) [redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

(6) [redacted]

(7) [redacted]

(8) Seat belt fastened.

(9) Hands at the "10" to "2" o'clock position.

(10) Arms relatively straight.

(11) Do not use brakes until steering control is reestablished.

(12) Use care in applying power--maintain control.

(13) De-clutch if you are driving a manual shift car.

(14) Counter-steer if you are skidding.

b. [redacted]

(1) [redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

(6) [redacted]

APPENDIX N

SECURITY TIPS FOR HOTELS AND MOTELS

1. Stay at DoD facilities while on TDY/TAD whenever possible.
2. Avoid staying in hotels with distinctively American names or predominantly American guests.
3. Make reservations in two or more hotels and use an assumed or modified name.
4. Avoid taking street-level rooms, terrace-level rooms with direct access to hotel grounds, or stairwells.
5. Retain control over all luggage upon arrival in a hotel lobby.
6. When in a hotel, note all escape routes.
7. Vary your pattern of entering and leaving your hotel.
8. Do not discuss travel plans over hotel phones.
9. Use extra caution in hotel lobbies and other public places where bombs may be placed.
10. Bellboys and other strangers in hotel lobbies should not be asked directions for specific places you intend to go.
11. Do not conduct official business nor meet casual acquaintances in your temporary living quarters; do not divulge the location of your quarters.
12. Discourage efforts to enter your room while you are gone by preserving a "lived-in" look in your room.
13. Keep your room neat.
14. Hallways should be checked before exiting from an elevator or your room, for out of place objects or for persons who seem to be loitering.
15. Packages should not be delivered to your room.
16. Unexpected mail left for you at the desk or slipped under the door of your room should be viewed with suspicion.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX O

FAMILY SECURITY QUESTIONS

A. INTRODUCTION

The following are questions that can be asked to help identify practices that may increase the likelihood that a DoD person or dependent will become a victim of a kidnapping or other terrorist act.

B. HEAD OF HOUSEHOLD

1. Is your telephone number and address in local directories?
2. Do you, your family members, or your domestic employees answer your telephone with your name and rank?
3. Have you had a a security check run on all domestic employees? If overseas, did you ask the Embassy to screen prospective employees' records? Did you contact the local military police and/or counterintelligence office or local police to obtain preemployment screening assistance?
4. Have you maintained a file on each household employee including the full name, address, description, date and place of birth, current photograph and a full set of fingerprints?
5. Have outside fuse boxes and/or circuit breakers been modified so that they can be locked at all times unless access is specifically required?

C. FAMILY

1. Have you adopted a family security program including duress codes and alarms, crime watch practices, and conscious efforts to avoid patterns in daily activities?
2. Have all family members learned emergency telephone numbers? Have they been able to memorize them? Do all family members know how to summon police in the local language? Do they carry 3 × 5 notecards with instructions on how to work local telephones and ask for assistance?
3. Have emergency numbers been posted near each telephone? Do these listings give away the nature of the family's assignment (Ambassador's home phone should not be listed, etc.)? Have all family members been given a sanitized list of phone numbers they can carry with them at all times?
4. Do you have a system for keeping family members informed about each other's whereabouts at all times? Have you included a family duress or trouble signal as part of your family check-in system?
5. Have you removed all symbols or signs from the outside of your residence indicating nationality, rank or grade, title, and name?
6. Have you unnecessarily disseminated personal, family, and travel plans to casual acquaintances or domestic employees who do not need to know your personal schedule on an hourly or daily basis?
7. Have you learned and practiced emergency phrases in the local language such as "I need a policeman, a doctor, help, etc."? Have you written these down in transliteration as well as in the native language so you could show a 3 × 5 card to obtain assistance?
8. Do you and your family members know how to work local pay telephones? Does each family member carry a small quantity of money necessary and sufficient to operate local pay telephones at all times?
9. Are residence doors and windows locked? Have additional security devices been added to door and window locks to increase resistance to intrusion and penetration?

10. Do you and your family members close draperies during periods of darkness? Are the draperies made of opaque, heavy material that provide maximum privacy (and can reduce the distribution of glass shards in the event windows are broken).

11. Have you considered obtaining a dog for protection of your house and grounds? Have you considered geese as an alternative guard animal, if commonly used for that purpose in your locale?

12. Have you or your family members left a spare key in the mailbox or in a similar insecure place?

13. Are tools used by the family, particularly ladders, under lock?

14. Do you have a private place to leave notes for family members or do you tack notes on the door for family, friends, criminals, and terrorists to read?

15. Have you developed a response plan for yourself and family members in the event that an unauthorized person is suspected to be inside your home upon your return? Does your plan emphasize the need to contact the police or the security office immediately and discourage personal investigation of the possible intrusion?

16. Do you or family members automatically open the residence door to strangers? Do you or your family members use a peephole or Closed Circuit TV monitor to identify callers? Do you request to see and verify credentials from utility, service, or other persons seeking to enter your residence?

17. Do you or your family members admit poll-takers and salespersons to your home? Are you aware of the presence of peddlers and all strangers in your neighborhood? Are your family members equally aware? (Terrorists are known to have gathered substantial information relative to their victims using these ruses.)

18. Have you and your family members reported frequent wrong numbers or nuisance telephone calls to the telephone company and the police? Have you considered that someone may be attempting to determine the presence of family members?

19. Have you reported the presence of strangers in the neighborhood? Does it appear that someone or some group may be trying to gain an intimate knowledge of the your family's habits?

20. Do you and your family members watch for strange cars cruising or parked frequently in the area, particularly if one or more occupants remain in the car for extended periods? Have you made a note of occupants, license numbers, and province designators of suspicious vehicles?

21. Do you discuss family activities with strangers?

22. Do you discuss family plans over the telephone?

23. Do you discuss detailed family or office plans over the telephone with people you do not personally know or know well?

24. Do you mail letters concerning family travel plans from your house or office? Are you sure that no one is intercepting your outbound mail, opening it, and then resealing it for delivery after collecting desired information enclosed in it?

25. Have you or family members accepted delivery of unordered or suspicious packages or letters?

26. Have you personally destroyed all envelopes and other items which reflect your name and rank?

27. Have you limited publicity concerning yourself and your family that may appear in local news media?

28. Do you and your family member shop on a set schedule? Do you and your family members always shop and the same stores? Do you and your family members always use the same routes to the office, to shopping, to school, and to after school activities?

29. Do you have a coordinated family emergency plan? Have you ensured that all family members know who to contact if they suspect another family member is in danger? Have you reviewed protective measures with all family members?

30. Have you made sure that each family member is prepared to evacuate the area quickly in the event of an emergency? Do you know where all critical documents such as passports, visas, immunization and other medical records are kept? Are these current, and can you or other family members extract them from their secure storage place on very short notice?

31. Do you find yourself in disputes with citizens of the host country over traffic, commercial transactions, or other subjects? Have you or your family members precipitated any incidents involving host-country nationals?

D. CHILDREN

1. Have school officials been advised that children are not to be released to strangers under any circumstances?
2. Have the children been instructed not only to refuse rides from strangers, but also to stay out of reach if a stranger in a car approaches them?
3. Have you located the children's rooms in a part of the residence that is not easily accessible from the outside?
4. Do you keep the door to your children's rooms open so that your can hear any unusual noises?
5. Do you ever leave your children at home alone or unattended?
6. Are you sure that the person with whom you leave your children is responsible and trustworthy?
7. Are you sure that outside doors and windows leading into the children's rooms are kept locked, especially in the evening?
8. Have you taught your children the following?
   a. Never let strangers into your house.
   b. Avoid strangers and never accept rides from anyone that he or she does not know.
   c. Refuse gifts from strangers.
   d. Never leave home without telling an adult where and with whom you are going.
   e. How to call the police.
   f. To call the police if ever you are away and they see a stranger around the house.
   g. Where possible, walk on main thoroughfares.
   h. Tell you if he or she notices a stranger hanging around your neighborhood.
   i. Play in established community playgrounds rather than in isolated areas.
   j. Give a false name if ever asked theirs by a stranger.

E. SCHOOLS

Have you asked schools attended by your children to:

1. Not give out any information on your students to anyone unless you specifically authorize them to do so in advance? Avoid any kind of publicity in which students are named or their pictures are shown.
2. Not release a student to someone other than his or her parents without first receiving authorization from a parent.
3. Allow children to call parents on the telephone in the presence of school officials before allowing an authorized release to actually occur. (This practice provides protection against a kidnapper who calls and claims to be the child's parent.)
4. Report to the police if any strangers are seen loitering around the school or talking to students. If such strangers are in a car, the teacher should note its make, color, model, and tag number and pass this information on to the police.
5. Have teachers closely supervise outside play periods.

F. NEIGHBORS

1. Have you met your neighbors? Have you gotten them interested in maintaining and improving neighborhood security?
2. Have you exchanged telephone numbers?
3. Have you established some sort of system for alerting one another to trouble in neighborhood?

G. STRANGERS

1. Have all family members been warned to keep strangers from entering the residence?
2. Have all family members and domestic employees been instructed on the requirement that maintenance work is to be performed only on a scheduled basis unless a clear emergency exists? Do you have procedures established on how to be contacted in the event that a utility emergency occurs and maintenance personnel must enter your residence? Do your family members and domestic employees know how to verify the identity of maintenance personnel?
3. Have you and your family discussed the kind of assistance you can offer to a person who comes to your door claiming to be the victim of an automobile accident, a mechanical breakdown, or some other kind of accident? Have you explained to your family that they can offer to call the police, the fire department, or an ambulance, but under no circumstances should they allow the victim into the residence?

APPENDIX P

HOUSEHOLD SECURITY CHECKLIST

A. EXTERIOR	Yes	No
1. If you have a fence or tight hedge, have you evaluated it as a defense against intrusion?	____	____
2. Is your fence or wall in good repair?	____	____
3. Are the gates solid and in good repair?	____	____
4. Are the gates properly locked during the day and at night?	____	____
5. Do you check regularly to see that your gates are locked?	____	____
6. Have you eliminated trees, poles, ladders, boxes, etc., that might help an intruder to scale the fence, wall, or hedge?	____	____
7. Have you removed shrubbery near your gate, garage, or front door which could conceal an intruder?	____	____
8. Do you have lights to illuminate all sides of your residence, garage area, patio, etc.?	____	____
9. Do you leave your lights on during hours of darkness?	____	____
10. Do you check regularly to see that the lights are working?	____	____
11. If you have a guard, does his post properly position him to have the best possible view of your grounds and residence?	____	____
12. Does your guard patrol your grounds during the hours of darkness?	____	____
13. Has your guard been given verbal or written instructions and does he understand them?	____	____
14. Do you have dogs or other pets that will sound an alarm if they spot an intruder?	____	____

B. INTERIOR	Yes	No
1. Are your perimeter doors of metal or solid wood?	____	____
2. Are the door frames of good solid construction?	____	____
3. Do you have an interview grill or optical viewer in your main entrance door?	____	____
4. Do you use the interview grill or optical viewer?	____	____
5. [redacted]	____	____
6. Are the locks in good working order?	____	____
7. Can any of your door locks be bypassed by breaking the glass or a panel of light wood?	____	____
8. Have you permanently secured all unused doors?	____	____

B. INTERIOR (continued)	Yes	No
9. [redacted]	____	____
10. Do you close all shutters at night and when leaving your residence for extended periods of time?	____	____
11. Are unused windows permanently closed and secured?	____	____
12. Are your windows locked when they are shut?	____	____
13. Are you as careful of second floor, or basement windows as you are of those on the ground floor?	____	____
14. [redacted]	____	____
15. If your residence has a skylight, roof latch, or roof doors, are they properly secured?	____	____
16. Does your residence have an alarm system?	____	____
17. Have you briefed your family and servants on good security procedures?	____	____
18. Do you know the phone number of the police security force that services your neighborhood?	____	____

C. GENERAL	Yes	No
1. Are you and your family alert in your observations of persons who may have you under surveillance, or who may be casing your house in preparation for a burglary or other crime?	____	____
2. Have you verified the references of your servants, and have you submitted their names for security checks?	____	____
3. Have you told your family and servants what to do if they discover an intruder breaking in or already in the house?	____	____
4. Have you restricted the number house keys?	____	____
5. Do you know where all your house keys are?	____	____

APPENDIX Q

LETTER AND PACKAGE BOMB RECOGNITION CHECKLIST

A. INTRODUCTION

The following information is useful in detecting the presence of letter or package bombs sent through U.S. and international mails. While by no means complete or foolproof, letters and packages exhibiting the characteristics below should be viewed with extreme caution.

B. RECOGNITION CHART

WEIGHT

_____ Weight unevenly distributed.

_____ Heavier than usual for its size.

_____ Heavier than usual for its postal class.

THICKNESS

_____ For medium size envelopes, the thickness of a small book.

_____ Not uniform or has bulges.

_____ For large envelopes, bulkiness, an inch or more in thickness.

ADDRESS

_____ No return address.

_____ Poorly typed or handwritten address.

_____ Hand-printed.

_____ Title for the executive (recipient) incorrect.

_____ Addressed to a high-ranking recipient by name, title, or department.

RIGIDITY

_____ Greater than normal, particularly along its center length.

STAMPS

_____ More than enough postage.

POSTMARK

_____ Foreign.

_____ From an unusual city or town.

WRITING

_____ Foreign writing style.

_____ Misspelled words.

_____ Marked "Air Mail," "Registered," "Certified," or "Special Delivery."

_____ Marked "Personal", "Confidential," "Private," or "Eyes Only."

ENVELOPE

_____ Peculiar odor.

_____ Inner sealed enclosure.

_____ Excessive sealing material.

_____ Oil stains.

_____ Springiness.

_____ Wires, string, or foil sticking out or attached.

_____ Ink stains.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX R

FAMILY "OPERATIONS SECURITY" TIPS

1. Do not place your name on exterior walls of residences.
2. Do not answer your telephone with your name and rank; children and domestic employees should be instructed not to identify the name, title, or affiliation of the occupants when answering the telephone
3. Do not list your telephone number and address in local directories.
4. Create the appearance that the house is occupied by using timers to control lights and radios while you are away.
5. Personally destroy all envelopes and other items that reflect personal information.
6. Safeguard financial records and other materials that could be used to identify bank accounts, credit card accounts, or brokerage acounts.
7. Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.
8. Do not let your trash become a source of information.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX S

BODY ARMOR STANDARDS, SPECIFICATIONS, AND SELECTION

A. INTRODUCTION

The National Institute of Justice has published NIJ Standard 0101.03, "Ballistic Resistance of Police Body Armor," which provides standards to judge personal body armor capabilities to provide protection against various types of threats. The following is a brief summary of the standard and the various threats against which each type of protective body armor has been tested.

B. BODY ARMOR STANDARD

1. Type I [redacted]

2. Type II-A [redacted]

3. Type II [redacted]

4. Type III-A [redacted]

5. Type III [redacted]

6. Type IV [redacted]

C. BODY ARMOR SELECTION

1. Although designed primarily to provide protection against handgun assualt, soft body armor has prevented serious and potentially fatal injuries in traffic accidents, from physical assault from improvised clubs, and to some extent from knives.

2. The fundamental considerations guiding selection of body armor are the threat to which protected persons will be exposed.

FOR OFFICIAL USE ONLY

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

THERE IS NO SUCH THING AS A BULLET-PROOF VEST. The routine use of appropriate soft body armor significantly reduces the likelihood of fatal injury, but 100-percent protection in all circumstances is impossible. Body armor selection is to some extent a trade-off between ballistic protection and wearability. The weight and comfort of soft body armor is inversely proportional to the level of ballistic protection that it provides.

Proper fitting can make more capable body armor more tolerable to the user.

D. ADDITIONAL INFORMATION

For additional information on body armor and other law enforcement equipment appropriate for consideration in combatting terrorism applications, contact the National Institute of Justice, National Criminal Justice Reference Service, Washington, DC 20531. Specific information published by the Law Enforcement Standards Laboratory and the Technology Assessment Program Information Center may be of special interest and assistance to personnel involved in DoD Combatting Terrorism Programs.

APPENDIX T

VEHICLE BOMB SEARCH

<<VEHICLE BOMB SEARCH>>

CHECKLIST DELETED

<<VEHICLE BOMB SEARCH>>
CHECKLIST DELETED

APPENDIX U

KIDNAPPING AND HOSTAGE-TAKING: MOTIVATION AND PARTICIPATION

A. INTRODUCTION

1. Hostage-taking has been used to gain control and influence over the behavior of societies for centuries. The entire foundation of modern diplomatic practice rests on the concept of legitimate hostage-taking. Ambassadors and other emissaries were exchanged among feudal kingdoms to ensure their mutual health and safety. Modern legal concepts surrounding the practice of diplomatic immunity reflect the traditional practice of legitimate hostage-taking by modern nation states--exchange of diplomats.

2. Contemporary international legal norms clearly hold kidnapping and holding diplomats, civil servants, military personnel, corporate officials, independent business persons, scholars, teachers, and students hostage in pursuit of political goals and objectives by individual groups to be a form of terrorism. Such behavior is criminal under U.S. law.

3. The United States has enacted a domestic statute which makes assaults, kidnappings, murders, or conspiracies to commit such against American citizens abroad a crime subject to the jurisdiction of U.S. courts. Under this statute, the United States asserts a right to seek cooperative or coercive extradition from foreign jurisdictions for the purpose of prosecuting those individuals accused of such crimes.

B. MOTIVES KIDNAPPING AND HOSTAGE-TAKING

1. Publicity for a Cause

a. Kidnappings and taking of hostages can generate massive news media coverage. While the scope, intensity, and amount of coverage is difficult to predict, terrorists know that successful, dramatic kidnappings of newsworthy people, as well as hijackings of airplanes, ferries, trains, and cruise liners can generate huge volumes of publicity. Terrorists have been known to capitalize on the initial newsworthiness of a kidnapping or hijacking by implementing a media campaign. Interviews with selected hostages, guards, terrorist group supporters, and even terrorist group members are allowed for privileged members of the press.

b. As a general rule, to which there are many exceptions, the more newsworthy a potential victim is, the greater the likelihood that an attempt may be made against that person.

c. There is noteworthy corollary to this general rule. Some terrorists elect to kidnap and hold hostage individuals who are not especially newsworthy in and of themselves, but represent newsworthy interests, causes, or organizations. Terrorists, for example, have captured and held hostage Peace Corps workers, junior American diplomats, and because they were U.S. Government representatives. These kidnappings were far less newsworthy than the kidnapping of American Ambassadors in Uruguay, Sudan, or Afghanistan. Nevertheless, these actions illustrated to host-country nationals that the U.S. and host governments could not safeguard U.S. Government employees. [redacted]

2. Publicity for a Group

a. Some terrorists seek to use kidnappings and hostage-taking to generate press coverage for their own group. This tactic is counterintuitive because it is inconsistent with the need for terrorists to operate covertly and to obtain their support through clandestine means. On the other hand, it is entirely consistent with the tactical goal of terrorism: induce dysfunctional levels of fear in the target group, society, or country.

b. Terrorist attacks intended solely to promote dysfunctional fear in the target population tend to be especially violent and deadly. There are few, if any, compunctions among terrorists which might mitigate the scope, magnitude, or intensity of such attacks if the

FOR OFFICIAL USE ONLY

principal goal is to scare as many members of the target audience as possible. Violent, deadly attacks on persons with little or no obvious importance, carried out in especially visible and picturesque ways, send powerful messages to an unsuspecting populace. These actions say in effect—we the terrorists are all powerful; we can decide who will live and who will die; the government is no longer able to protect you.

3. Source of Funds or Supplies

Sometimes victims are selected for kidnapping because they are valuable to individuals or organizations; e.g., families, hometown friends, or employers. Families have paid ransoms. Contribution drives were started in the hostage's hometown to collect the ransom. Civilian firms are forced to pay ransoms because if they do not pay, employees will not want to work overseas. Sometimes, victims can be ransomed with supplies including food, medicine, weapons, and ammunition.

4. Symbols of Hated Authorities

a. Some terrorists develop world views that effectively dehumanize individuals and give human-like (anthropomorphic) qualities to societal institutions. For example, the "Government" or the "Church" becomes the enemy. These institutions, according to the terrorists, engage in repression, state-sanctioned violence against the people, robbing and enslaving the people, denying the people human rights, and so forth. As a consequence, human representatives of the enemy, be they police officers, mail carriers, civil servants or priests, monks, nuns, novitiates in the case of a church, are fair quarry.

b. American government representatives are often selected as targets by terrorists operating from this anti-authoritarian perspective, because the U.S. Government is frequently allied or associated with governments that are trying to deal with widespread social violence in a manner that appears to terrorists and their supporters to be repressive, violent, corrupt, and inconsistent with their perspectives on human rights. In conflicts based on such fundamental discrepancies in perceptions of right and wrong, proper and improper roles for social institutions, DoD personnel and their dependents are by their simple association with the U.S. Government at risk for kidnapping and being taken hostage.

c. On many occasions, hostages have been seized as symbols of hated authorities with the expressed intent of trading the hostages, dead or alive, for terrorist comrades incarcerated by the authorities.

5. Specific Threats to Terrorist Support or Activities

a. Terrorists will kidnap individuals identified as specific threats to their political and/or economic activities. As noted in Chapter 2, many terrorist groups operate within a tightly disciplined, cellular structure to protect the identity of its membership. Terrorist intelligence networks collect information about potential targets and defend the terrorist organizations against law enforcement efforts to arrest, prosecute, and incarcerate or punish members of the terrorist organization.

b. Terrorist organizations will kidnap and hold hostage individuals believed to be a threat to the survival of the organization. [redacted] Those kidnapped or taken hostage because they are perceived to be a threat to the long-term survival of a terrorist organization are in substantially greater peril than individuals taken hostage merely because they were present at the scene of a terrorist incident and might be able to identify members of the group.

C. TYPES OF HOSTAGE-TAKERS

Dr. Frederick Hacker, author of *Crusaders, Criminals and Crazies: Terror and Terrorism in Our Time*, divides hostage-takers into the three main groups. This is an easy way to remember broad, somewhat stylized categories of hostage-takers. As with all stereotypes, they are useful as an aid to understanding problems and possible remedies, but usually are of little help in dealing with specific situations.

1. Crusaders

a. Many hostage incidents involve political or religious extremists. Such extremists are labeled "crusaders."

b. "Crusaders" are highly motivated. They are capable of planning extensive, intricate, and very complete actions based on extensive intelligence collection against potential targets.

They organize their activities in a manner that makes detection difficult if not impossible. They frequently bring to bear knowledge, professional abilities, and social skills reflecting their middle to upper middle class upbringing.

c. "Crusaders" vary widely in personality, but seem to share certain common characteristics. They tend to be highly if not abnormally idealistic and inflexible. Sometimes they are prepared to die for their cause because of their dedication. They are not likely to give up hostages unless their own escape is guaranteed to their satisfaction.

d. Protecting DoD personnel and their dependents against kidnapping and hostage-taking efforts by terrorists who are "crusaders" is most challenging. When such terrorists are allied with states which provide logistic support, information, weapons, training, and even direction, DoD personnel may face a threat as formidable as one posed by special operating forces of potential adversary states.

2. Criminals

a. Common street criminals can become kidnappers or hostage-takers. Kidnapping and hostage-taking are usually the result of a bungled crime, not a politically inspired terrorist plan. Kidnapping or hostage-taking can occur in the midst of another crime. Kidnappings and hostage-taking are common, for example, in robberies or larcenies where the perpetrators commingle with innocent civilians and are caught on the premises by law enforcement officers.

b. Kidnapping and hostage-taking by criminals in the midst of a crime puts the victims in immediate danger. The criminal, the victim(s), and law enforcement personnel are virtually without script; tensions are high; fears and the ability to predict behavior on the part of adversaries is exceedingly low.

c. Victims in such circumstances have at least one factor that works in their favor. They have utility to their captors as bargaining chips for freedom. Victims who are injured or killed have no value to criminals; there is shared interest on the part of both the victim and the kidnapper in avoiding bodily harm. While this situation does not mean the victims are not at risk, it does suggest that the longer a hostage situation continues without violence, the greater the likelihood that hostages will eventually be released without further injury.

d. There is, however, an equally sobering corollary: In the event that a hostage situation becomes violent, it is possible, if not likely, the criminals will inflict injury or death upon the hostages as retribution against law enforcement authorities before the fact of their apprehension.

3. "Crazies" or Mentally Disturbed Individuals

a. Although individuals with diagnosed psychiatric or psychological conditions are not usually associated with organized terrorist groups, mentally disturbed individuals figure prominently in kidnappings and hostage-taking in the United States. Hostage-taking by mentally unstable individuals may be spontaneous or planned.

b. Victims of kidnappings and hostage-takings by mentally ill individuals may find themselves in extraordinarily difficult circumstances because of extreme difficulty in communicating with the kidnapper. In addition to language and cultural barriers, the victim must also find a vehicle or path around or through the kidnappers psychiatric and psychological impairments. Delusions and hallucinations characteristic of many mental illnesses probably will not impair the kidnapper's ability to use hostages for personal gain or other purposes. These conditions will, however, make it much more difficult for victims to reason or negotiate with "crazy" kidnappers.

c. Kidnappers acting out facets of their mental illnesses usually act alone. While capable of stalking potential victims, the "sole-proprietor" character of a mentally ill kidnapper's modus operandi facilitates detection and counteraction against this type of kidnapping threat. As is often the case, however, caution must be exercised in dealing with mentally ill kidnappers. They usually are as capable of committing violent acts against hostages as frightened criminals or calculating crusaders seeking press or ransom for their causes. In addition, the mentally ill hostage-taker may also have a death wish that can be satisfied by the murder of the hostages, suicide, or both.

D. MULTIPLE HOSTAGE-TAKING

1. Taking multiple hostages offers terrorists tactical advantages that may be offset by logistical disadvantages. Capture of multiple hostages; e.g., hijacking an airplane, or seizing and holding a building, places tremendous pressure on governments to respond to terrorist demands. There seems to be a threshold of public concern and sympathy for hostages and a willingness to respond to terrorist demands.

Individual hostages and groups of hostages greater than several hundred to several thousands evoke relatively little concern. Groups of hostages numbering in the 10's to 100's seem to evoke tremendous public concern that can be mobilized as pressure on governments to assent to terrorist demands.

2. Groups of hostages are attractive to terrorists for several reasons including the following:

a. Potential for finding a person of news interest (media).

b. Potential for finding a person of prominence (ransom).

c. Potential for finding a person who represents "the enemy" (retribution).

d. Potential to commit especially terrifying acts (airplane bombings, wholesale executions, etc.)

e. On the other hand, even if one hostage is good, more may not always be better from a terrorist's perspective. More hostages may mean the following:

(1) More people to feed, to water, and to provide for hygiene.

(2) More opportunities for hostage-led counteraction.

(3) More opportunities to make mistakes and generate sympathy for the hostages on the one hand and opposition to the cause on the other.

f. For some potential kidnappers, especially those terrorist groups operating without state support or state direction, safety for potential victims can be found in numbers. Being part of a large group while traveling or working makes it difficult to be singled out for kidnapping or being held hostage. The logistic requirements for such operations exceed the logistic support available to criminals, "crazies" and even many terrorist groups.

g. For other potential kidnappers, however, there is little or no safety to be found in numbers. Terrorist organizations operating with state support or state direction have the means, the opportunity, and the logistic support necessary to seize a large number of people. They can, for example, hijack an aircraft, land at a field controlled by a sympathetic if not co-operative government, provide minimal logistic support to sustain the terrorists and their hostages, and go through a careful review of the passengers until persons of value to the terrorists are found.

E. SUMMARY

Understanding the possible motivation underlying a kidnapping or hostage situation can be very important in helping victims develop strategies and tactics to minimize further risk of harm and to aid law enforcement authorities in bringing about a swift end to their situation. This appendix presents a broad overview; understanding the history, capability, and intentions of terrorist threat group operating in an area of concern combined with better understanding of possible kidnapping or hostage-taking motives may help combatting terrorism program managers design more effective measures to protect DoD-affiliated personnel.

APPENDIX V

CODE OF CONDUCT EDUCATIONAL MATERIALS

OVERVIEW

A. The following material is extracted from DoD Directive 1300.7 (reference (ii)).

B. Section I is a reproduction of Section B to Enclosure 2, Guidance for Instruction in Support of the Code of Conduct to DoD Directive 1300.7. This material restates each Article of the Code of Conduct and highlights educational objectives for Levels A, B, and C training.

C. Section II is a reproduction of Enclosure 3, Guidance for Instruction to Assist U.S. Military Personnel in Captivity or Hostile Detention During Peacetime, to reference (ii).

D. Use of these materials in support of Code of Conduct training for DoD personnel and their dependents as part of broader antiterrorism awareness, education, and training programs is encouraged.

SECTION I

ARTICLES OF THE CODE OF CONDUCT (E.O. 10631) AND IMPLEMENTING INSTRUCTIONS.

1. Article I. I AM AN AMERICAN, FIGHTING IN THE FORCES WHICH GUARD MY COUNTRY AND OUR WAY OF LIFE. I AM PREPARED TO GI MY LIFE IN THEIR DEFENSE.

a. Explanation

(1) Article I of the Code of Conduct (reference (b)) applies to all Service members at all times. A member of the Armed Force has a duty to support U.S. interests and oppose U.S. enemies regardless of the circumstances, whether in active participation in combat or in captivity.

(2) Medical personnel and chaplains are granted, by virtue of their special retained status under the Geneva Conventions (reference (h)), certain latitude under the Code of Conduct (reference (b)). That flexibility is directly related to the policies of the captors as to whether they adhere to the requirement of the Geneva Conventions (reference (h)) to let medical personnel and chaplains perform their professional duties. All personnel should understand the latitude and limits of this flexibility (see section C., below, of this enclosure).

b. Training Guidance for Levels A, B, and C. Familiarity with the wording and basic meaning of Article I is necessary to understand that:

(1) Past experience of capture Americans reveals that honorable survival in captivity requires that a Service member posses a high degree of dedication and motivation. Maintaining these qualities requires knowledge of and a strong belief in the following:

(a) The advantage of American democratic institutions and concepts.

(b) Love of and faith in the United States and a conviction that the U.S. cause is just.

(c) Faith in and loyalty to fellow POWs.

(2) Possessing the dedication and motivation fostered by such beliefs and trust shall enable POWs to survive long and stressful periods of captivity, and return to their country and families honorably with self-esteem intact.

2. Article II. I WILL NEVER SURRENDER OF MY OWN FREE WILL. IF IN COMMAND, I WILL NEVER SURRENDER THE MEMBERS OF MY COMMAND WHILE THEY STILL HAVE THE MEANS TO RESIST.

a. Explanation. Members of the Armed Forces may never surrender voluntari Even when isolated and no longer able to i casualties on the enemy or otherwise defenc selves, it is their duty to evade capture and in the nearest friendly force.

(1) It is only when evasion by Service members is impossible and further fighting would lead to their death with no significant loss to the enemy that the means to resist or evade might be considered exhausted.

(2) The responsibility and authority of a commander never extends to the surrender of command, even if isolated, cut off, or surrounded, while the unit has the power to resist, break out, or evade to rejoin friendly forces.

b. Training Guidance

(1) Levels A, B, and C. Training should ensure that each individual is familiar with the wording meaning of Article II, as stated in paragraph B.2.a., above.

(2) Levels B and C. Training should be oriented toward additional depth of knowledge on the following topics. Specifically, Service members must:

(a) Understand that when they are cut off, shot down, or otherwise isolated in enemy-controlled territory, they must make every effort to avoid capture. The courses of action available include concealment until recovered by friendly rescue forces, evasive travel to a friendly or neutral territory, and evasive travel to other prebriefed areas.

(b) Understand that capture does not constitute a dishonorable act if all reasonable means of avoiding it have been exhausted and the only alternative is death.

3. Article III. IF I AM CAPTURED I WILL CONTINUE TO RESIST BY ALL MEANS AVAILABLE. I WILL MAKE EVERY EFFORT TO ESCAPE AND AID OTHERS TO ESCAPE. I WILL ACCEPT NEITHER PAROLE NOR SPECIAL FAVORS FROM THE ENEMY.

a. Explanation. The duty of a member of the Armed Forces to continue resistance to enemy exploitation by all means available is not lessened by the misfortune of capture. Contrary to the 1949 Geneva Conventions (reference (h)), enemies whom U.S. forces have engaged since 1949 have regarded the POW compound as an extension of the battlefield. The POW must be prepared for this fact.

(1) In disregard of the Geneva Conventions (reference (h)), the enemy has used a variety of tactics to exploit POWs for propaganda purposes or to obtain military information. Resistance to captor exploitation efforts is required by the Code of Conduct (reference (b)). Physical and mental harassment, general mistreatment, torture, medical neglect, and political indoctrination have all been used against POWs in the past.

(2) The enemy has tried to tempt POWs to accept special favors or privileges not given to other POWs in return for statements or information desired by the enemy or for a pledge by the POW not to attempt escape.

(3) A POW must not seek special privileges or accept special favors at the expense of fellow POWs.

(4) The Geneva Conventions (reference (h)) recognize that the regulations of a POW's country may impose the duty to escape and that POWs may attempt to escape. Under the guidance and supervision of the senior military person and POW organization, POWs must be prepared to take advantage of escape opportunities whenever they arise. In communal detention, the welfare of the POWs who remain behind must be considered. A POW must "think escape," must try to escape if able to do so, and must assist others to escape.

(5) The Geneva Conventions (reference (h)) authorize the release of POWs on parole only to the extent authorized by the POW's country, and prohibit compelling a POW to accept parole. Parole agreements are promises given the captor by a POW to fulfill stated conditions, such as not to bear arms or not to escape, in consideration of special privileges, such as release from captivity or lessened restraint. The United States does not authorize any Military Service member to sign or enter into any such parole agreement.

b. Training Guidance

(1) Levels A, B, and C. Training should ensure that Service members are familiar with the wording and basic meaning of Article III, as stated in paragraph B.3.a., above.

(2) Levels B and C. Training should be oriented toward an additional depth of knowledge on the following topics. Specially, Service members must:

(a) Understand that captivity is a situation involving continuous control by a captor who may attempt to use the POW as a source of military information, for political purposes, and as a potential subject for political indoctrination.

(b) Be familiar with the rights and obligations of both the POW and captor under the Geneva Conventions of 1949 (reference (h)) and be aware of the increased significance of resistance should the captor refuse to abide by the provisions of the Geneva Conventions (reference (h)). Be aware that the resistance required by the Code of Conduct (reference (b)) is directed at captor exploitation efforts, because such efforts violate the Geneva Conventions (reference (h)). Understand that resistance beyond the identified above subjects the POW to possible punishment by the captor for order and discipline violations or criminal offenses against the detaining power.

(c) Be familiar with, and prepared for, the implications of the Communist Block Reservation to Article 85 of the Geneva Conventions (reference (h)). Article 85 offers protection to a POW legally convicted of a crime committed before capture. Understand that Communist captors often threaten to use their reservation to Article 85 as the basis for adjudging all members of opposing armed forces as "war criminals." As a result, POWs may find themselves accused of being "war criminals" simply because the waged war against their Communist captor before capture. The U.S. Government does not recognize the validity of this agreement.

(d) Understand that a successful escape by a POW causes the enemy to divert forces that might otherwise be fighting, provides the United States valuable information about the enemy and other POWs in captivity, and serves as a positive example to all members of the Armed Forces.

(e) Understand the advantages of early escape in that members of the ground forces are usually relatively near friendly forces. For all captured individuals, and early escape attempt takes advantage of the fact that the initial captors are usually not trained guards, that the security system is relatively lax, and that the POW is not yet in a debilitated physical condition.

(f) Be familiar with the complication of escape after arrival at an established POW camp, including secure facilities and an experienced guard system, increased distance from friendly forces, debilitated physical condition of prisoners, psychological factors that reduce escape motivation ("barbed-wire syndrome"), and the often differing ethnic characteristics of the escapee and the enemy population.

(g) Understand the importance of being alert for escape opportunities, especially for POWs immediately after capture, or when confined alone.

(h) Understand the command supervisory role of the senior military person and the POW organization in escapes from established POW camps. Understand the responsibilities of escapees to their fellow POWs.

(i) Understand that acceptance of parole means a POW has agreed not to engage in a specified act, such as to escape or to bear arms, in exchange for a stated privilege, and that U.S. policy forbids a POW to accept such parole.

(j) Understand the effects on POW organization and morale, as well as the possible legal consequences, of accepting a favor from the enemy that results in gaining benefits or privileges include acceptance of release before the release of sick or wounded POWs or those who have been captivity longer. Special favors include improved food, recreation, and living conditions not available to other POWs.

(3) Level C. Training should be oriented toward additional details and the topics set forth in subparagraph B.3.b.2., above, as well as understanding the necessity for and the mechanics of covert organizations in captivity. Those organizations serve the captive ends, such as effecting escape.

4. Article IV. IF I BECOME A PRISONER OF WAR, I WILL KEEP FAITH WITH MY FELLOW PRISONERS. I WILL GIVE NO INFORMATION OR TAKE PART IN ANY ACTION WHICH MIGHT BE HARMFUL TO MY COMRADES. IF I AM SENIOR, I WILL TAKE COMMAND. IF NOT, I WILL OBEY THE LAWFUL ORDERS OF THOSE APPOINTED OVER ME AND WILL BACK THEM UP IN EVERY WAY.

a. Explanation. Officers and non-commissioned officers shall continue to carry out their responsibilities and exercise their authority in captivity.

(1) Informing, or any other action detrimental to a fellow POW, is despicable and is expressly forbidden. POWs especially must avoid helping the enemy to identify fellow POWs who may have knowledge of value to the enemy and who may be made to suffer coercive interrogation.

(2) Strong leadership is essential to discipline. Without discipline, camp organization, resistance, and even survival may be impossible.

(3) Personal hygiene, camp sanitation, and care of the sick and wounded are imperative.

(4) Wherever located, POWs, for their own benefit, should organize in a military manner under the senior military POW eligible for command. The senior POW (whether officer or enlisted) in the POW camp or among a group of POWs shall assume command according to rank without regard to Military Service. That responsibility and accountability may not be evaded. (See section C, below, of this enclosure.)

(5) When taking command, the senior POW shall inform the other POWs and shall designate the chain of command. If the senior POW is incapacitated, or is otherwise unable to act for any reason, command shall be assumed by the next senior POW. Every effort shall be made to inform all POWs in the camp (or group) of the members of the chain of command who shall represent them in dealing with enemy authorities. The responsibility of subordinates to obey the lawful orders of ranking American military personnel remains unchanged in captivity.

(6) U.S. policy on POW camp organization requires that the senior military POW shall assume command. The Geneva Conventions (reference (h)) on POWs provide additional guidance to the effect that in POW camps containing enlisted personnel only, a prisoners' representative will be elected. POWs should understand that such a representative is regarded by U.S. policy only as a spokesperson for the senior POW. The prisoners' representative does not have command, unless the POWs elect the senior POW to be the prisoners' representative. The senior POW shall assume and retain actual command, covertly if necessary.

(7) Maintaining communications is one of the most important ways that POWs may aid one another. Communication breaks down the barriers of isolation that an enemy may attempt to construct and help strengthen a POW's will to resist. Each POW, immediately upon capture, shall try to make contact with fellow POWs by any means available and, thereafter, shall continue to communicate and participate vigorously as part of the POW organization.

(8) As with other provisions of the Code of Conduct, E.O. 10631, (reference (b)), common sense and the conditions in the POW camp will determine the way in which the senior POW and the other POWs structure their organization and carry out their responsibilities. It is important that:

(a) The senior POW establish an organization.

(b) The POWs in that organization understand their duties and know to whom they are responsible.

b. Training Guidance

(1) Levels A, B, and C. Training should ensure that Service members are familiar with the wording and basic meaning of Article IV, as stated in paragraph B.4.a., above, and understand that:

(a) Leadership and obedience to those in command are essential to the discipline required to effect successful organization against captor exploitation. In captivity situations involving two or more POWs, the senior ranking POW shall assume command; all others shall obey the orders and abide by the decisions of the senior POW regardless of differences in Military Service affiliations. Failure to do so shall result in the weakening of organization, a lowering of resistance, and, after repatriation, may result in legal proceedings under the UCMJ (reference (i)).

(b) Faith, trust, and individual group loyalties have great value in establishing and maintaining an effective POW organization.

(c) A POW who voluntarily informs or collaborates with the captor is a traitor to the United States and fellow POWs and, after repatriation, is subject to punishment under the UCMJ (reference (i)) for such actions.

(2) Levels B and C. Training should be oriented toward additional depth of knowledge on the following topics. Specifically, Service members must:

(a) Be familiar with the principles of hygiene, sanitation, health maintenance, first aid, physical conditioning, and food utilization, including recognition and emergency self-treatment of typical POW camp illnesses by emergency use of primitive materials and available substances (e.g., toothpaste, salt, and charcoal). Such knowledge exerts an important influence on POW ability to resist and assists an effective POW organization.

(b) Understand the importance of, and the basic procedures for, establishing secure communications between separated individuals and groups of POWs attempting to establish and maintain an effective organization.

(c) Be familiar with the major ethnic, racial, and national characteristics of the enemy that may affect POW-captor relationships to the detriment of individual POWs and the POW organization.

(d) Further understand that:

1. An informer or collaborator should be insulated from sensitive information on POW organization, but that continuing efforts should be made by members of the POW organization to encourage and persuade the collaborator to cease such activities.

2. Welcoming a repentant collaborator "back to the fold" is generally a more effective POW organization resistance technique than continued isolation, which only may encourage the collaborator to continue such treasonous conduct.

3. There is a significant difference between the collaborator who must be persuaded to return and the resister who, having been physically or mentally tortured into complying with a captor's improper demand (such as to provide information or a propaganda statement), should be helped to gather strength and resume resistance.

(e) Understand that, in situations where military and civilian personnel are imprisoned together, the senior military POW should make every effort to persuade civilian prisoners that the Military Service member's assuming overall command leadership of the entire prisoner group, based upon experience and specific training, is advantageous to the entire prisoner community.

(3) Level C.Understand the need for, and the mechanics of, establishing an effective covert organization in situations where the captor attempts to prevent or frustrate a properly constituted organization.

5. Article V. WHEN QUESTIONED, SHOULD I BECOME A PRISONER OF WAR, I AM REQUIRED TO GIVE NAME, RANK, SERVICE NUMBER, AND DATE OF BIRTH. I WILL EVADE ANSWERING FURTHER QUESTIONS TO THE UTMOST OF MY ABILITY. I WILL MAKE NO ORAL OR WRITTEN STATEMENTS DISLOYAL TO MY COUNTRY AND ITS ALLIES OR HARMFUL TO THEIR CAUSE.

a. Explanation. When questioned, a POW is required by the Geneva Conventions (reference (h)) and the Code of Conduct, E.O. 10631 (reference (b)), and is permitted by the UCMJ (reference (i)), to give name, rank, Service number, and date of birth. Under the Geneva Conventions (reference (h)), the enemy has no right to try to force a POW to provide any additional information. However, it is unrealistic to expect a POW to remain confined for years reciting only name, rank, Service number, and date of birth. There are many POW camp situations in which certain types of conversation with the enemy are permitted. For example, a POW is allowed, but not required by the Code of Conduct, the UCMJ, or the Geneva Conventions (references (b), (i), and (h)), to fill out a Geneva Conventions "capture card" to write letters home, and to communicate with captors on matters of health and welfare.

(1) The senior POW is required to represent fellow POWs in matters of camp administration, health, welfare, and grievances. However, it must be borne constantly in mind that the enemy has often viewed POWs as valuable sources of military information and propaganda that may be used to further the enemy's war effort.

(2) Accordingly, each POW must exercise great caution when filling out a "capture card" when engaging in authorized communication with the captor, and when writing letters. A POW must resist, avoid, or evade, even when physically and mentally coerced, all enemy efforts to secure statements or actions that may further the enemy's cause.

(3) Examples of statements or actions POWs should resist include giving oral or written confessions, answering questionnaires, providing personal history statements, making propaganda recordings and broadcast appeals to other POWs to comply with improper captor demands, appealing for U.S. surrender or parole, engaging in self-criticisms, or providing oral or written statements or communications on behalf of the enemy or harmful to the United States, its allies, the Armed Forces, or other POWs.

(4) A POW should recognize that any confession or statement may be used by the enemy as part of a false accusation that the captive is a war criminal rather than a POW. Moreover, certain countries have made reservations to the Geneva Conventions (reference (h)) in which they assert that a war criminal conviction has the effect of depriving the convicted individual of POW status, thus removing the POW from protection under the Geneva Conventions (reference (h)). The right to repatriation is thus revoked until a prison sentence is served.

(5) If a POW finds that, under intense coercion, unauthorized information was unwillingly or accidentally disclosed, the Service member should attempt to recover and resist with a fresh line of mental defense.

(a) Experience has shown that, although enemy interrogation sessions may be harsh and cruel, it is usually possible to resist, if there is a will to resist.

(b) The best way for a POW to keep faith with the United States, fellow POWs, and oneself is to provide the enemy with as little information as possible.

b. Training Guidance

(1) Levels A, B, and C. Training should ensure that Service members are familiar with the wording and basic meaning of Article V, as stated in paragraph B.5.A., above.

(2) Levels B and C. Additional understanding of the following topics should be acquired at levels B and C. Specifically, Service members must:

(a) Be familiar with the various aspects of the interrogation process, its phases, the procedures, methods and techniques of interrogation, and the interrogator's goals, strengths, and weaknesses.

(b) Understand that a POW is required by the Geneva conventions and the Code of Conduct (references (h) and (b)) to disclose name, rank, Service number, and date of birth, when questioned. Understand that answering further questions must be avoided. A POW is encouraged to limit further disclosure by use of such resistance techniques as claiming inability to furnish additional information because of previous orders, poor memory, ignorance, or lack of comprehension. The POW may never willingly give the captor additional information, but must resist doing so even if it involves withstanding mental and physical duress.

(c) Understand that, short of death, it is unlikely that a POW may prevent a skilled enemy interrogator, using all available psychological and physical methods of coercion, from obtaining some degree of compliance by the POW with captor demands. However, understand that if taken past the point of maximum endurance by the captor, the POW must recover as quickly as possible and resist each successive captor exploitation effort to the utmost. Understand that a forced answer on one point does not authorize continued compliance. Even the same answer must be resisted again at the next interrogation session.

(d) Understand that a POW is authorized by the Code of Conduct (reference (b)) to communicate with the captor on individual health or welfare matters and, when appropriate, on routine matters of camp administration. Conversations on those matters are not considered to be giving unauthorized information, as defined in subparagraph B.5.a(3), above.

(e) Understand that the POW may furnish limited information on family status and address in filling out a Geneva Conventions (reference (h)) capture card. Be aware that a POW may write personal correspondence. Be aware that the captor shall have full access to both the information on the capture card and the contents of personal correspondence.

(f) Be familiar with the captor's reasons for and methods of attempting to involve POWs in both internal and external propaganda activities. Understand that a POW must utilize every means available to avoid participation in such activities and must not make oral or written statements disloyal to the United States or its allies, or detrimental to fellow POWs.

(g) Be familiar with the captor's reasons for and methods of attempting to indoctrinate POWs politically. Be familiar with the methods of resisting such indoctrination.

(3) Level C Training should provide additional details, and Service members specifically should:

(a) Understand that, even when coerced beyond name, rank, Service number, date of birth, and claims of inabilities, it is possible to thwart an interrogator's efforts to obtain useful information by the use of certain additional ruses and stratagems.

(b) Understand and develop confidence in the ability to use properly the ruses and stratagems designed to prevent successful interrogation.

6. Article VI. I WILL NEVER FORGET THAT I AM AN AMERICAN, FIGHTING FOR FREEDOM, RESPONSIBLE FOR MY ACTIONS, AND DEDICATED TO THE PRINCIPLES WHICH MADE MY COUNTRY FREE. I WILL TRUST IN MY GOD AND IN THE UNITED STATES OF AMERICA.

a. Explanation. A member of the Armed Forces remains responsible for personal actions at all times. Article VI is designed to assist members of the Armed Forces to fulfill their responsibilities and survive captivity with honor. The Code of Conduct, E.O. 10631 (reference (b)), does not conflict with the UCMJ (reference (i)), and the latter continues to apply to each military member during captivity or other hostile detention.

(1) When repatriated, POWs can expect their actions to be subject to review, both as to circumstances of capture and as to conduct during detention. The purpose of such review is to recognize meritorious performance and, if necessary, investigate any allegations of misconduct.

(2) Such reviews will be conducted with due regard for the rights of the individual and consideration for the conditions of captivity.

(3) A member of the Armed Forces who is captured has a continuing obligation to resist all attempts at indoctrination and remain loyal to the United States.

(4) The life of a POW may be very hard. POWs who stand firm and united against enemy pressures shall aid one another immeasurably in surviving this ordeal.

b. Training Guidance for Levels A, B, and C. Training should ensure that members are familiar with the wording and basic meaning of Article VI, and:

(1) Understand the relationship between the UCMJ and the Code of Conduct, E.O. 10631 (references (i) and (b)), and realize that failure to follow the guidance of the Code of Conduct (reference (b)) may result in violation of reference (i). Every member of the Armed Forces of the United States should understand that Service members legally may be held accountable for personal actions while detained.

(2) Be knowledgeable of the national policy expressed by the President in reference (b) promulgating the Code of Conduct:

FOR OFFICIAL USE ONLY

No American prisoner of war will be forgotten by the United States. Every available means will be employed by our government to establish contact with, to support and to obtain the release of all our prisoners of war. Furthermore, the laws of the United States provide for the support and care of dependents of the armed forces including those who become prisoners of war. I assure dependents of such prisoners that these laws will continue to provide for their welfare.

(3) Understand that both the POW and dependents shall be taken care of by the Armed Forces and that pay and allowances, eligibility and procedures for promotion, and benefits for dependents continue while the POW is detained.

(4) Understand the importance of military members ensuring that their personal affairs and family matters (pay, powers of attorney, will, car payments, and children's schooling) are kept current through discussion, counseling or filing of documents before being exposed to risk of capture.

(5) Understand that failure to accomplish the matters set forth in subparagraph B.6.b.(4) above, has resulted in an almost overwhelming sense of guilt on the part of the POWs and has placed unnecessary hardship on family members.

C. SPECIAL ALLOWANCES FOR MEDICAL PERSONNEL AND CHAPLAINS

The additional flexibility afforded medical personnel and chaplains under the circumstance cited in the explanation to Article I is further clarified, as follows:

1. Article I

a. Medical personnel and chaplains are granted, by virtue of their special retained status under the Geneva Conventions (reference (h)), certain latitude under the Code of Conduct (reference (b)) if the policies of the captors adhere to the requirement of the Geneva conventions (reference (h)) permitting those personnel to perform their professional duties.

b. If the captors allow medical personnel and chaplains to perform their professional duties, those personnel may exercise a degree of flexibility with regard to some of the specific provisions of the Code of Conduct (reference (b)) to perform their professional duties.

c. This degree of flexibility only may be employed if it is in the best interests of the medical and spiritual needs of fellow POWs and the United States. Like all members of the Armed Forces, medical personnel and chaplains are accountable for their actions.

2. Article II. No additional flexibility.

3. Article III. Under the Geneva Conventions (reference (h)), medical personnel and chaplains who fall into the hands of the enemy are entitled to be considered "retained personnel" and are not to be considered POWs. The enemy is required by the Geneva Conventions (reference (h)) to allow such persons to continue to perform their medical or religious duties, preferably for POWs of their own country. When the services of those "retained personnel" are no longer needed for these duties, the enemy is obligated to return them to their own forces.

a. The medical personnel and chaplains of the U.S. Armed Forces, who fall into the hands of the enemy, must assert their rights as "retained personnel" to perform their medical and religious duties for the benefit of the POWs and must take every opportunity to do so.

b. If the captor permits medical personnel and chaplains to perform their professional functions for the welfare of the POW community, special latitude is authorized those personnel under the Code of Conduct, E.O. 10631 (reference (b)), as it applies to escape.

c. Medical personnel and chaplains, as individuals, do not have a duty to escape or to actively aid others in escaping as long as they are treated as "retained personnel" by the enemy. U.S. experience since 1949, when the Geneva Conventions (reference (h)) were written, reflects no compliance by captors of U.S. personnel with those provisions of the Geneva conventions (reference (h)). U.S. medical and chaplain personnel must be prepared to be subjected to the same treatment as other POWs.

d. If the captor does not permit medical personnel and chaplains to perform their professional functions, they are considered identical to all other POWs with respect to their responsibilities under the Code of Conduct (reference (b)). Under no circumstances shall the latitude granted medical personnel and chaplains be interpreted to authorize any actions or conduct detrimental to the POWs or the interest of the United States.

4. Article IV. Medical personnel generally are prohibited from assuming command over nonmedical personnel and chaplains generally are prohibited from assuming command over military personnel of any branch. Military service regulations that restrict eligibility of those personnel for command shall be explained to all personnel at an appropriate level of understanding to preclude later confusion in a POW camp.

5. Article V. This Article and its explanation also apply to medical personnel and chaplains ("retained personnel"). They are required to communicate with a captor in connection with their professional responsibilities, subject to the restraints discussed in Articles I, above, and VI, below.

6. Article VI. No additional flexibility.

SECTION II

GUIDANCE FOR INSTRUCTION TO ASSIST U.S. MILITARY PERSONNEL IN CAPTIVITY OR HOSTILE DETENTION DURING PEACETIME

A. POLICY

This policy on the conduct of U.S. military personnel, isolated from U.S. control, applies at all times. U.S. military personnel finding themselves isolated from U.S. control are required to do everything in their power to follow DoD policy. The DoD policy in this situation is to survive with honor.

B. SCOPE

The Code of Conduct, E.O. 10631 (reference (b)) is a moral guide designed to assist military personnel in combat or being held as POWs to live up to the ideals in the DoD policy. The guidance in this enclosure shall assist U.S. military personnel who find themselves isolated from U.S. control in peacetime, or in a situation not related specifically in the Code of Conduct (reference (b)). This enclosure is the special guidance referred to in paragraph A.3.b. of enclosure 2. Procedures shall be established by the Military Departments to ensure that all U.S. military personnel under their control are made aware of the guidance in this enclosure. Dissemination procedures should parallel those used to ensure proper education and training in support of the Code of Conduct (reference (b)) throughout the Department of Defense.

C. RATIONALE

U.S. military personnel, because of their wide range of activities, are subject to peacetime detention by unfriendly governments or captivity by terrorist groups. The guidance in this enclosure seeks to help U.S. military personnel survive those situations with honor and does not constitute a means for judgment or replace the UCMJ (reference (i)) as a vehicle for enforcement of proper conduct. The guidance in this enclosure, although exactly the same as the Code of Conduct (reference (b)) in some areas, applies only during peacetime. The term "peacetime" means that armed conflict does not exist or where armed conflict does exist, but the United States is not involved directly. For specific missions or in areas of assignment where U.S. military personnel may have a high risk of peacetime detention or terrorist captivity, the Military Services are obligated to provide training and detailed guidance to such personnel to ensure their adequate preparation for the situation. Training shall be reviewed and monitored for adequacy and consistency with this guidance by the Executive Agent for the ASD(FM&P).

D. GENERAL

U.S. military personnel captured or detained by hostile foreign governments or terrorists often are held for exploitation of the captives, or the U.S. Government or both. That exploitation may take many forms, but each form of exploitation is designed to assist the foreign government or the terrorist captors. In the past, detainees have been exploited for information and propaganda efforts, including confessions to crimes never committed, all of which assisted or lent credibility to the detainer. Governments also have been exploited in such situations to make damaging statements about themselves or to force them to appear weak in relation to other governments. Ransoms for captives or terrorists have been paid by governments, and such payments have improved terrorist finances, supplies, status, and operations, often prolonging the terror carried on by such groups.

E. RESPONSIBILITY

U.S. military personnel, whether detainees or captives, may be assured that the U.S. Government shall make every good faith effort to obtain their earliest release. Faith in one's country and its way of life, faith in fellow detainees or captives, and faith in one's self are critical to surviving with honor and resisting exploitation. Resisting exploitation and having faith in these areas are the responsibility of all Americans. On the other hand, the destruction of such faith must be the assumed goal of all captors determined to maximize their gains from a detention or captive situation.

F. GOAL

Every reasonable step must be taken by U.S. military personnel to prevent exploitation of themselves and the U.S. Government. If exploitation may not be prevented completely, every step must be taken to limit exploitation as much as possible. Detained U.S. military personnel often are catalysts for their own release, based on their ability to become unattractive sources of exploitation, i.e., one who resists successfully may expect detainers to lose interest in further exploitation attempts. Detainees or captives very often must make their own judgments as to which actions shall increase their chances of returning home with honor and dignity. Without exception, the military member who may say honestly that he or she has done his or her utmost in a detention or captive situation to resist exploitation upholds DoD policy, the founding principles of the United States, and the highest traditions of military service.

G. MILITARY BEARING AND COURTESY

Regardless of the type of detention or captivity, or harshness of treatment, U.S. military personnel shall maintain their military bearing.

They should make every effort to remain calm, courteous, and project personal dignity. That is particularly important during the process of capture and the early stages of internment when the captors may be uncertain of their control over the captives. Discourteous, unmilitary behavior seldom serves the long-term interest of a detainee, captive, or hostage. Additionally, it often results in unnecessary punishment that serves no useful purpose. Such behavior, in some situations, may jeopardize survival and severely complicate efforts to gain release of the detained, captured, or hostage-held military member.

H. CLASSIFIED INFORMATION

There are no circumstances in which a detainee, or captive, should voluntarily give classified information or materials to those who are unauthorized to receive them. To the utmost of their ability, U.S. military personnel held as detainees, captives, or hostages shall protect all classified information. An unauthorized disclosure of classified information, for whatever reason, does not justify further disclosures. Detainees, captives, and hostages must resist, to the utmost of their ability, each and every attempt by their captor to obtain such information.

I. CHAIN OF COMMAND

In group detention, captivity, or hostage situations, military detainees, captives or hostages shall organize, to the fullest extent possible, in a military manner under the senior military member present and eligible to command. The importance of such organization may not be overemphasized. Historically, in both peacetime and wartime, establishment of a military chain of command has been a tremendous source of strength for all captives. Every effort shall be made to establish and sustain communications with other detainees, captives, or hostages. Military detainees, captives, or hostages shall encourage civilians being held with them to participate in the military organization and accept the authority of the senior military member. In some circumstances, such as embassy duty, military members may be under the direction of a senior U.S. civilian official. Notwithstanding such circumstances, the senior military member still is obligated to establish, as an entity, a military organization and to ensure that the guidelines in support of the the DoD policy to survive with honor are not compromised.

J. GUIDANCE FOR DETENTION BY GOVERNMENTS

Once in the custody of a hostile government, regardless of the circumstances that preceded the detention situation, detainees are subject to the laws of that government. Detainees shall maintain military bearing and should avoid any aggressive, combative, or illegal behavior. The latter might complicate their situation, their legal status, and any efforts to negotiate a rapid release.

1. As American citizens, detainees should be allowed to be placed in contact with U.S. or friendly embassy personnel. Detainees should ask immediately and continually to see U.S. embassy personnel, or a representative of an allied or neutral government.

2. U.S. military personnel who become lost or isolated in a hostile foreign country during peacetime shall not act as combatants during evasion attempts. Since a state of armed conflict does not exist, there is no protection afforded under the Geneva Conventions (reference (h)). The civil laws of that country apply. Delays in contacting local authorities may be caused by injuries affecting the military member's mobility, disorientation, fear of captivity, or a desire to see if a rescue attempt might be made.

3. Since the detainer's goals may be maximum political exploitation, U.S. military personnel who are detained must be extremely cautious of their captors in everything they say and do. In addition to asking for a U.S. representative, detainees should provide name, rank, social security account number, date of birth, and the innocent circumstances leading to their detention. Further discussions should be limited to and revolve around health and welfare matters, conditions of their fellow detainees, and going home.

a. Historically, the detainers have attempted to engage military captives in what may be called a "battle of wits" about seemingly innocent and useless topics as well as provocative issues. To engage any detainer in such useless, if not dangerous, dialogue only enables a captor to spend more time with the detainee. The detainee should consider dealings with his or her captors as a "battle of wills;" the will to restrict discussion to those items that relate to the detainee's treatment and return home against the detainer's will to discuss irrelevant, if not dangerous, topics.

b. As there is no reason to sign any form or document in peacetime detention, detainees shall avoid signing any document or making any statement, oral or otherwise. If a detainee is forced to make a statement or sign documents, he or she must provide as little information as possible and then continue to resist to the utmost of his or her ability. If a detainee writes or signs anything, such action should be measured against how it reflects on the United States and the individual as a member of the military, or how it could be misused by the detainer to further the detainer's ends.

c. Detainees are not likely to earn their release by cooperation. Release may be gained by the military member doing his or her best to resist exploitation, thereby reducing his or her value to a detainer, and thus prompting a hostile government to negotiate seriously with the U.S. Government.

4. U.S. military detainees should not refuse to accept release, unless doing so requires them to compromise their honor or cause damage to the U.S. Government or its allies. Persons in charge of detained U.S. military personnel shall authorize release of any personnel under almost all circumstances.

5. Escape attempts shall be made only after careful consideration of the risk or violence, chance of success, and detrimental effects on detainees remaining behind. Jailbreak in most countries is a crime. Escape attempts would provide the detainer with further justification to prolong detention by charging additional violations of its criminal or civil law and might result in bodily harm or even death to the detainee.

K. GUIDANCE FOR CAPTIVITY BY TERRORISTS

Capture by terrorists is generally the least predictable and structured form of peacetime captivity. The captor qualifies as an international criminal. The possible forms of captivity vary from spontaneous hijacking to a carefully planned kidnapping. In such captivities, hostages play a greater role in determining their own fate since the terrorists in many instances expect or receive no rewards for providing good treatment or releasing victims unharmed. If U.S. military personnel are uncertain whether captors are genuine terrorists or surrogates of government, they should assume that they are terrorists.

1. If assigned in, or traveling through, areas of known terrorist activity, U.S. military personnel shall exercise prudent antiterrorism measures to reduce their vulnerability to capture. During the process of capture and initial internment, they should remain calm and courteous, since most casualties among hostages occur during this phase.

2. Surviving in some terrorist detentions may depend on hostages conveying a personal dignity and apparent sincerity to the captors. Hostages may discuss nonsubstantive topics such as sports, family, and clothing, to convey to the terrorists the captive's personal dignity and human qualities. They shall make every effort to avoid embarrassing the United States and the host government. The purpose of that dialogue is for the hostage to become a "person" in the captor's eyes, rather than a mere symbol of his or her ideological hatred. Such a dialogue also should strengthen the hostage's determination to survive and resist. A hostage also may listen actively to the terrorist's feeling about his or her cause to support the hostage's desire to be a "person" to the terrorist. However, he or she should never pander, praise, participate, or debate the terrorist's cause with him or her.

3. U.S. military personnel held hostage by terrorists should accept release using guidance in subsection J.4., above. U.S. military personnel must keep faith with their fellow hostages and conduct themselves according to the guidelines of this enclosure. Hostages and kidnap victims who consider escape to be their only hope are authorized to make such attempts. The hostage must weigh carefully the unique circumstances of the terrorist situation and all aspects of a decision to attempt escape.

APPENDIX W

COMBATTING TERRORISM CHECKLIST FOR NEW MANAGERS AND COMMANDERS

CHECKLIST DELETED

CHECKLIST DELETED

APPENDIX X

CRISIS MANAGEMENT PLAN CHECKLIST

<<CRISIS MANAGEMENT PLAN>>
CHECKLIST DELETED

FOR OFFICIAL USE ONLY

<<CRISIS MANAGEMENT PLAN>>
CHECKLIST DELETED

Appendix X-2

FOR OFFICIAL USE ONLY

<<CRISIS MANAGEMENT PLAN>>
CHECKLIST DELETED

Appendix X-3

FOR OFFICIAL USE ONLY

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX Y

CRISIS MANAGEMENT PLAN FORMAT

OVERVIEW

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.

While the format presented is most applicable to the Military Services or organizations under the control of Unified and Specified Commands, the approach outlined may be helpful to managers of OSD Agencies as they consider appropriate mechanisms to protect activities, organizations, personnel, and materiel under their control.

<<CRISIS MANAGEMENT PLAN>>
FORMAT DELETED

Appendix Y-2

FOR OFFICIAL USE ONLY

<<CRISIS MANAGEMENT PLAN>>
CHECKLIST DELETED

Appendix Y-3

FOR OFFICIAL USE ONLY

<<CRISIS MANAGEMENT PLAN>>
CHECKLIST DELETED

APPENDIX Z

BOMB AND HOSTAGE THREAT TELEPHONE CALL PROCEDURES

1. Upon receiving an anonymous telephone call:
   a. Try to keep a word for word 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 or she 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 security officer or the officer of the day.
2. During the call:
   a. Try to obtain answers to the questions listed on the telephone threat information sheets found as attachments 1 or 2 to 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 complete, 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.

Enclosures - 2

1. Telephone Threat Information Sheet
2. Threat Information Sheet

<<TELEPHONE THREAT INFORMATION SHEET>>

ENCLOSURE DELETED

<<TELEPHONE THREAT INFORMATION SHEET>>

ENCLOSURE DELETED

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX AA

TERRORIST INCIDENT RESPONSE: PUBLIC AFFAIRS GUIDANCE

A. INTRODUCTION

1. A major goal of terrorist groups is to capture the attention of the news media. During and immediately after a terrorist incident occurring on a Defense Department installation or involving DoD personnel, the Public Affairs Officer (PAO) plays an important role in supporting U.S. Government policy, in maintaining the flow of authoritative information between the authorities and the media, and in protecting the interests of hostages or DoD personnel participating in the resolution of the incident.

2. The PAO has specific functions to perform, including screening information provided to the media to ensure operational security, preserving the privacy of hostages, victims, and their families, and advising DoD and other U.S. Government or foreign government officials managing the crisis on public affairs matters.

B. BACKGROUND

1. Risks

Many aspects of combatting terrorism operations are inherently sensitive and may involve various risks to DoD personnel or their dependents which may be heightened by the release of information to the public. These include (1) risks to the personal safety of law enforcement and intelligence personnel involved in terrorism investigations, analyses, or other related activities; (2) the risk of jeopardizing follow-on activities related to a terrorist incident ; (3) the risk of jeopardizing the prosecution of people arrested for terrorist acts which inherently involve criminal acts; (4) risks to the operational security (OPSEC) of on-going operations; (5) risks to intelligence systems and sources; and (6) the risks to relations with other governments whose citizens, vessels, territory, etc., may be involved in terrorist activities, either by providing support or direction, or by being targets for future terrorist assault. These risks can be minimized only through a comprehensive coordination process before any information is released to the public.

2. Teamwork

[redacted]rely will a single agency and/or organization be able to take full credit for the termination of an event and the successful restoration of public order. By their nature, DoD combatting terrorism and counterterrorism efforts triggered by a terrorist incident will never be unilateral. They always will be in support of U.S. law enforcement agencies or cooperating host national military, police or security forces.

C. RELEASE OF INFORMATION

1. Policy Statements

DoD components will not attempt to publicly discuss or interpret overall DoD policy regarding use of armed forces in law enforcement matters. Components may provide copies of speeches and other printed material originated within OSD, but will refer to OASD(PA) any news media questions on matters beyond their purview.

2. Missions Statements

Previously approved statements and associated Q's and A's pertaining to unified/specified command missions in the DoD effort may be used by the commands concerned in the military departments for public affairs purposes as they deem appropriate.

3. Announcements of Investigations and Arrests

The announcement regarding a terrorism-related investigation or arrest normally will be made by the agency/organization that conducted the investigation or actually made the arrest. Such announcements will indicate that the operation was a "coordinated federal effort" and will list participating agencies and/or

organizations following coordination with each. Although DoD Components will not make announcements of investigations and arrests, it may be of interest to note the general ground rules that the law enforcement agencies observe in making such announcements.

a. The normally will include the following:

(1) That an investigation has been launched or completed.

(2) Than an arrest has been made.

(3) Name and home town of the suspect.

(4) Description of act for which the individual(s) is charged.

(5) Date, time and general location of the arrest.

(6) List of all agencies and organizations participating in investigation and/or arrest (unless precluded by OPSEC on the request of a participating agency and/or organization) to include combined operations with other nations or state and local law enforcement agencies.

(7) Whether resistance or pursuit was involved.

(8) Video if it goes through lead agency and/or organization which must clear the release with the U.S. attorney handling the case.

(9) Numbers of DoD casualties resulting from a terrorist incident in general terms, including general discussion of medical condition (grave, very critical, critical, serious, acute, treated and released from the hospital, treated as the scene)

(10) General statement as to the damage to DoD property; provided that no statement shall be made that would allow terrorists to estimate the results of an attack had it been executed in a different matter.

[redacted]

([redacted]

(2) [redacted]

(3) [redacted]

(4) [redacted]

(5) [redacted]

(6) [redacted]

(7) [redacted]

(8) [redacted]

(9) [redacted]

(10) [redacted]

4. News Media Travel on DoD Missions

a. Approval to provide transportation to news media seeking to cover a terrorist incident involving DoD personnel shall be in accordance with reference (nn).

b. Once approval is granted, the following guidelines apply:

(1) Embarked media have exclusive rights to whatever material they gather unless a prior pool agreement has been made.

(2) Media may not be given access to classified or sensitive law enforcement information, but otherwise should be allowed to cover all activities.

(3) Media may, at the discretion of the Commanding Officer (in consultation with the senior U.S. Government official on scene), embark on military vehicles to observe antiterrorist responses in progress

(4) Media may not interview prisoners.

(5) Media may be afforded reasonable access to document activities of DoD personnel responding to a terrorist incident; provided that in so doing, media representatives do not expose themselves to hostile or friendly fire, nor do they interfere in any manner with the combatting terrorism program response.

(6) Media may photograph and/or videotape prisoners only as they are moved in the normal course of business; e.g., from a vessel to a dock, from a building to a vehicle, etc. Prisoners will not be lined up for media photography.

(7) The following personnel will not be photographed by media in such a way that they can be readily identified: law enforcement, DoD personnel and host-nation military, policy, or security personnel.

(8) All on-scene agencies and/or organizations will be made aware of media presence and which areas media will be in.

(9) Media must remain with the escort officers at all times, until released, and follow their instructions regarding their activities. These instructions are not intended to hinder reporting by media, but are given only to facilitate movement of media and ensure safety.

(10) Media will be cautioned that they cannot report on:

(a) Course, speed, estimated arrival times and other similar information on ship or aircraft embarks.

(b) Sensitive equipment and/or capabilities that they might observe or come in contact with.

(c) Future operations of forces assigned.

(d) Tactics (in use or planned) to voice various threats of terrorists.

(e) Specific locations of ships, aircraft or ground forces. Instead, media will use "on board the U.S.S. (name) in the (name) sea/ocean" or "along the southwest border with the (law enforcement agency) and the U.S. (branch of service)."

(11) Ground rules may be modified by the operational commander to adapt to changing media requirements and operational considerations.

(12) Media representatives who do not abide by the ground rules are subject to expulsion and jeopardize future media embarks.

(13) Media representatives may suggest other arrangements for consideration and adoption as the situations change.

(14) Media participation on a combatting terrorism response embark indicates their understanding of these guidelines and their willingness to abide by them.

D. INTERVIEWS AND PRESS CONFERENCES

1. Interviews

a. Numerous interview requests concerning the DoD Combatting Terrorism Program may be received at the installation, base or unit levels. OASD(PA) has no objection to such interviews if the following criteria are met:

(1) All interviews will be on the record.

(2) Interviewees will discuss only information within their personal purview and expertise. No classified information will be discussed.

(3) Interviewees will not discuss or interpret overall DoD policy regarding armed forces support of the U.S. Government's Counterterrorism efforts; i.e., preemptive or retaliatory use of force against terrorist groups, their state sponsors, or states which direct terrorist attacks against U.S. interests.

(4) Responses given during the interview will meet operational security requirements. Interviewees wishing to protect their identity must establish appropriate media ground rules prior to interview. Appropriate public affairs offices must be included in planning and conducting all interviews.

(5) Interviewees will not answer questions regarding hypothetical situations. Furthermore, interviewees will not comment on matters pertaining to other U.S. federal/state/local organizations/agencies and/or the military, police or security forces of other nations.

(6) A summary of controversial interview discussions and/or notification of interview results that might require OASD(PA) response will be provided through appropriate command channels to OASD(PA):DDI.

2. **Joint Press Conferences**

a. DoD spokespersons may be invited to participate in joint press conferences organized by federal/state/local law enforcement agencies following the conclusion of a terrorist episode involving DoD personnel, facilities, or materiel or where DoD support contributed to the success of the combatting terrorism operation. OASD(PA) has no objection to such participation if the following criteria are met:

(1) Appropriate public affairs offices in the chain of command must be included in the planning for such press conferences.

(2) Spokespersons will discuss only information within their personal purview and expertise. No classified information will be discussed.

(3) Spokespersons will not discuss or interpret overall DoD policy regarding armed forces support of the U.S. Government's Counterterrorism policy (use of force against terrorist groups, their state supporters, or those states which direct attacks by terrorist groups against U.S. interests).

(4) Responses given during the press conference will meet operational security requirements.

(5) Spokespersons will not answer questions on hypothetical situations. They will not comment on matters pertaining to other U.S. federal organizations and/or agencies and/or the military, policy or security forces of other nations.

(6) After-action reports and/or transcripts of press conferences will be provided through appropriate command channels to OASD(PA)/DDI.

3. **Training Versus Operations**

OASD(PA) understands that media may be interested in covering training involving the Department of Defense and other agencies to get an idea of the type of support the Department of Defense is providing. OASD(PA) has no objection to this type of coverage as long as thorough coordination has been completed with other agencies and foreign govern-ments where foreign personnel are involved, and operational security considerations have been addressed.

D. COORDINATION PROCEDURES

1. **Interagency Public Affairs Coordination Efforts**

a. Early contact with local/regional public affairs counterparts or designated spokespersons in other agencies/organizations is encouraged. This will enable DoD PAO's to establish a working relationship with their agency counterparts and more importantly, it will identify DoD points of contact for the other agencies. This becomes important when the lead agencies release information or hold press conferences regarding combatting terrorism operations with DoD involvement. Determining who must be coordinated with is a process that will be unique to each command, but there are some generalities that can be applied to all combatting terrorism operations to help you make that determination.

(1) Operational Channels

Start with the command's operations section. The operators are probably already dealing with these other agencies when planning DoD support. They should known which agencies are involved, who will have operational control, etc.

(2) Joint Task Forces

Is there an established DoD joint task force in your command area?

(3) U.S. Embassy

In foreign countries, the U.S. Embassy can put you in touch with appropriate spokespersons for combatting terrorism operations in host countries.

(4) Request Coordinating Instructions

If you still cannot determine points of contact in participating agencies for a particular combatting terrorism operations, request coordinating instructions when submitting proposed public affairs guidance for that operation through your chain of command. Depending on the nature of the request, it would eventually reach OASD(PA) where the request for coordinating instructions would be staffed with the appropriate federal agencies. The response would be sent back through your chain of command.

b. Coordinating departments and agencies at the Federal level include:

(1) Department of State (all overseas DoD activities)

(2) Department of Justice

(a) Federal Bureau of Investigation (all CONUS and selected overseas DoD activities where FBI jurisdiction is asserted)

(b) Drug Enforcement Administration

(3) Department of the Treasury

(a) Bureau of Alcohol, Tobacco and Firearms

(b) U.S. Customs Service

(c) U.S. Secret Service

(4) Department of Transportation

(a) Federal Aviation Administration

(b) U.S. Coast Guard

(5) United States Information Agency

(6) Department of Energy

(7) Nuclear Regulatory Commission

(8) General Services Administration

c. Each agency listed above has its own method of granting approval for release of information. It is important to understand this when coordinating public affairs activities. All of these agencies require that policy issues be forwarded to the national level. Remember that the potential to attract national and international media attention to the Department of Defense combatting terrorism efforts has increased significantly since the destruction of the Marine Barracks in Beirut, the murder of Petty Officer Stethem, and continuing assaults on DoD personnel in the Eastern Mediterranean region. Keep the chain of command informed.

E. SENSITIVE ISSUES

[redacted]

[redacted]

F. [redacted]

Enclosure: Public Affairs Checklist

ENCLOSURE 1

PUBLIC AFFAIRS CHECKLIST

A. PAO FUNCTIONAL CONSIDERATIONS

The following checklist contains outlines functional considerations for the PAO during a crisis management situation:

1. ___ Check with the center commander upon entering the operations center.
2. ___ Establish a public affairs plan to include a location for the media.
3. ___ Disseminate information to the news media in accordance with the established plan.
4. ___ Control press releases.
5. ___ Coordinate press releases with commander, other operations center staff and higher echelon PAO before release.
6. ___ Control movement of news media personnel with press passes, escorts, etc.
7. ___ Obtain approval for the following items from the commander:
   - (a) ___ News releases.
   - (b) ___ News media personnel to enter outer perimeter.
   - (c) ___ Release of photographs of suspects, victims, and immediate scene.
   - (d) ___ Interviews with anyone other than the commander.
   - (e) ___ Direct communication with press personnel and suspect(s).

B. FOCUS

The major public affairs focus of the antiterrorist plan should be to ensure accurate information is provided to all publics (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.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX BB

DoD THREATCON SYSTEM

SECTION I
BASIC THREATCON PROCEDURES

A. GENERAL

1. The threat conditions (THREATCONs) outlined below describe the progressive level of a terrorist threat to all U.S. military facilities, assets, and personnel under DoD Direc-tive 0-2000.12 (reference (a)). As approved by the Joint Chiefs of Staff, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of U.S. Military antiterrorism activities.

2. The purpose of the THREATCON system is accessibility to, and easy dissemination of, appropriate information. The declaration, reduction, and cancellation of THREATCONs remains the exclusive responsibility of the commanders specified in the order.

3. While 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.

4. Once a THREATCON is declared, the selected security measures are implemented immediately. Directive DoD 0-2000.12 (reference (a)) recommended measures are:

B. THREATCON NORMAL

THREATCON NORMAL exists when a general threat of possible terrorist activity exists, but warrants only a routine security posture.

C. THREATCON ALPHA

1. 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.

2. It may be necessary, however, 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.

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

e. [redacted]

f. [redacted]

g. [redacted]

h. [redacted]

i. [redacted]

j. [redacted]

D. THREATCON BRAVO

1. THREATCON BRAVO applies when an increased and more predictable threat of terrorist activity exists.

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>
MEASURES DELETED

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>
MEASURES DELETED

<<THREATCON PROCEDURES>>
MEASURES DELETED

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>
MEASURES DELETED

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>
MEASURES DELETED

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>

MEASURES DELETED

Appendix BB-7

FOR OFFICIAL USE ONLY

<<THREATCON PROCEDURES>>
MEASURES DELETED

FOR OFFICIAL USE ONLY

APPENDIX CC

PERSONNEL SEARCH TECHNIQUES

A. INTRODUCTION

During the course of higher alert states, it may be necessary to augment the security force with additional personnel who have not received as much training in law enforcement techniques as their regular security personnel counterparts. The information provided below is intended to be used a reference material in conjunction with additional field training for regular and backup security personnel.

B. GENERAL SEARCH TECHNIQUE

1. Position the person being searched out from a wall (or car) with legs apart and hands against the wall in a leaning position, in such a way that he cannot move without falling down, or can be easily knocked over.

a. The searcher should always work from behind.

b. Two searchers should be employed, one searching and the other covering.

c. All searches are conducted in a business-like manner with conversation limited to requests and/or instruction necessary for conduct of the search. Extend proper respect to all personnel being searched; the aim is to provide security without creating animosities that could develop into trouble in the future.

C. TYPES OF SEARCH.

1. There are two types of search:

a. Quick body search or frisk.

b. Detailed body search.

D. QUICK BODY SEARCH OR FRISK

1. The frisk is used either as a preliminary search to detect weapons, or as the usual from of search in a low threat area (perhaps 1 out of 10 people can be selected for the detailed search).

a. Follow a logical sequence from head to toe. Use both hands and stroke (rather than pat) all clothing. If possible, for quick body searches, a metal detection system should be used.

b. The following areas should be carefully checked:

(1) Hair, and in or under hats.

(2) Armpits.

(3) Inside legs.

(4) Groin or crotch area.

(5) Half-clenched hands

(6) Any medical dressings.

(7) Any bags or cases carried.

(8) Walking sticks, umbrellas, crutches, etc.

(9) Shoes/boots.

E. DETAILED BODY SEARCH.

1. Where possible, a special room or area should be set aside for this; a doctor and female searcher should also be in attendance. The following sequence should be used:

a. Establish identity.

b. Establish ownership to baggage.

c. Invite person to turn out all pockets.

d. Invite person to remove all clothes, jewelry, watches, etc.

e. Inspect body from head to foot, paying special attention to hair, ears, mouth, teeth, body orifices, crotch, groin, between toes, etc.

f. Examine clothing, paying particular attention to linings, seams, buttons, belts, shoe/boot soles and heels, etc.

g. Examine contents of pockets.

h. Examine baggage and other articles (sticks, umbrellas, etc.)

F. REMEMBER ALWAYS

1. WOMEN MUST SEARCH WOMEN; MEN MUST SEARCH MEN.

2. Watch for facial reactions, nervousness, or sweating.

3. Work in pairs and search each individual separately.

4. Be courteous.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX DD

CALCULATED AND ANALYZED BLAST EFFECTS

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-3

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-4

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-6

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-10

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-11

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-13

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

450

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-15

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-16

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-18

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-19

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-20

FOR OFFICIAL USE ONLY

456

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

Appendix DD-22

FOR OFFICIAL USE ONLY

4/55

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

<<BLAST EFFECTS TABLES AND CHARTS>>

ANALYSIS DELETED

FOR OFFICIAL USE ONLY

APPENDIX EE

FORCE PROTECTION DESIGN CONSIDERATIONS

A. INTRODUCTION

1. The following is derived from DOD Security Engineering manuals to aid engineers and planners in identifying key parameters that may affect analyses of physical security aspects of terrorist threats and measures to mitigate threats. Use source materials for detailed investigation and preliminary design considerations involving systems security engineering for threat remediation.

2. The material in this appendix is for educational purposes. The intent is to illustrate how creative use of physical security equipment and environmental design techniques can enhance security of DOD personnel and resources. This appendix is not authoritative and should be used with discretion; however, the directives and technical manuals from which information is derived are authoritative in nature. Installation and facility physical environments have tremendous bearing on physical security designs. Tactics and operational techniques for employing terrorist weapons, as well as physical security equipment to defeat such efforts, also have significant bearing on detailed design, construction, and operation of installations and facilities.

3. Feedback is encouraged from commanders, and AT/FP, engineering, and security staffs to make this material more useful.

B. MINIMUM LEVELS OF FORCE PROTECTION CHECKLIST

1. Table EE-1 provides basic facility defensive measures for consideration. These measures offer capabilities at low cost through

application of effective layout or prudent use of elements not specifically required for protection. They also facilitate future upgrades and may deter acts of aggression.

C. MINIMUM THREAT PARAMETERS

1. The physical threat should be described in terms of tactics, tools, weapons, and explosives associated with attacks against DOD assets.

Table EE-1. Minimum Levels Checklist[1]

Site Work Elements:

[redacted]

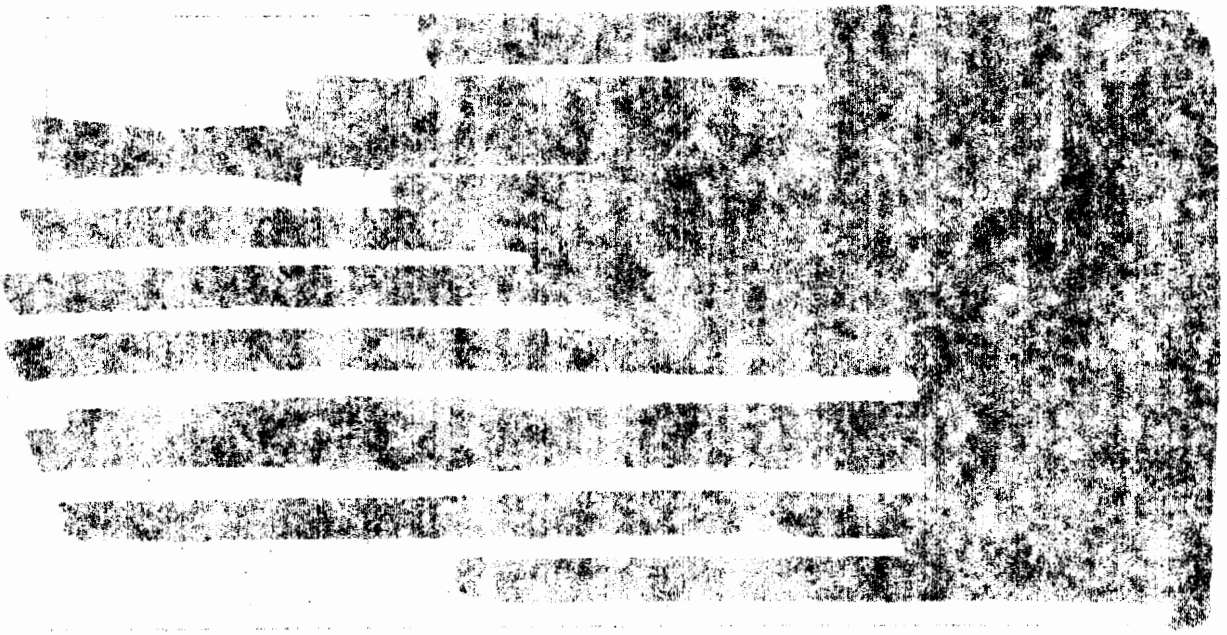
[1] Data Derived from Army TM 5-853-2, Vol. 2 (SECD), Table 2-1, p. 2-2

FOR OFFICIAL USE ONLY

Building Elements:

[redacted]

FOR OFFICIAL USE ONLY



<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-4

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-5

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-6

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-7

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-8

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-9

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-10

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-11

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-12

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-13

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-14

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-15

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-17

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-18

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-19

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-20

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-21

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-22

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-23

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-25

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-27

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-28

FOR OFFICIAL USE ONLY

519

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-29

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-30

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-31

FOR OFFICIAL USE ONLY

52R

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-32

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-33

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-34

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-35

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-37

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-38

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-39

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-41

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-42

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-43

FOR OFFICIAL USE ONLY

5 of

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-44

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-45

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-46

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-47

FOR OFFICIAL USE ONLY

<<FP DESIGN CONSIDERATIONS>>

ANALYSIS AND TECHNICAL DATA DELETED

Appendix EE-48

FOR OFFICIAL USE ONLY