FMFM 7-14

Combating Terrorism



U.S. Marine Corps

PCN 139 000575 00

MCCDC (C 42)
27 Nov 2002

E R R A T U M

to

MCRP 3-02D

COMBATING TERRORISM

1. For administrative purposes, FMFM 7-14 is reidentified as MCRP 3-02D.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-0001

5 October 1990

FOREWORD

1. PURPOSE

Fleet Marine Force Manual (FMFM) 7-14, *Combating Terrorism*, describes the United States and Marine Corps policy, concepts, procedures, terminology, and programs regarding terrorism.

2. SCOPE

FMFM 7-14 provides guidance for the installation/unit commander, his staff, and subordinate commanders to prevent, plan, prepare, and conduct combating terrorism operations. FMFM 7-14 addresses the fundamental principles on which the Marine Corps' combating terrorism program is built, its overall concept, and implementation procedures. The appendixes will assist staff officers and subordinate commanders in carrying out their commander's guidance. Many of the appendixes are presented in a manner that will make them easy to reproduce and distribute. FMFRP 7-14A, *Individual Guide to Understanding and Surviving Terrorism*, and FMFRP 7-37, *Vehicle Bomb Search*, are designed to be used in conjunction with this manual.

3. SUPERSESSION

FMFM 7-14 supercedes OH 7-14, *Terrorism Counteraction*, and OH 7-14.1, *Unit Terrorism Counteraction*.

4. CHANGES

Recommendations for improving this manual are invited from commands as well as directly from individuals. Forward suggestions using the User Suggestion Form format to—

Commanding General
Doctrine Division (C 42)
Marine Corps Combat Development Command
2042 Broadway Street Suite 210
Quantico, VA 22134-5021

5. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS



M. P. CAULFIELD
Major General, U.S. Marine Corps
Deputy Commander for Warfighting
Marine Corps Combat Development Command
Quantico, Virginia

DISTRIBUTION: 139 000575 00

User Suggestion Form

From:

To: Commanding General, Doctrine Division (C 42), Marine Corps Combat Development Command, 2042 Broadway Street Suite 210, Quantico, Virginia 22134-5021

Subj: RECOMMENDATIONS CONCERNING FMFM 7-14 *COMBATING TERRORISM*

1. In accordance with the foreword to FMFM 7-14, which invites individuals to submit suggestions concerning this FMFM directly to the above addressee, the following unclassified recommendation is forwarded:

____	_____	_____	_____
Page	Article/Paragraph No.	Line No.	Figure/Table No.

Nature of Change:

- ☐ Add
- ☐ Delete
- ☐ Change
- ☐ Correct

2. Proposed new verbatim text: (Verbatim, double-spaced; continue on additional pages as necessary.)

3. Justification/source: (Need not be double-spaced.)

Note: Only one recommendation per page.

(reverse blank)

Record of Changes

Change No.	Date of Change	Date of Entry	Organization	Signature

(reverse blank)

Combating Terrorism

Table of Contents

Chapter 1. Nature of the Threat

Paragraph		Page
1001	Terrorism Today	1-1
1002	Terrorist Profile	1-2
1003	Organizational Structure	1-2
1004	Terrorist Operations	1-3
1005	Terrorist Tactics and Training	1-4
1006	Terrorist Targets	1-4

Chapter 2. National Response

2001	United States Policy and Responsibility	2-1
2002	Tri-Level Concept	2-2
2003	Military Responsibility	2-4
2004	Marine Corps Role	2-5

Chapter 3. Intelligence and Threat Estimation

3001	Intelligence Support	3-1
3002	Essential Elements of Information	3-3
3003	Threat Estimates	3-3

Chapter 4. Security

Section I. Preventive Security Measures

4101	Tactical and Rear Area Security	4-1
4102	Operations Security	4-1
4103	Physical Security	4-3
4104	Personnel Security	4-3

Section II. Protective Security Measures

4201	Protecting Security Operations	4-6
4202	Searches	4-13
4203	Tactical Responses	4-17

Chapter 5. Crisis Management Planning

Paragraph		Page
5001	Incident Response Phases	5-1
5002	Crisis Management Team	5-3
5003	Crisis Management Force	5-4
5004	Interior Guard	5-8
5005	Crisis Management Plan	5-8
5006	Communication Requirements	5-10
5007	Public Affairs	5-10

Chapter 6. Crisis Management Employment

6001	Initial Response	6-1
6002	Confirmation	6-1
6003	Use of Force Options	6-2
6004	Preparation	6-2
6005	Response	6-3
6006	Typical Response to a Terrorist Incident	6-3
6007	Identify Inconsistencies	6-5
6008	Establish Communications	6-5
6009	Obtain Evidence	6-5
6010	Disposition of Apprehended Personnel	6-5
6011	After-Action Report	6-6

Appendixes

A	United States Policy and Legal Considerations	A-1
B	Memorandum of Understanding Between the Department of Defense, the Department of Justice, and the Federal Bureau of Investigation	B-1
C	Physical Security Plan Format	C-1
D	THREATCON System	D-1
E	Installation Vulnerability Assessment	E-1
F	Individual Security Precautions in High-Risk Areas	F-1
G	Senior Officer's Security Measures	G-1
H	Office Procedures	H-1
I	Lock Security	I-1
J	Soft Target Procedures	J-1
K	Postal Bombs	K-1
L	Telephone Call Procedures	L-1
M	Procedures for Drivers	M-1
N	Assassination Threat Procedures	N-1
O	Explosive Device Procedures	O-1
P	Crisis Management Plan Format	P-1

		Page
Q	Crisis Management Plan Checklist	Q-1
R	Public Affairs Checklist	R-1
S	Glossary	S-1
T	References and Related Technical Publications	T-1
Index		Index-1

Chapter 1

Nature of the Threat

Terrorism is "the unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives." (Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*) Terrorism is a criminal act that is symbolic in nature. Its intent is to influence an audience beyond that of the victim.

The use of terror to accomplish a goal is not new. Violent acts, or threats of violence, have been used throughout history to intimidate individuals and governments into meeting terrorist's demands. Terrorism is cheap, low-risk, highly effective, and allows the weak to challenge the strong. Individuals or groups use terrorism to gain objectives beyond their inherent ability.

Terrorism affords a weak nation an inexpensive form of warfare while stronger nations use terrorism to effect covert acts. Stronger nations use surrogates to employ terror while reducing their risk of retaliation and protecting their reputation. A nation is insulated from retaliation as long as its relationship with the terrorist remains unproven.

Terrorism is employed throughout the spectrum of conflict to support political or military goals. Terrorists are an integral element in an insurgency and also play a major role in conventional warfare. Terrorists can disrupt economic functions, demonstrate a government's incompetence, eliminate opposition leaders, and elevate social anxiety.

Terrorism's goal is to project uncertainty and instability in economic, social, and political arenas. Short-term terrorist goals focus on gaining recognition, reducing government credibility, obtaining funds and equipment, disrupting communications, demonstrating power, delaying the political process, reducing the government's economy, influencing elections, freeing prisoners, demoralizing and discrediting the security force, intimidating a particular group, and causing a government to overreact. Long-term goals are to topple governments, influence top level decisions, or gain legitimate recognition for their cause.

However, terrorists are not invincible. Every failure hurts their cause. The keys to defeating terrorists are awareness, education, and intelligence in order to deny, deter, delay, and detect terrorist acts. Rapid coordination between military units, military services, local police, and host nations is essential in denying the terrorist targets and refuge.

1001. Terrorism Today

Terrorism is a fact of contemporary life. Although terrorism is not new, it is a new challenge to our society and way of life. The economic and political power of sovereign nations are becoming increasingly concentrated in large cities. This concentration enables terrorists to influence large groups of people in relatively small areas. Modern technology provides the terrorist with free publicity, lucrative targets, ease of transportation, and advanced weaponry. Terrorists rely on media coverage to broadcast terrorist events.

International transportation affords the terrorist easy travel. Technical advances and industrialization present the terrorist with lucrative targets (e.g., power plants, factories). Modern weapons (e.g., nuclear devices, missiles) offer terrorists the tools for destruction.

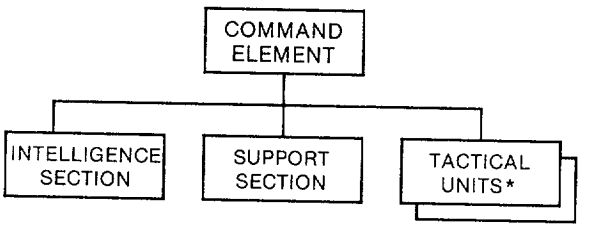
1002. Terrorist Profile

The terrorist, urban guerrilla, saboteur, revolutionary, and insurgent are often the same depending upon the circumstance or political view. Although difficult to generalize a terrorists' character and motivation, a profile has been developed. Typically, terrorists are intelligent, well-educated, obsessed with initiating a change in the status quo, reared in middle class or affluent families, and 22 to 25 years of age. The ability to develop a terrorist profile provides a clearer image of the enemy and dispels dangerous misconceptions.

Terrorists are dedicated to their cause—even to the point of death. Terrorists are motivated by religion, prestige, power, political change, or material gain. Terrorists believe they are an elite society, and act in the name of the people. Their dedication is evident in their education and training, arms and equipment, planning methods, and ruthless execution. Their dedication makes them a formidable enemy.

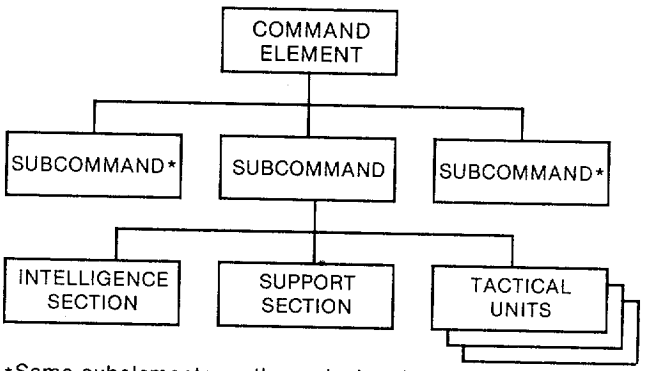
1003. Organizational Structure

Security, more than any other factor, drives the organizational structure of terrorist groups. Secrecy is essential to success and maintained only through good organization, leadership, and support. Organization is characterized by small, covert cells with little interaction and tight, central control held by a few individuals. Typically, small terrorist groups are organized into the functional cells shown in figure 1-1. Larger terrorist groups contain more than proof100 people but less than 500. Larger groups are organized into subgroups with built-in functional cells. Figure 1-2 depicts the typical structure of a large terrorist group. If popular support exists, large terrorist groups operate freely with far less concern for security.



*Each unit may have 2 or 3 cells of 2 to 6 persons each.

Figure 1-1. Small Terrorist Group.



*Same subelements as those depicted.

Figure 1-2. Large Terrorist Group.

Diverse terrorist groups, small or large, operate under a veil of camaraderie. Terrorist groups share resources, expertise, and safe havens. Different terrorist groups frequently participate in joint operations. Intergroup cooperation is encouraged and supported by sympathetic foreign governments. Terrorist members are classified as hardcore leaders, active cadre, active supporter, and passive supporter.

a. Hardcore Leaders. Except for some anarchist groups, some form of leadership governs all terrorist groups. Leaders establish policy, develop plans, and give direction. In covert, cellular terrorist organizations, deterring attacks against the central leadership is priority. Terrorist leaders are the groups major vulnerability.

b. Active Cadre. The active cadre carry out orders from higher commands. The active cadre

are an elite, close-knit group. Their identity and ability are well-guarded secrets. Typically, the active cadre in one terrorist cell will have only one point of contact within another terrorist cell. Due to its selective nature, the active cadre's secrecy is relatively easy to ensure.

Typically, the active cadre organizes into small cells containing two to six terrorists. Each cell specializes in a particular tactic or contains experts in various fields. The active cadre also contain the trainers. Typically, terrorists within a cell are trained bombers, arsonists, or assassins.

c. Active Supporters. Active supporters provide the logistic support needed to sustain terrorist operations. They provide safe houses, weapons, ammunition, vehicles, medical support, food, and money. Active supporters are a valuable source of intelligence information. Their day-to-day activities and low profile enable them to perform various intelligence-gathering activities not possible by members of the active cadre. Active supporters often come from the professional classes, such as lawyers, doctors, and businessmen. Active supporters provide a source of replacement for the active cadre.

d. Passive Supporters. Passive supporters are the most difficult to define and recognize. They are sympathetic to the cause but fear reprisal if exposed or identified. Passive supporters may be ignorant to the cause's intent and the use of their support. They may unwittingly provide money through anonymous giving. Passive support is extremely important to the politically-motivated terrorist who relies on popular support to survive.

1004. Terrorist Operations

a. Explosives. Explosives contributed to 67 percent of all terrorist incidents in the last decade. Explosive devices are cheap, reliable, and easy to make, and materials are readily available. If terrorists mix real bombs and hoaxes, they can effectively hamper security forces and keep the public in a panic. Terrorists use explosives in pairs in case one fails. Explosives are hidden and delivered in a variety of ways. Modern explosive devices are smaller, contain greater destructive capability, and are harder to detect.

b. Arson. Incendiary devices are cheap and easy to hide. Arson is a useful tactic against public utilities, hotels, houses of government, and industrial centers. Terrorists use arson to draw a crowd, which in turn provides terrorists with the opportunity to use explosives or other weapons.

c. Vehicle Theft. Stolen vehicles provide terrorists with a means of delivering explosives that will be traced back to the original car owner and not to the terrorist organization.

d. Skyjacking and Aircraft Theft. Skyjacking provides terrorists with hostages and draws media attention. Aircraft theft provides terrorists with a tool for a kamikaze attack. Aircraft mobility and distance makes retaliation difficult.

e. Marjacking. Marjacking (also called maritime theft) provides terrorists with a unique method of intimidating international travelers. Due to a ship's size and ability to endure long periods of isolation, marjacking presents a variety of benefits to terrorists and risks to legal authorities. While occurrences of marjacking are infrequent, the possibility should not be underestimated.

f. Ambush. A well-planned ambush provides terrorists with the opportunity to kidnap or assassinate intended victims. An ambush allows terrorists to choose the time and place of attack. An ambush is easily planned if the victim uses the same daily routine.

g. Kidnapping. Kidnapping is a preferred terrorist tactic. Kidnapping prominent personnel can force a government into acceding to terrorist demands in order to safeguard prisoner release.

Kidnapping for ransom also helps finance terrorist activity. Kidnapping requires a safe house in which to keep the victim while bargaining.

h. Hostage-Taking. Hostage-taking is overt and designed to attract and hold media attention. Threats to a hostage's life can be used to exact concessions from a government. The terrorists' bargaining chip is the life of the hostage. The terrorists' intended target is the audience affected by the hostage's confinement, not the hostage.

i. International Narcotics Support. Drug activities finance some terrorist groups. Terrorist groups may provide security for narcotics networks in return for financial support of their operations.

j. Robbery and Extortion. In some environments; e.g., South America, robbery and extortion enhance other terrorist activities. These methods are unnecessary when terrorists receive funding and support from sympathetic nations.

k. Psychological Terror. Psychological terror alters behavioral characteristics of an individual, group, or organization through the application of sophisticated techniques.

l. Nuclear, Biological, and Chemical Attack. There has been no precedence for nuclear, biological, and chemical (NBC) activity in the past, but the threatened use of NBC materials by terrorists cannot be dismissed. Always consider the potential use of NBC warfare when combating terrorism.

m. Assassination. Historically, terrorists have killed specific individuals for psychological effect. Expect continued use of this tactic due to its impact.

1005. Terrorist Tactics and Training

Terrorist operations are meticulously planned. Prior to execution, detailed reconnaissance missions, training periods, and rehearsals ensure precise execution and minimum failure. Only select members of the terrorists' command element have knowledge of the entire operation. Separate cells perform planning, reconnaissance, support, and execution missions to prevent compromise. Contingency plans cover unforeseen events and alternate targets. Carefully staged movement of personnel and equipment avoids detection. Withdrawal is planned in detail.

Terrorists train in subversion, weaponry, infiltration, negotiation, and any other required skills. Specialized training takes place in countries known for their sympathetic terrorist affiliations.

1006. Terrorist Targets

Terrorists attack targets which are vulnerable, have a high psychological impact on a society, produce significant publicity, and demonstrate the government's inability to provide security. Both critical facilities and prominent individuals are potential terrorist targets. Of these, individuals are the preferred target. Corporate executives are prime targets because they are symbols of economic imperialism and are often covered by *kidnap insurance*. Military personnel and facilities have become increasingly appealing targets. Military facilities are a symbol of national power; a source of arms, ammunition, and explosives (AA&E); and a prestigious target that adds to the terrorist's reputation. It is a dangerous mistake to think that only high-ranking military personnel or those in key positions are terrorist target.

Chapter 2

National Response

By virtue of our presence throughout the world, United States military forces are convenient terrorist targets. Marines and their families must remember they can become terrorist victims anywhere in the world. They can inadvertently become involved in terrorist acts directed against others. To demonstrate the potential danger, review the following statistics. The U.S. Department of State (DOS), Threat Analysis Division reported 162 lethal attacks during the 1973 to 1986 timeframe. Four hundred and forty Americans died in these attacks. Nine of these attacks were specifically directed against United States military facilities resulting in the death of 269 military personnel.

The United States considers the practice of terrorism against a United States citizen or facility a threat to national security. The United States aggressively counters hostile acts directed against its citizens, property, or national interests. The United States uses federal, military, and civilian resources in conjunction with ally support to combat terrorism. The United States overall concept based on antiterrorism and combating terrorism tactics is to deter and eliminate terrorism.

Antiterrorism tactics use defensive measures to reduce the vulnerability to injury, damage, or loss of personnel, dependents, and property. These tactics include limited response and containment by local military forces. Counterterrorism tactics use offensive measures to prevent, deter, and respond to terrorist acts. However, there is no distinct separation between the two tactics, and discussions in one area may apply to the other.

2001. United States Policy and Responsibility

Military personnel should be aware of the United States' policy for combating terrorism. Military personnel must be aware of legal considerations affecting planning and execution. Appendix A provides United States legal considerations and policies when combating terrorism.

Terrorist incidents must be properly identified to determine appropriate national response and authority. If individuals are identified as terrorists (either by themselves, law enforcement, or intelligence forces), treat the incident as a terrorist operation. Once identified as a terrorist action, immediately notify the appropriate authorities.

Elements responding to a terrorist incident quickly assess the situation, evaluate authority and jurisdiction, and begin appropriate actions. The United States has tasked various agencies with the responsibility to combat terrorism. These agencies interact as required. These agencies network to provide information throughout the chain of command. Table 2-1 identifies agency responsibility.

a. Department of Justice. The Department of Justice (DOJ) is the lead agency for combating domestic terrorism. DOJ manages terrorist acts within the United States and its possessions. Within the DOJ, the Federal Bureau of Investigation (FBI) is the lead agency for handling and investigating domestic terrorist acts committed in the United States. Jurisdictional authority rests with the FBI, but the National Command Authorities (NCA) may become the focal point of a major incident that threatens national objectives and internal security.

Table 2-1. Terrorist Incident Jurisdictional Authority

Location	Initial Response	Primary Authority/ Jurisdiction	Primary Enforcement Responsibility	Exercise Control of Military Assets	Primary Investigative Responsibility
CONUS					
On Base	Military Police	FBI/Installation Commander	FBI/Installation Commander	Installation/Unit Commander (FBI support)	FBI/NISCOM/PMO
Off Base	Local Civilian Authority	FBI/Local Civilian Authority	FBI/Local Civilian Authority	FBI to Attorney General to Secretary of Defense	FBI/Local Civilian Authority
OCONUS					
On Base	Military Police	Host Nation/ Installation	Host Nation/ Installation	Installation/Unit Commander (IAW applicable status-of-forces agreement or other bilateral agreement governing the employment of military forces)	Host Nation/ NISCOM/PRO
Off Base	Host Nation	Host Nation	Host Nation	Installation/Unit Commander/Host Nation (IAW applicable status-of-forces agreement or other bilateral agreement governing the employment of military forces)	Host Nation

NOTE: Coordinate with the local staff judge advocate to clarify authority and questions of jurisdiction. Coordinate with DOS officials as required. Coordinate with local law enforcement agencies to ensure support procedures are in place and information/communication channels are functioning.

The FBI shares jurisdictional responsibility with the Federal Aviation Administration (FAA) during air operations. Under Title 49 U.S. Code, Section 1357(e), the FAA assumes law enforcement responsibility once an aircraft is in-flight. In-flight begins the moment all external aircraft doors are closed and embarkation is complete. In-flight continues until aircraft doors are opened for disembarkation. The FBI resumes responsibility once aircraft doors are opened.

b. Department of State. The DOS is the lead agency for combating terrorism against American personnel and facilities outside the Continental United States (OCONUS). The DOS is also responsible for the foreign relations aspects of domestic terrorism. Under international law and status-of-forces agreements, host nations are responsible for safety of diplomatic personnel. The Department of Defense (DOD) coordinates activity between the United States and host nation.

c. Department of Defense. Federal law, interagency agreements, status-of-forces agreements, international agreements, and memorandums of understanding (MOU) determine the DOD's combating terrorism role. Military policies, directives, and plans support the DOJ and DOS under applicable federal laws or memorandas of agreement. The DOD retains the command and control of military forces involved in combating terrorist operations.

If terrorists attack a DOD target, the National Military Command Center (NMCC) becomes the command post for the Joint Chiefs of Staff (JCS) and the Secretary of Defense. Each military service patterns its internal command center after the NMCC. Each military service communicates with the NMCC. The Marine Corps Command Center (MCCC) is the Commandant's command post. The MCCC communicates with appointed commands throughout the Marine Corps and other services.

2002. Tri-Level Concept

The United States uses a tri-level concept to combat terrorism. Figure 2-1 depicts the tri-level concept.

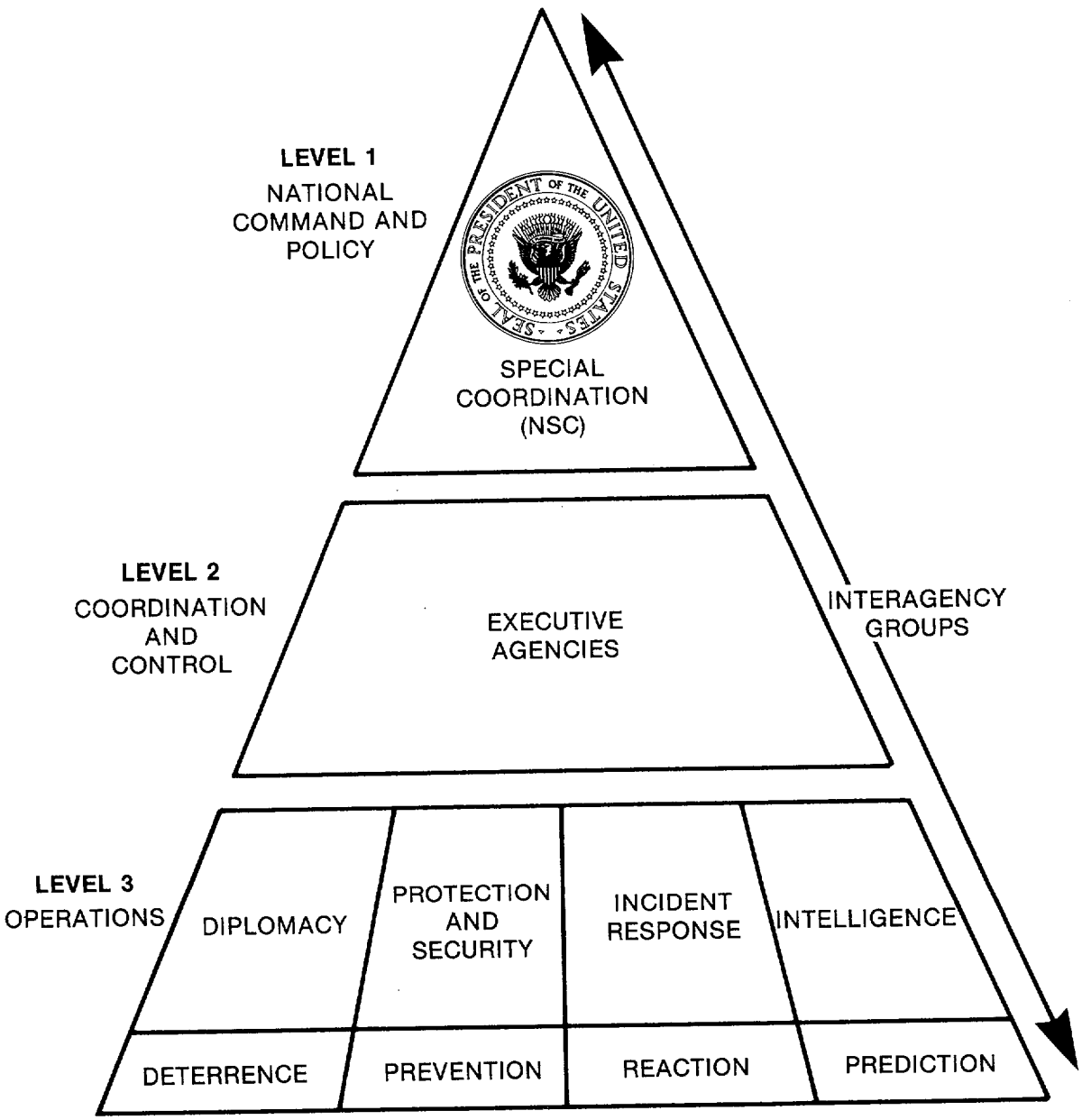


Figure 2-1. United States Antiterrorism Program.

The first level develops national command and policy procedures. This is the responsibility of the National Security Council under the direction of the President. The second level establishes coordination and control. This is the responsibility of eight federal agencies, including DOD. The third level contains operational procedures used to deter, prevent, react, and predict terrorist activity. This is the responsibility of 29 federal agencies. These federal agencies comprise the terrorist working group.

2003. Military Responsibility

The MOU between the DOD, DOJ, and FBI (see app. B) outlines responsibilities during terrorist incidents in the Continental United States (CONUS). The installation commander provides the initial response to a terrorist incident occurring on a military installation. The installation commander immediately notifies the FBI. The FBI assumes jurisdiction if the incident is of significant federal interest. OCONUS, status-of-forces agreements and MOUs dictate that host nations have primary responsibility for managing terrorist incidents. However, our definition of terrorism may differ from those of other nations. Prior mutual agreement is necessary to prevent misunderstandings. The installation commander has the authority to maintain order and security of overseas installations. Because of the complexity of terrorist incidents, commanders should obtain legal guidance from the staff judge advocate.

a. CONUS On-Base Incidents. The installation commander maintains law and order on the installation. The U.S. Supreme Court recognizes the installation commander's authority. Military police derive their authority from the commander's authority. Military police are the commander's agents. If a terrorist incident occurs on a military installation, the installation commander uses the command's law enforcement assets (military police) and support elements (investigative services) to re-establish control.

The installation commander's initial priority is to defend against further incidents, contain the problem at hand, and restore order. Once a terrorist incident is identified, the installation commander notifies the FBI. The FBI determines if it needs to exercise jurisdictional control. If the FBI declines jurisdiction, the installation commander resolves the incident. Regardless of who obtains jurisdictional control, military personnel remain under direct control of the military commander.

b. CONUS Off-Base Incidents. Terrorist incidents in the civilian community are treated as civil, criminal activity. The use of military troops off-base requires specific approval by the President (Title 10 U.S. Code, Sections 331-334). Using military troops to combat terrorism is a statutory exception to the Posse Comitatus Act. Certain statutes (e.g., Title 18 U.S. Code, Section 112) permit the use of military forces to assist the Attorney General. The DOD requires Presidential approval before using military forces to respond to terrorist incidents off-base. The following govern the use of Marine Corps resources to combat off-base terrorism:

- DOD Dir 5525.5, DOD Cooperation with Civilian Law Enforcement Officials (FMFP).
- SECNAVINST 5820.7AB, Cooperation with Civilian Law Enforcement Officials; Posse Comitatus Act.
- Memorandum of Understanding between the Department of Defense, the Department of Justice, and the Federal Bureau of Investigation, dated 5 Aug 1983 (see app. B).

c. OCONUS On-Base Incidents. The installation commander is responsible for incidents occurring on installations OCONUS. The installation commander contacts the DOS, not the FBI, and host nation officials. The DOS and U.S. Embassy coordinate United States and host nation responses. The installation's response is subject to limitations, guidelines, and procedures established in agreements made with host nations. Installation commanders have the authority to establish internal force structures to protect the installation. The commander assembles internal forces from military personnel currently in the country. Augmentation of additional forces from outside the host nation requires host nation consent.

d. OCONUS Off-Base Incidents. Host nations are responsible for off-base incidents. American military assistance depends on status-of-forces agreements and MOUs. The DOS and the U.S. Embassy coordinate military assistance. The commander does not provide military forces and equipment without specific DOS approval.

2004. Marine Corps Role

Marine Corps policy works within the confines of United States policy. Marine Corps policy is to protect, to the best of its ability and authority, Marine Corps personnel, their dependents, facilities, and equipment from terrorist acts. Reducing the risk of terrorist attacks to Marine Corps personnel is a command responsibility. Each Marine exercises proper caution and prudent judgment to reduce individual vulnerability. Give particular attention to protecting high-risk targets; e.g., key personnel, training and advisory teams in foreign countries, special weapons, facilities, logistics storage areas.

The Marine Corps Combat Readiness Evaluation System (MCCRES) Mission Performance Standards provide operational standards to measure installation/unit readiness. The MCCRES Mission Performance Standards provide training objectives. These programs prepare and evaluate a unit's ability to combat terrorism.

a. Marine Corps Structure. The Commandant of the Marine Corps (CMC) has overall command responsibility to combat terrorist aggression against the Marine Corps. The Deputy Chief of Staff for Plans, Policies, and Operations, Headquarters, U.S. Marine Corps (HQMC) has overall staff cognizance to combat terrorism. The Commanding General, Marine Corps Combat Development Command (MCCDC) establishes doctrine, training, and educational requirements to combat terrorism. The Director of Intelligence, HQMC coordinates with national level intelligence agencies to monitor terrorist threat situations. The MCCC disseminates information to and receives reports from commanders during a crisis. Each installation commander is responsible for combating terrorism on the installation. Typically, staff responsibility rests with the operations officer. The provost marshal assists the operations officer.

b. Command Antiterrorism Program. Marine Corps policy stresses deterrence of terrorist incidents through preventive measures. Figure 2-2 illustrates the Marine Corps' antiterrorism program. The Marine Corps antiterrorist program addresses—

- Threat estimation.
- Installation/unit criticality and vulnerability assessments.
- Operations security.
- Personnel security.
- Physical security.
- Crisis management planning.
- Employment of tactical measures to contain and counter terrorist incidents.

If a terrorist incident occurs, apply military resources to gain control of the situation. Installation and tenant/operational commanders develop operational programs. These programs offer in-depth defense against terrorist attack and address—

- Terrorism threat and security briefings for all personnel and their dependents before overseas travel or duty.
- Terrorism awareness training for all Marines. (Training begins at the time of initial entry and continues throughout a Marines' career.)
- Annual tests and evaluations to determine a unit's ability to combat terrorism.
- Organization of both a crisis management team (CMT) and crisis management force (CMF).
- Annual review of the CMT and CMF through operational exercises. Conduct these exercises in conjunction with tenant commands and supporting activities.
- Mission-critical assets and their vulnerability to terrorists.
- Annual update and review of threat assessments.
- Annual update and review of installation/unit assessments.
- Infrastructures (e.g., telephone exchange, electrical transformer sites, water tanks, fuel tanks) and key assets critical to the operation of the installation.
- Redundancy of key assets and infrastructure.

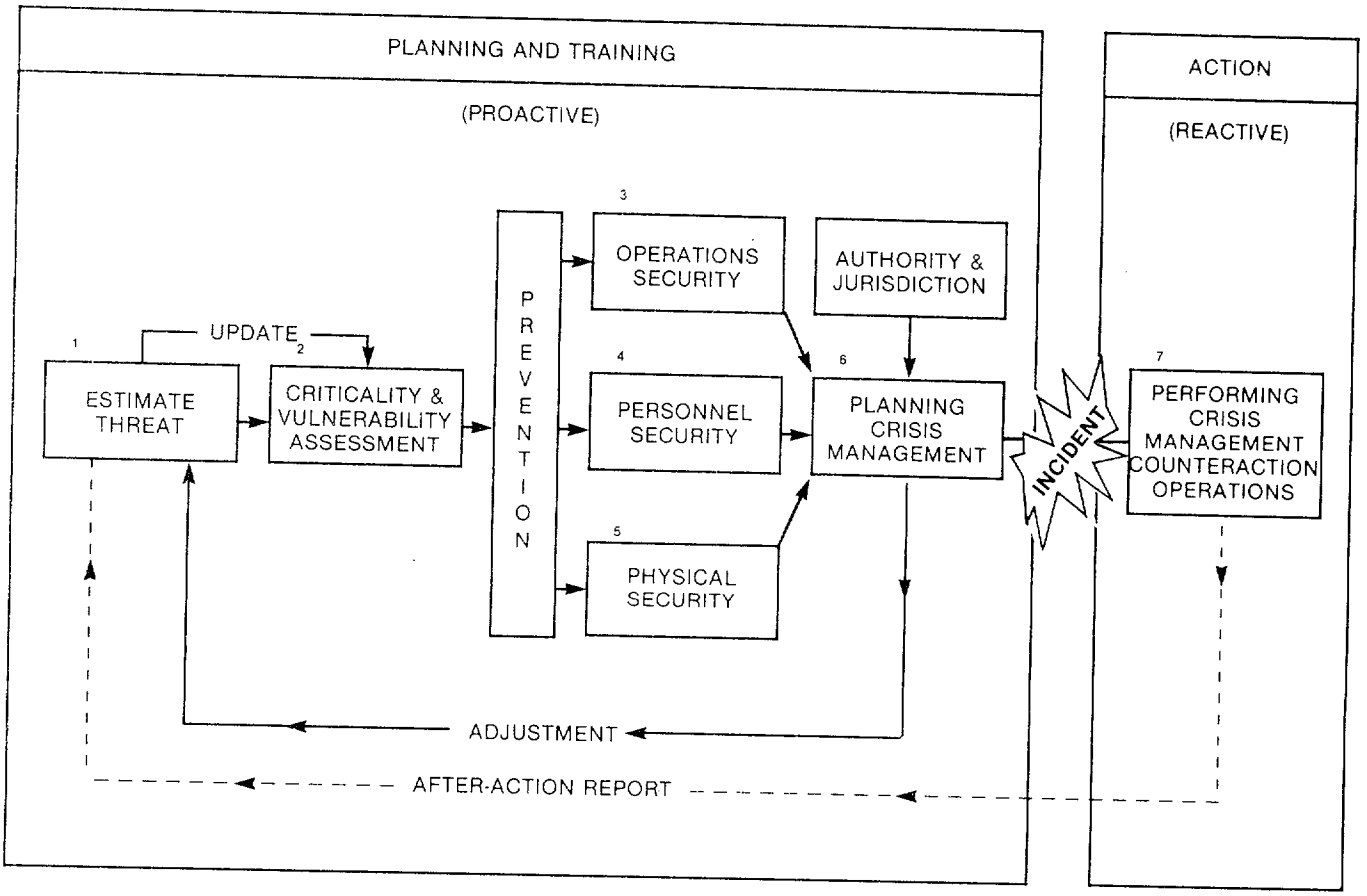
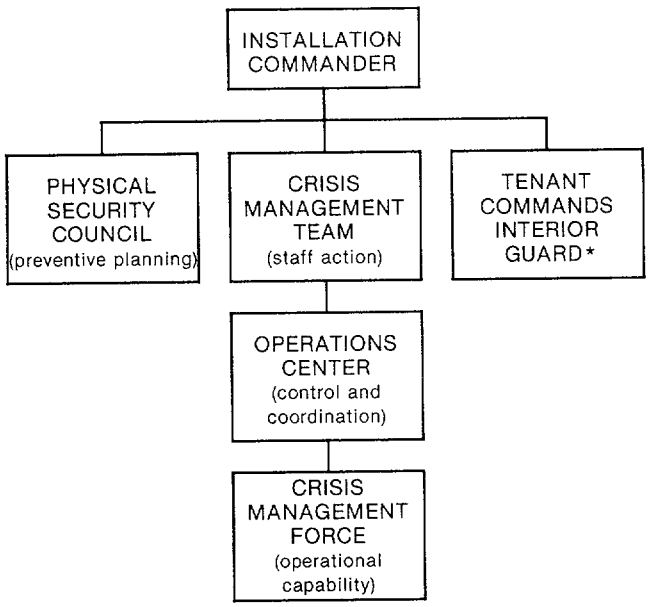


Figure 2-2. Marine Corps Antiterrorism Program.

- Disaster preparedness plans for damage control and recovery procedures for infrastructures and key assets.
- Combination of different key assets and infrastructures into security enclaves.

c. Installation Commanders. Commanders directly responsible to the CMC for operating bases, stations, facilities, and centers are termed installation commanders. Installation commanders are responsible for the overall security and protection of the installation. This responsibility includes personnel, equipment and material, facilities, and tenants. Installation commanders establish programs to combat terrorism aboard their installations. Commanders ensure proper physical security is provided. Installation commanders develop orders and standing operating procedures (SOPs) tailored to local conditions and assigned missions. They exercise operational control over host units providing additional support. Installation commanders organize their installations in accordance with Marine Corps security procedures. (See fig. 2-3.)

(1) Physical Security Council. Installation commanders with tenant command representation form physical security councils. Physical security councils develop and coordinate combating terrorist programs. Installation commanders establish a threat committee to maintain and access current threat assessments. The threat committee reports to the physical



* Responsibility for critical assets located within or adjacent to the areas under control of a tenant command's interior guards should be assigned to the commander of those interior guards.

Figure 2-3. Command Security Organization.

security council. Installation commanders ensure that the physical security council conducts threat assessments at least annually.

(2) CMT. Installations establish a CMT to coordinate the command's combating terrorism efforts. The CMT coordinates the installation's response and recovery for a variety of incidents, including terrorism. The CMT identifies infrastructures and key assets critical to the installation's operation.

Regardless of the type of incident, members of the CMT respond and resolve various situations—from contingency planning to evaluation exercises to actual incident resolution and recovery. The type of incident and duration determines the degree of involvement. Predesignated members of the general or executive staff perform CMT duties collaterally during a crisis. Members are under the control of the chief of staff or executive officer. Members and alternates of staff agencies and primary and alternate representatives from tenant commanders serve on the CMT.

(a) Operations Center. A predesignated operations center must be readily available. The CMT establishes desk-top procedures and adequate communications facilities in the operations center. The CMT develops procedures to assist in performance of duties. The CMT distributes information to all CMT members. The CMT reviews and updates SOPs annually. The CMT validates SOPs during the installation's annual operational terrorism evaluation exercise. A security force command center can be used as a tactical command post, alternate operations center, or forward command post.

(b) CMF. The installation commander organizes assets into a CMF to provide overall security and internal reactive capabilities. If necessary, the tenant command's interior guard activities are coordinated through the tenant command's CMT representative. Once military police assume responsibility at an incident site, interior guard personnel are employed only with the expressed permission of the on-scene commander. Figure 2-4 illustrates CMF organization.

(3) Tenant/Operational Commanders. Commanders who occupy, use, or share installations but do not have responsibility for their overall operation and security are termed tenant commanders. Tenant commanders are guided by the physical security and terrorist counteraction plans and policies of the installation commander. The tenant Marine commander is responsible for physical security and terrorism planning if these items are not provided by the installation commander.

For purposes of this discussion, operational commanders are commanders of the Fleet Marine Force (FMF) and 4th Division/Wing Team units. Operational commanders acting as tenant commanders support installation

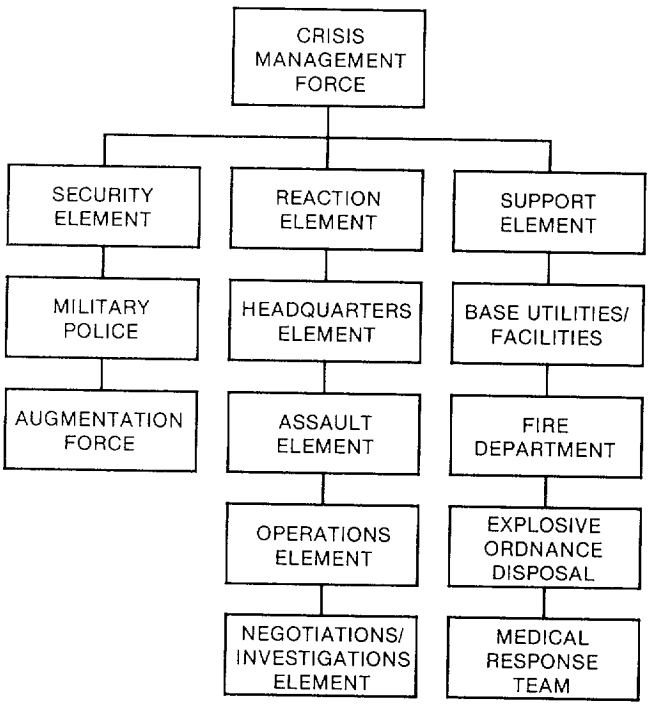


Figure 2-4. Crisis Management Force.

commanders. While deployed or not in a tenant status, operational commanders organize and provide their command's security. Unlike installation commanders, operational commanders have existing organizations; e.g., tactical units and operations centers, which execute the combating terrorism functions of the CMF and CMF.

d. Education and Training. Individual terrorist training and awareness are critical to the Marine Corps' combating terrorism effort. The Commanding General, MCCDC is responsible for the development and maintenance of education and training programs which address terrorism. The Deputy Commander for Training and Education, MCCDC coordinates and establishes education and training policies and standards for individual and collective training programs which address terrorism.

At the formal school and installation/unit level, terrorist education and training programs heighten awareness of the threat and provide physical and personnel security training. Marine Corps terrorist programs consist of—

- Threat awareness instruction. At a minimum, training covers threat assessment, terrorist tactics, residential security, vehicle security, travel security, and bomb defense.
- Combating terrorism and low-intensity conflict instruction.
- Terrorism correspondence courses.
- Mobile training teams from a variety of external sources.
- Specialized terrorism education and training.

Terrorist instruction addresses proactive avoidance techniques and self-defense measures for personnel assigned to high-risk areas. Terrorism awareness programs support the educational process. Table 2-2 provides a list of courses and their locations. Non-DOD contractors offer specialized training courses in security and terrorism. Information on additional non-DOD courses of instruction is available from CMC (POS-40).

Table 2-2. Available Terrorism Courses

Subject	Institute
Combating terrorism	MCCDC, Education Center Quantico, VA
Low-intensity conflict	MCCDC, Education Center Quantico, VA
Terrorism correspondence courses	Marine Corps Institute Quantico, VA
Terrorism curriculum subject to change—contact school for current listing	USAF, Special Operations School Hurlburt Field, Florida
Terrorism curriculum subject to change—contact school for current listing	USA, Military Police School Fort McClellan, Alabama
Terrorism curriculum subject to change—contact school for current listing	USA, John F. Kennedy Special Warfighting Center & School Fort Bragg, North Carolina

Chapter 3

Intelligence and Threat Estimation

Terrorism knows no rules or boundaries—only objectives. Combating terrorism requires knowledge of terrorist goals, intentions, and capabilities and an active intelligence program. Intelligence programs exploit military, civilian, and foreign information sources. Effective intelligence support requires intelligence production (collection and processing of intelligence information), intelligence dissemination (distribution of intelligence information), counterintelligence (deterring, disrupting, or defeating terrorist intelligence activities), and threat estimation. Of these, threat estimation is the key. Threat estimation unites the intelligence effort into logical analyses and possible conclusions from which the intelligence officer advises security and counteraction efforts.

3001. Intelligence Support

Countering the terrorist threat is a command function. The intelligence officer is the commander's primary advisor. Intelligence personnel and complex intelligence networks support the intelligence officer.

a. Organizational Sources

(1) U.S. Embassy. The U.S. Embassy (or a friendly nation's embassy) provides overseas installations and deployed units with information pertinent to the current terrorist situation.

(2) Host Nation Support. The host nation's civil or military authority may provide overseas installations and deployed units with information regarding the current terrorist situation.

(3) Fleet or Joint Force Intelligence. Units deployed as part of a naval or joint task force receive United States military intelligence through normal channels.

(4) Naval Investigative Service Command. Navy and Marine Corps personnel form the Naval Investigative Service Command (NISCOM) The NISCOM monitors worldwide terrorist incidents. The NISCOM responds to counterintelligence command requirements. The NISCOM provides counterintelligence/antiterrorism information to all Marine Corps commands, except combat-related counterintelligence matters within the functional responsibility of the Marine Corps.

The Navy's Antiterrorist Alert Center (ATAC) was established within NISCOM to process real-time information. The ATAC operates on a 24-hour basis. ATAC threat assessments provide commanders with enough information to make prudent security decisions. ATAC threat assessments are not stand-alone documents. The ATAC provides the documents listed in table 3-1. Submit requests for ATAC documents through the command's local Naval Investigative Service Resident Agency (NISRA). The local NISRA also provides current, local antiterrorism information.

(5) Marine Corps Counterintelligence Teams/Representatives. The Marine Corps' terrorist counterintelligence mission provides commanders with terrorist threat information. To accomplish

Table 3-1. ATAC Documents

Document	Purpose
ATAC Summary (ATACSUM)	Distributed to all Marine Corps installations and major commands. Released 6 days a week (Sunday-Friday). Provides current operational intelligence relevant to terrorist threat. Identifies relevant unconventional warfare tactics and threats.
ATAC Spot Report	Distributed to affected commands only. Identifies indications and warnings of imminent terrorist activity. Identifies activities, conditions, or events which could lead to potential terrorist incidents directed against DON assets and personnel.
ATAC Supplement	Supplements ATACSUMs or ATAC Spot Reports. Provides in-depth analysis of terrorist groups, threats, and attacks.
ATAC Warning Report	Distributed to affected commands only. Provides threat information. Identifies terrorist group activities. Establishes threat levels for specific geographic areas.
ATAC Threat Assessments	Distributed upon requests received from Marine Corps installation/units, major Marine Corps commands in tenant status, Marine Corps units deployed OCONUS, and Marine Corps units not in a tenant status. Provides current operational intelligence relevant to terrorist threat. Identifies relevant unconventional warfare tactics and threats. Establishes threat levels for specific geographic areas.
ATAC Threat Briefings	Conducted upon requests received from commands preparing to deploy OCONUS. Conducted by ATAC representative. Provides unit personnel with overview of terrorist threat and specifics regarding area of deployment.

this mission, the Marine Corps has counterintelligence teams within the FMF. The teams inform commanders of the terrorist threat. The teams provide information, evaluations, and assistance to develop methods of deterring or neutralizing terrorist acts. They recommend measures to protect personnel, installations, and units. Marine Corps counterintelligence representatives are assigned to major Marine Corps installations.

(6) HQMC, Intelligence Division, Counterintelligence Branch. HQMC, Intelligence Division, Counterintelligence Branch has primary staff responsibility for handling terrorist threat information. This includes interfacing with national-level intelligence and security organizations, providing periodic terrorist information reports, maintaining terrorist organization/activity files, and representing the Marine Corps at national intelligence committees addressing terrorism.

(7) Higher/Subordinate/Adjacent Headquarters. Whether in garrison or deployed, a commander expects intelligence support from other headquarters. A doctrinal responsibility is the timely provision of information/intelligence to subordinate, adjacent, and higher commanders.

b. Information Sources

(1) Open Sources of Information. Open sources of information are extremely valuable, yet the most overlooked source of information. There are commercial publications addressing terrorism and criminal activities. These publications may be in the command library or they may be ordered. Terrorism schools and seminars provide comprehensive information. Local newspapers and television stations present terrorism information. The Central Intelligence Agency, Defense Intelligence Agency, FBI, DOS, Department of Energy, Department of the Treasury, and National Criminal Justice Reference Service publish terrorism data. Other potential sources include command deployment after-action reports and the overseas theater commanders.

(2) Criminal Information. The criminal information system is a primary source of data for domestic terrorism. The command's provost marshal, local law enforcement agencies, and Naval Investigative Service (NIS) agents provide this information.

(3) Intelligence. DOD directives govern Marine Corps intelligence activities. The intelligence community's ability to disseminate intelligence information is strictly regulated. Although restrictions apply, data is available through Navy/Marine intelligence organizations. These organizations operate under executive orders and regulations. The ATAC is an excellent source of terrorist intelligence information.

(4) Reports from Subordinates. Military personnel provide valuable observations. Unit sentries and patrols should be familiar with the area of responsibility and vigilant when patrolling. Assign personnel to the same area in order to develop an understanding of the locality's activities. Individual and unit training should stress observation and immediate reporting of abnormal circumstances encountered on patrol.

c. Expeditionary Operations. Once committed to combat operations, FMF units have an increased capability to collect information with organic assets. If predicting a terrorist threat, incorporate appropriate tasks into the collection plan. Sources of information increase to include United States assets, host nation support, and the local populace. Terrorist intelligence information becomes part of the intelligence effort. Terrorist intelligence information is prioritized as dictated by the circumstances.

3002. Essential Elements of Information

The following terrorist considerations assist the intelligence officer in developing essential elements of information:

- Organization, size, and composition of group.
- Motivation.
- Long- and short-range goals.
- Religious, political, and ethnic affiliations.
- International and national support (e.g., moral, physical, financial).
- Recruiting methods, locations, and targets (e.g., students).
- Identity of group leaders, opportunists, and idealists.
- Group intelligence capabilities.
- Sources of supply/support.
- Important dates (e.g., religious holidays).
- Planning ability.
- Degree of discipline.
- Preferred tactics and operations.
- Willingness to kill.
- Willingness for self-sacrifice.
- Group skills (e.g. , sniping, demolitions, masquerade, industrial sabotage, airplane/boat operations, tunneling, underwater maneuvers, electronic surveillance, poisons/contaminants).
- Equipment and weapons (on-hand and required).
- Transportation (on-hand and required).
- Medical support availability.

3003. Threat Estimates

Terrorist threat estimates are a routine, continuous process performed by the intelligence officer. If the command does not have an intelligence officer, the commander appoints a substitute. The NISCOM assists in formulating threat estimates. Staff interaction is essential to develop a thorough threat estimate. Members of the staff, physical security council, or CMT exchange and combine terrorist information in staff conferences. The results effectively evaluate security and counteraction abilities.

Carefully exercise judgment in estimating both the existing terrorist threat and the need for changes in security and counteraction measures. Key questions are:

- What has changed (mission, installation/unit, terrorist capabilities)?
- What conclusions may be drawn?

There is no impervious defense. Extraordinary security measures draw attention and detract from mission accomplishment. Sound physical security, accurate intelligence, and a well-rehearsed counteraction plan reduces the prospects of a successful terrorist venture. The aim is to make the level of risk unacceptable to the terrorist while reducing the risk to the installation/unit. A thorough threat estimate helps achieve this goal.

Development of a threat estimate follows the intelligence estimate format prescribed in appendix B of Joint Pub 0-2, *Unified Action Armed Forces (UNAAF)*, and FMFM 3-1, *Command and Staff Action*. Deployed units incorporate the threat estimate into the intelligence estimate. Installation, ship, and area vulnerability are assessed in the paragraph entitled "Characteristics of the Area of Operations." The terrorist situation is assessed in the paragraph entitled "Enemy Unconventional and Psychological Warfare Situation." In garrison, the information in figure 3-1 guides the installation/unit commander in the development of a terrorist threat estimate.

NOTE: Based upon the installation/unit's mission and assessments, the CMT recommends location and type of security (e.g., procedural, physical, electronic).

a. Mission. Review and analyze the mission of the installation/unit in relation to the terrorist threat. Perform this review and analysis during peacetime and mobilization.

b. Installation/Unit Assessment. Combine the results of the following assessments to create the installation/unit assessment. The installation/unit assessment provides the CMT with the installation's/unit's overall vulnerability to terrorist attack. The following assessments are informal documents developed by the CMT. Perform these assessments in high-risk situations.

Determine installation/unit commander's mission. Include any implied missions related to the installation's/unit's security.

Develop installation/unit assessment.

Develop installation vulnerability assessment.

Develop criticality assessment.

Determine feasibility of spreading or combining key assets and infrastructures. Input this data into the Installation Base Master Plan.

Determine if redundancy of key assets and infrastructures exists on the installation or within the geographic area.

Develop procedural plans in the event current assets are disabled.

Develop damage control procedures to minimize the effects of damage or destruction to key assets and infrastructure.

Develop procedures to recover damaged or destroyed key assets and infrastructures.

Develop a threat assessment in order to determine the following factors: *

1. Existence, or potential existence, of a terrorist group.
2. Acquired, assessed, or demonstrated terrorist capability level.
3. Stated or assessed intention to United States forces.
4. Previously demonstrated terrorist activity.
5. Probable terrorist target based on current information.
6. Internal political and security considerations.

*Level of Threat

Critical	Factors 1, 2, and 5 are present. Factor 4 or 3 may or may not be present.
High	Factors 1, 2, 3, and 4 are present.
Medium	Factors 1, 2, and 4, are present. Factor 3 may or may not be present.
Low	Factors 1 and 2 are present. Factor 4 may or may not be present.
Negligible	Factor 1 and/or 2 may or may not be present.

Figure 3-1. Guidance in Development of Terrorist Threat Estimate.

The CMT develops the physical security plan (see app. C) from the installation/unit assessment. The physical security plan addresses all terrorist threat levels regardless of the present level. Apply terrorist threat conditions (THREATCON) (see app. D) in accordance with the local threat.

(1) Installation Vulnerability Assessment. The installation vulnerability assessment (IVA) is a self-assessment tool. The installation/unit uses the IVA to evaluate its vulnerability to terrorist attack. The more vulnerable an installation/unit, the more attractive it becomes to terrorist attack. Appendix E provides an IVA format.

(2) Criticality Assessment. The criticality assessment identifies key assets and infrastructures located aboard and adjacent to the installation. It addresses impact of temporary or permanent loss of key assets or infrastructures to the installation's/unit's ability to perform its mission. The CMT determines and prioritizes critical assets. The commanding officer approves the prioritized list. The assessment—

- Selects installation's/unit's key assets and infrastructures.
- Determines whether key assets or infrastructures can be duplicated.
- Determines time required to duplicate key assets or infrastructures efforts if temporarily or permanently lost.
- Determines vulnerability of key assets or infrastructures to bombs, vehicle crashes, armed assault, and sabotage.
- Determines key assets and infrastructures priority of response in the event of fire, multiple bombings, or other terrorist acts.

(3) Damage Control Assessment. The damage control assessment determines the installation's/unit's ability to respond to a terrorist attack against key assets and infrastructures. Develop the damage control plan from this assessment. The damage control plan addresses key assets and infrastructures identified in the criticality assessment.

(4) Recovery Procedures Assessment. The recovery procedures assessment determines the installation's/unit's ability to recover from the temporary or permanent loss of key assets and infrastructures. Based on this assessment, the CMT establishes recovery procedures to ensure the installation's/unit's ability to perform its mission.

c. Threat Assessment. The CMT prepares or approves the threat assessment. Threat assessments examine the existence, goals, capabilities, history, activity trends, and targeting preferences of terrorist groups. Consideration of capabilities include leadership, resources, intelligence gathering, mobility, personnel, training, and preferred tactics/techniques. Address the possibility of attack from the ground, air, sea, and underground (e.g., tunneling, sewer lines). This assessment process generates additional essential elements of information. The ATAC through the local NISRA provides additional information concerning terrorist groups and capabilities to formulate this assessment.

Specific conditions show the potential for politically-motivated violence. The following list identifies conditions that appear as the normal exercise of people's rights, but when taken into context with other activities they become indicators of potential terrorist activity. The threat level is determined based on assessment of the following factors:

- Political, social, or ethnic dissention.
- Charges brought against local government.
- Formation of radical groups, branches of national subversive groups, or secret societies.
- Antigovernment or anti-United States agitation.
- Local government or United States accused of being the source of problems.
- New spokesmen for the people's cause emerges.
- Arrival of out-of-town organizers.
- Meetings, rallies, and demonstrations organized.
- Grievances take political overtones.

- Inflammatory speeches which contain accusations.
- Police or military authorities intervene or overreact.
- Appearance of anti-establishment posters, leaflets, or underground press.
- People's concerns taken into the political arena.
- Use of known personalities as draws for rallies.
- Demonstrations, civil disobedience, and protest marches with the actual causes overshadowed by political rhetoric.
- Increased recruiting, especially by known front groups and radical organizations.
- Increased activism in political spheres at colleges and universities.
- Speeches and communications advocating violence as the only means of solution.
- Identification of foreign influence or aid.
- Threats against public works, utilities, or transportation.
- Threats of violence against prominent personalities.

d. Terrorist vs. Friendly Vulnerabilities and Capabilities. Mentally wargame possible terrorist attacks against ability to respond in order to analyze an installation's/unit's ability. This is largely an exercise in "what if" thinking. Drills and exercises test suspected vulnerabilities and counteraction measures. These exercises and drills also train the CMT and CMF leadership.

Chapter 4

Security

Security measures are taken by military units, activities, or installations to protect effectiveness. Commanders are responsible for an installation's/unit's protection in garrison, forward deployed, or in combat. No unit is secure unless completely protected; e.g., front, flank, rear, air.

The threat of terrorist attack requires protection in the United States, foreign countries, and expeditionary operations. Commanders constantly assess installation/unit security against the terrorist threat in order to effectively evaluate security requirements.

Section I. Preventive Security Measures

4101. Tactical and Rear Area Security

Commanders are responsible for the security of their installations/units, including attachments. Security against terrorist attack in a combat zone is integrated into the command's overall operational plan. Protecting the Marine Air-Ground Task Force (MAGTF) rear area includes local security of installations (e.g., ports, bases, airfields, dumps), route security of lines of communication, control of indigenous personnel, defense against the enemy's stay-behind/deep attack units, counterintelligence, and operations security (OPSEC). Security forward of the ground combat element's (GCE) rear boundary is tactical in nature and coordinated by the GCE commander. The MAGTF commander establishes the general trace of the GCE rear boundary and assigns security coordination responsibilities. The aviation combat element (ACE) commander coordinates protection against air surveillance and attack. Generally, the combat service support element (CSSE) commander coordinates rear area security between the GCE and MAGTF rear boundaries. Rear area security requires coordination with host nation and joint/combined force authorities.

4102. Operations Security

Effective OPSEC programs continuously estimate the terrorist, train to eliminate compromise, and reduce targets of opportunity. Usually, the operations officer has staff cognizance over OPSEC. The operations officer coordinates with the intelligence officer. The intelligence officer is responsible for counterintelligence and terrorist threat estimates. To be effective, the OPSEC program avoids stereotyping operations, understands terrorist intelligence-gathering methods (see table 4-1), denies intelligence and information to the enemy, and integrates OPSEC into physical and personnel security protection programs. The OPSEC program denies the enemy access to intelligence and information. It relies on information security, physical security, signal security, and deception to deny enemy access. Counterintelligence efforts focus on the hostile intelligence threat and possible methods of defeat.

The OPSEC plan avoids set patterns within operations. When the pattern of an operation cannot be altered, use deception or other security procedures to confuse terrorist intelligence efforts.

Table 4-1. Terrorist Intelligence-Gathering Sources

Exploitable Sources	Activities	Countermeasures
Human Intelligence	Casual conversations Planting agents	Training personnel Countersurveillance Counterintelligence
Signal Intelligence	Interception of communication signals	Communications security Information security
Photo Intelligence	Photographing activities from aircraft, high terrain, or automobile	Counterintelligence Countersurveillance Access control
Operational Patterns of Military Organizations	Observing stereotyped operations	Randomize operational patterns Employ deception

Change operational procedures on a random basis to confuse the terrorist and increase the terrorist's risk. This is not only an OPSEC measure, but also a physical security measure.

For example, terrorists have difficulty anticipating patrolling patterns when patrol routes are changed on a random basis.

Increase the degree of random action by altering routes, changing patrol schedules, or assigning personnel to different areas and shifts.

For example, instruct security patrols to check vehicles using a predetermined indicator on a random basis. Establish the time period as a 3-hour span. The first 45 minutes security patrols check vehicles with a 5 on the license plate. The next 75 minutes security patrols check vehicles with an L on the license plate. The next 30 minutes security patrols check all blue vehicles. The last 30 minutes security patrols check every vehicle with two or more occupants.

Use a similar schedule to inspect the identification of personnel entering an installation. Terrorists gain entry to commands during peak traffic periods because they can predict vehicle checks. Because vehicle and personnel restrictions apply, consult the staff judge advocate before conducting random inspections. Simple security procedures are effective when enforced. Simple, low-cost methods of OPSEC include controlling the itineraries of high-risk personnel (see apps. F and G), locking offices and buildings (see apps. H and I), and stopping strangers for proper identification (see app. H). Effective OPSEC can also reduce soft target risk (see app. J).

Essential elements of friendly information (EEFI) are items associated with friendly planning and capabilities. EEFIs exposed to hostile intelligence agencies or terrorists could compromise friendly intentions. The operations officer, in coordination with the CMT, develops an EEFI list. The EEFI list identifies intelligence indicators of interest to terrorists. The indicators guide the OPSEC program. Table 4-2 provides samples of intelligence indicators and is not inclusive.

Table 4-2. Intelligence Indicators

Sources	Indicators
Operation	Troops restricted to the post before an operation.
	Patrolling/air reconnaissance increases.
	Patrolling halted.
	Movement between locations increases.
	Requisition of rations, transportation assets, and ammunition increases.
Human Intelligence	Newspaper or media coverage increases.
	Farewells and visits by VIPs or senior officers.
	Church services the night before an operation.
	Base bulletin notices stress increases in rest, changes in dispensary hours, etc.
	Public signs announce changes in procedures (e.g., restricting civilian travel/access).
Communication	Call signs and frequencies change.
	Auxiliary communication equipment repositioned.

4103. Physical Security

Physical security protects and safeguards personnel from criminal and terrorist acts. Physical security programs prevent unauthorized access to equipment, facilities, material, and documents. Physical security programs deny, delay, deter, and detect criminal/terrorist activity. A sound physical security program includes analyzing, planning, executing, and evaluating courses of action to improve the security of offices, quarters, and installation facilities. See appendixes H, I, J, K, and L.

Tailor the physical security program to the local threat and security requirements determined by the installation's/unit's commanding officer. The commanding officer receives information and recommendations from the installation physical security council, threat committee, CMT, military police, provost marshall office (PMO), and installation/unit threat assessments. The commanding officer establishes the physical security council to oversee planning and coordination of all internal security matters. Military police and PMO conduct physical security surveys and analysis. Within the PMO, Marines who have completed the physical security course at Fort McClellan, Alabama (or its equivalent) conduct physical security surveys. The threat committee generates and maintains the threat assessment. The CMT can serve as the threat committee. Executing a physical security program requires centralized command and control (performed by the CMT), a group (usually the physical security council) to plan and coordinate activities, a security force (composed of the CMF and interior guard), and an active THREATCON system (see app. D).

The installation physical security program is described in a comprehensive physical security plan (see app. C). The physical security plan addresses specific detection, assessment, response, delay, and communications measures taken to safeguard personnel, material, and equipment. At a minimum, the physical security plan addresses establishment of an interior guard, access criteria, protective barriers, lighting, intrusion/sensor systems, lock and key controls, communications, special security measures (patrols, vehicle searches, etc.), liaison with civil agencies, and community relations programs. Most importantly, it addresses the crisis management procedures designed to combat terrorist activity.

Physical security surveys, crime prevention surveys, and personal security assessments for high-risk personnel identify existing or potential conditions conducive to terrorist activity. The IVA (see app. E) analyzes an installation's/unit's vulnerability. The IVA provides an accurate assessment of installation vulnerability when used in conjunction with the installation's OPSEC plan and crime prevention program.

4104. Personnel Security

Personnel security involves measures taken to reduce vulnerability of an individual to attack (from simple larceny to assassination). This includes self-protection measures, personal security, and protective services. No one is immune from the threat of terrorism. DOD personnel must remember they can easily become objects of terrorist activity. Terrorists select specific people as targets for kidnapping, extortion, hostage-taking, and assassination. Terrorists also select offices, power stations, manufacturing plants, on-base housing, or other installation assets as targets for bombings, sabotage, or assaults. Personnel occupying these facilities innocently become terrorist targets. Because attacks on DOD personnel continue to increase, it is critical to include personnel security procedures in antiterrorism planning. Personnel security plans decrease risk and improve chances of survival. Incorporate awareness briefings and basic crime prevention training into personnel security programs. Review and constantly update the personnel security program to develop a list of high-risk personnel and recommend protective measures.

Personnel become terrorist targets because they have unique expertise or special knowledge. Usually, the higher a person's rank or status, the greater the risk. In high-risk areas, implement special procedures to protect ranking officers, dignitaries, and dependents. Potential targets are classified as primary, secondary, or random targets.

Primary targets include ranking officers, dignitaries, very important persons (VIP), and individuals possessing sensitive information. Terrorists select primary targets because of their publicity value. Primary targets are identified during threat assessments or named in intelligence reports. If a primary

target is identified and personnel security procedures are implemented, risk to the terrorists rise and terrorists attack a secondary target instead.

Terrorist acts against DOD personnel are often against secondary targets. Secondary targets are usually persons of lower rank and pose less risk than primary targets, but they are used by terrorists to achieve publicity. These actions usually occur after primary targets are hardened. Unfortunately, security resources for secondary target personnel are not always available. If resources are not available, self-protection is the only recourse.

Many terrorist attacks are initiated against randomly-selected DOD personnel. Some attacks are against off-duty enlisted personnel wearing civilian clothing. DOD personnel must realize that they are not safe overseas.

a. Prevention. The three stages of prevention in a personnel security program are planning, awareness, and education. The planning stage includes a threat analysis and an assessment of available personnel/security resources. Integrate awareness and education stages into an installation's/unit's normal operating and training procedures. Explain the need for personnel security procedures during the awareness stage. Present preventive procedures during the education stage. Develop special preventive procedures for primary and secondary targets. Develop general preventive procedures for other personnel; e.g., dependents and civilian employees, who might become random targets. Marine Corps personnel, dignitaries, civilian employees, and dependents must be aware of the overall terrorist threat, as well as the installation's/unit's perceived threat level.

Periodic briefings and the preparation and dissemination of printed materials enhance awareness and education. When preparing material for dissemination, consult the nearest counterintelligence unit/team, PMO, or the NIS office. Also, consult with the staff judge advocate to ensure compliance with current directives and regulations. The public affairs office and PMO can help develop and deliver awareness briefings outside normal training channels.

Awareness briefings are not restricted to terrorism awareness. They can include crime prevention awareness which reduces the probability of victimization and heightens overall awareness. Make presentations to on-post schools and social and service organizations. These briefings heighten awareness of the area's personnel security risks, tactics and strategies used by terrorists, and types of facilities and personnel targeted. In addition to briefings, the public affairs office and PMO can use other multimedia means to promote awareness.

Because it is logistically impossible to protect all targets, self-protection and crime prevention determines overall success of the program. All personnel at the installation should receive crime prevention training. Crime prevention techniques augment individual protective measures. Encourage military personnel and dependents to participate in crime watch programs and to report all suspicious activities.

b. Individual Protective Measures. Individual protective measures decrease an individuals vulnerability to terrorist attack. Alert and trained individuals minimize the likelihood of terrorist success and act as deterrents to terrorist activity. FMFRP 7-14A, *The Individual's Guide for Understanding and Surviving Terrorism*, provides individual protection measures. Appendix F provides a checklist of security precautions. Appendixes G, J, M, and N contain additional personnel security measures.

c. Security Precautions

(1) High-Risk Personnel. General officers, VIPs, and their families are high-risk personnel. High-risk personnel follow the precautions identified in appendixes F and G. Other individuals are termed high-risk because of their nationality (pastor present), duty position, and assignment areas. Examples of other high-risk personnel are law enforcement personnel, embassy personnel, United States military, foreign area specialists, recruiters, and personnel in isolated special assignments. High-risk personnel

have special security needs regardless of rank. Drivers for high-risk personnel should be aware of the precautions contained in appendix M. NIS agents provide personal security to high-risk personnel. The PMO assists NIS agents. The PMO does not normally provide personnel security off the installation. During combat operations, the PMO is not restricted to the installation when performing personnel security. The primary mission of personal security teams is to protect, cover, and evacuate high-risk personnel.

(2) Individual Travel. Appendix F addresses security measures designed to reduce personal risk while traveling. FMFRP7-14, *The Individual's Guide for Understanding and Surviving Terrorism*, provides additional information on individual travel. Education and awareness are the cornerstones to personnel security. Individuals are vulnerable when separated from their units. Remember OKINAWA when traveling.

O bey security orders

K now your interior guard routines

IN quisitive

AW are

A lert

(3) Liberty Parties. Unique security precautions apply to Marines on liberty. Initial preparation for a port visit includes coordination with United States authorities and host nation officials to determine potential for terrorist attack of liberty parties; host nation responsibilities and procedures for protecting personnel on liberty, piers, landings, and visiting ships; and coordination between local authorities and shore patrol. The commander may request an ATAC threat assessment. Deployed units embarked aboard Navy ships in the Mediterranean automatically receive a threat assessment 7 to 10 days before each port call.

Liberty party preparations include organization and schooling for the shore patrol; indoctrination of troops regarding the situation ashore, response to trouble, deployment precautions, courtesy, and areas to avoid; and coordination with the Navy to assist in security. Develop recall provisions. Make officers and noncommissioned officers aware of their responsibilities in a developing situation.

Organize liberty parties around the buddy system. No Marine or sailor goes on liberty alone. Depending on the situation, organize the liberty party into two- or four-man buddy teams. Each member of the team is responsible for the safety of his shipmates. The aim is avoidance and prevention of trouble. Keep in mind you are a guest and have no authority ashore except that extended by the host nation.

Section II. Protective Security Measures

Defense against terrorist acts demands a continual awareness of the terrorist threat, but it also requires units to take certain protective measures in order to minimize danger. OCONUS units may be required to implement aggressive protective measures in support of the host nation. The following equipment is suggested for all units operating in a terrorist environment.

Pyrotechnic pistols
Riot guns
Tear gas launchers
Hand-held flashlights
Antiriot helmets
Side-handled batons
Handcuffs
Body armor
Leg armor
Hand-held radios
Shields, 3-feet 6-inches
Cameras w/flash attachments, tripods
Marshaling wands
Telescopes and tripods
Binoculars
Infrared devices
Loud speakers
Telescopic sights
Photographic filter
Polaroid camera
Whistles
Fire extinguisher
Shields, 6-feet

4201. Protecting Security Operations

a. Urban Installations. Forces are frequently employed in urban areas for security operations or other short, conventional, combat-related tasks. Easily defended locations are rare in urban areas. Political restrictions limit the military's ability to construct fortifications or disrupt urban areas. Adapt masonry structures or other urban formations to provide protection based on the mission, avoid enemy attack, and effectively use surroundings.

(1) Estimate Situation. Prior to starting work, complete a thorough estimate of the situation using mission, enemy, terrain, troops-time (METT-T) factors. The following questions aid in developing an estimate of the situation (see fig. 4-1).

(2) Develop Plan. Defend installations with a combination of fortifications, obstacles, local security, interior guard, and on-call support from reaction forces. Each situation requires its own combination of abilities.

Fortification is an aid to defense; not defense as a whole. Select masonry buildings and determine roof/floor load bearing limitations before stacking sandbags. Use engineer support as available. Fortification options include wire fences, screens, canopies, and sandbags (see table 4-3). If additional coverage is required, dig down rather than building up. Wire fences delay access, channel movement of personnel and vehicles through manned control points, and act as barriers against grenades and high explosive antitank (HEAT) rockets. Fences are as high as possible and covered by observation and direct fire. Place screens on frames and locate outside buildings or inside windows. Screens deny observation and sniping opportunities. Tape window glass to reduce blast splintering. Place canopies at least 1 meter from the roof to provide roof protection and detonate mortar projectiles before they reach the roof. Sandbags directly on the roof absorb shrapnel. Heavy machine guns and air defense teams on rooftops provide air defense and cover. Use internal defense to establish internal fighting positions. Designate safe rooms (interior rooms offer best structural protection

Mission
- What is happening?
- What is your role?

Enemy
- Who is the enemy?
- What is known about the enemy?
- How does the enemy receive information?
- How might the enemy attack? (Think like the enemy! Would you ambush, raid, or swarm? Would you use a sniper, mortars, rockets, air or ground attacks, suicide attacks, or bicycle/car/truck bomb?)
- Are there any known daily routines?

Terrain
- What are the strengths/weaknesses of the installation and local surroundings?
- Are avenues of approach above or below the ground?
- Are there key buildings that could become a valuable asset?
- Are there observation areas, dead spaces, fields of fire, illumination, or no-fire areas (e.g., schools)?

Troops
- Determine the friendly situation.
- Are there forces or equipment available?
- Are there engineers in the area? Will they be able to provide support?
- Are there emergency reinforcements available?
- What are the host nation responsibilities and capabilities?

Time
- Determine the duration of the mission.
- Are there time constraints?

Figure 4-1. Estimating the Situation.

against collapse) for noncombatant personnel. Personnel should know the location of safe rooms. Locate fighting positions away from windows to make best use of enfilade fire. As a final defensive measure, use sandbags to strengthen fortification of safe rooms.

Obstacles slow down or stop vehicles and personnel approaching an area. Construct vehicle barriers using trenches, masonry barriers, concrete-filled oil drums, and vehicles. Obstacles are staggered across the route creating a zig-zag maze. This forces the vehicle to slow down and make sharp turns, and exposes the driver to direct fire. Scatter speed bumps or sandbags on the route to further slow traffic. Design entrance gates to allow access to authorized personnel, deny access to unauthorized personnel, and provide time and protection to guards. Illuminate and cover fences, entrance gates, and obstacles by observation and fire.

Establish local security and interior guards around-the-clock to provide observation and fire capabilities. Post sentries at entrances to check right of entry and in observation posts (OPs) and on rooftops to view surrounding area. Sentries also patrol the perimeter.

Table 4-3. Fortification Materials

Fortification	Material	Purpose
Wire fences	Barbed wire	Delays access.
	Concertina wire Chain link/weld mesh	Channels movement through manned control points. Chain link/weld mesh can be used as grenade and HEAT rocket barriers.*
Screens	Canvas Plywood Corrugated iron	Denies observation. Denies sniping attacks.
Canopies	Chain link/weld mesh	Protects roofs.
	Corrugated iron	Detonates mortar projectiles before they reach the building. Absorbs shrapnel. Covers machine guns positioned on roofs.
Sandbags	Sandbags	Absorbs shrapnel. Protects personel and equipment.

* At least 10 meters standoff distance to neutralize HEAT blasts.

(3) Establish Defense. Continually review measures taken to establish the defense and update to counter the changing threat. Defensive measures include—

- Determining priority of work (assign sectors of observation and fire, construct obstacles, fortify).
- Improving obstacles, fortifications, and the defense as a whole.
- Establishing watch routines, inspections, and immediate action drills.
- Maintaining radio communications with the reaction force.
- Keeping abreast of current military and host nation intelligence assessments.

b. Sentries in Urban Areas. Sentry duties are detailed in FMFM 6-4, *Marine Rifle Company/Platoon*, and in general and special orders. Special orders address details of authorized passes and provide samples of passes; how to search people and vehicles; response to approach by unauthorized personnel or hostile crowds; response to potential damage, looting, or arson; procedures to call for assistance; and response to unauthorized photography. There must always be a reaction force a sentry can call for immediate assistance. The sentry must know the extent of his post, specific duties, time span of his duty, designated uniform and equipment, and rules of engagement (ROE) in regard to minimum force and its application. A sentry's responsibilities in an urban area include—

- Detecting and deterring anyone seeking to gain unauthorized access to the security area.
- Detecting and deterring anyone seeking to gain intelligence about the security area.
- Preventing damage, arson, or looting to the security area.
- Ensuring maintenance of essential services.
- Dealing appropriately with individuals in the vicinity who could be either a curious civilian or terrorists.

c. Road Movement. Road movement is always vulnerable in high-risk areas. If possible, use alternate forms of transportation (e.g., helicopters). If road movement is required,—

- Avoid establishing a regular pattern.
- Vary routes and timing.
- Never travel in a single vehicle.
- Avoid traveling at night or during periods of agitation.
- Keep a low profile.
- Plan alternate routes and reactions to various threatening scenarios.
- Plan communications requirements.
- Avoid dangerous areas.
- Provide adequate security.

(1) Driving Procedures. A driver's defense lies in alertness, driving skill, and vehicle's mechanical condition. FMFRP 7-37, *Vehicle Bomb Search*, provides excellent information on preventing and detecting explosive devices. FMFRP7-37 should be located in all Marine Corps vehicles, especially those used by high-risk personnel. Appendix M contains detailed procedures for drivers operating in a high-risk area.

(2) Vehicle Protection. Take the following precautions when using vehicles in a high-risk area:

- Place sandbags on floorboards and fenders.
- Cover sandbags with rubber or fiber mats.
- If carrying troops, sandbag the vehicle bed as well as the driver's compartment.
- Remove canvas so passengers can see and shoot.
- Fold windshield in driver's compartment and fit high-wire cutter.
- Carry no more than one squad per truck.
- Passengers riding in truck bed face outboard and are assigned sectors of observation and fire.
- Rig chicken wire or chain link screens on bow frame to deflect rocks, bottle, and grenades.
- Carry pioneer tools, a line with grappling hook to clear obstacles, and tow bars for disabled vehicles.

(3) Convoys. In high-risk areas, use armed escorts for convoy protection. Develop and rehearse immediate action drills before movement. Perform route clearance prior to movement. Establish and maintain communications throughout the route. Develop deception plans to conceal or change movement timing and route and to deploy false convoys to contribute to the convoy's security.

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. Due to the presence of civilians, exercise caution when responding to ambushes.

Escort composition depends on available forces. Light armored vehicles and entrucked infantry are desirable, but high mobility multipurpose wheeled vehicles (HMMWV) or trucks equipped with M-2 50 caliber and MK-19 40mm machine guns can also be used. Overhead helicopters provide excellent escort if available. Escorts are organized into an advance guard, main body escort, and reaction or strike group.

(a) Advanced Guard. Amphibious tractors (LVTP7), light armored vehicles (LAVs), or vehicle-mounted infantry can form the advanced guard. The advanced guard clears obstructions and alerts the convoy to danger. The advanced guard travels forward of the convoy to effectively accomplish its mission while remaining close enough to provide required support.

(b) Main Body Escort. LVTP7, LAVs, or vehicle-mounted infantry can form the main body escort. The main body escort provides immediate close protection for the convoy. The main body escort is scattered within the convoy. Collocate the main body escort commander with the convoy commander. The main body escort commander remains in constant communication with the advance guard and reaction or strike group.

(c) Reaction or Strike Group. LVTP7, LAVs, or vehicle-mounted infantry can form the reaction or strike group. The reaction or strike group follows the convoy's main body. The reaction or strike group conducts counterattack if the main body is ambushed.

(d) Convoy Orders. The convoy commander coordinates with the transport commander, estimates the situation, and develops plans. Thoroughly brief road movement personnel on convoy/escort composition and order of march; chain of command; alertness posture; communications and special signals; objectives, routes, and schedules; and response to emergencies and at halts. Convoy orders follow the typical five-paragraph format with the execution paragraph containing the information emphasized in figure 4-2.

d. Rail Movement. Rail movement is the most difficult to conceal and protect. It follows a predictable route and loading is difficult to conceal. Opportunities for deception are limited and physical protection is critical. The following security precautions should be considered:

- Restrict passengers to military personnel only.
- Search for explosives or possible hijackers before departure and after every halt.
- Ensure railway is free of obstructions or explosives.
- Patrol the railway area.
- Place armed security personnel on duty throughout the journey.
- Patrol and guard departure and arrival stations.
- Use deception measures.
- Air patrol the route.
- Maintain communications within the train and with outside agencies.

e. Sea Movement. Sea movement, especially aboard military vessels, can give a ground force commander a false sense of security. Sea operations

1. Situation
   a. Enemy Forces
   b. Friendly Forces
2. Mission
3. Execution
   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 vehicle, and expected arrival of first and last vehicle at destination.
   g. Identify action upon arrival.
   h. Determine required coordinating instructions for–
      - **Speed.**
      - **Spacing.**
      - **Halts.**
      - **Immediate action drills (e.g., sniper, ambush).**
      - **Vehicle breakdown plans.**
      - **Drivers who get lost or separated.**
4. Administration and Logistics
5. Command and Signal

Figure 4-2. Convoy Orders.

are certainly more secure than urban patrols; however, ships in harbor or anchored off hostile coastlines are visible threats and high-risk targets. Use visible forms of military readiness such as troops in battle dress, bayonets, sharpshooters, and OPs to discourage terrorist attack. Ships in harbors need to evaluate each new port and determine possible terrorist threat. Crew members must be aware of host nation support/responsibilities while in port or anchored foreign waters. Vary routines (security practices can be passed from one port to another by opposing forces). Inspect all personnel and provisions coming aboard or alongside the ship and before allowing visitors off the quarterdeck.

Troop commanders and the ship's captain coordinate duties and responsibilities for their mutual defense. Remember that the ship's captain is solely responsible for the ship and all those embarked. Establish agreement on uncomplicated chains of command. Personnel must understand the roles of sailors and troops. Establish methods of embarkation/debarkation and patrol activities for all personnel. Identify vital areas of the ship (e.g., engine room, weapons storage, command and control bridge) and assign security guards. Coordinate above and below waterline responsibilities. Since large numbers of troops are confined to a ship, establish a weapons/ammunition policy and ROE, appoint a reaction force, drill frequently, and know weapon capabilities and ricochet effects.

NOTE: Ensure all hands understand a drill is underway.

f. Air Movement. For the most part, while a unit is being transported by air, it is in the hands 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 liaison with airfield security personnel, assist departures and arrivals at airfields and en route, and determine weapons and ammunition policies. Personnel usually travel with their personal weapons. If the threat is high, deposit limited ammunition with the air crew and issue shortly before landing.

Road transport security when driving to and from airfields is critical. Keep arrival arrangements low profile. Do not preposition road transport at the airport for extended periods before arrival. If prepositioned transport is required, attach a security element and station within the airfield perimeter. Security at the arrival airfield can be host nation responsibility and require close liaison. Maintain an open communications net between all elements until the aircraft is loaded and re-establish communications upon arrival.

g. Urban Patrolling. Many of the procedures, especially planning, contained in FMFM 6-7,

Scouting and Patrolling for Infantry Units, apply to urban patrolling. Units OCONUS may be called upon to conduct patrols in urban environments. Urban patrols support police operations, dominate a hard area, gather information, police clubs and restaurants, make planned arrests, conduct hasty searches, and emplace hasty roadblocks. 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. In urban areas, base sentries or guards, other vehicle patrols, helicopters, OPs, and reaction forces provide support.

Often, the patrol's main mission is to display a presence, thereby creating public confidence. In low-risk areas, walk with an atmosphere of relaxed confidence and talk and interact with local citizens. This provides a potential source of information and instills confidence and respect from an area's citizens.

(1) **Foot Patrols.** Foot movement in an urban area follows the principles of mutual support, fire, and maneuver.

(a) Formations. A foot patrol's basic unit is a fire team. Two or more fire teams perform urban patrolling. Fire teams operate 100 meters apart. Internally, members of a fire team patrol in column formation, with men on each side of the street, 15 to 25 meters apart.

(b) Covering Fire. Individuals within a patrol may work in pairs. Individuals within and between pairs provide covering fire. Within the pair, one covers the rear yet remains in sight of the other member.

(c) Hard Targeting. In high-risk areas, move from one firing position to another. Never move without cover from the other member of the pair. Assume proper firing positions, keep rifles at the ready, and scan the area through weapon sights. Avoid hard targeting if possible. Use hard targeting when crossing obstacles, reacting to contact, leaving or entering a static base or OP, in areas with high sniping threat or history of contact, or when breaking up a pattern of movement.

(d) Obstacle Crossing. Normally, a fire team provides its own cover by fire with either pairs or individuals moving. To cross open ground, use whole fire teams within a multiple as cover.

(2) **Vehicle Patrols.** Vehicle patrols can be separate patrolling operations or combined with foot patrols to form a highly mobile patrolling operation. Vehicle patrols consist of two vehicles moving within sight of each other, but not presenting a joint target. Vehicles travel at no more than 10 to 15 miles per hour. Vehicle crews dismount at every stop to provide security. Crews should hard target on foot into and out of a site.

h. Urban Roadblocks. There are two types of roadblocks: deliberate and hasty. Deliberate roadblocks are permanent or semipermanent roadblocks used on borders, outskirts of cities, or the edge of controlled areas. Use deliberate roadblocks to check identification and as a deterrent. Use hasty roadblocks to spot-check, with or without prior intelligence. Hasty roadblocks use the element of surprise. Their maximum effect is reached within the first half hour of being positioned. Hasty roadblocks can consist of two vehicles placed diagonally across a road, a coil of barbed wire, or other portable obstacles.

OH 3-5, *Employment of Military Police in Combat*, (currently being developed for release as FMFM under the same number and title) provides procedures used to establish and conduct a roadblock. 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 relinquish suspects to civil police promptly. General principles considered in establishing roadblocks are concealment, security, construction and layout, manning, equipment, communications, and legal issues.

(1) Concealment. Position roadblocks so they cannot be seen from long distances. Sharp bends or dips in a road provide ideal concealment.

(2) Security. Man roadblocks with enough personnel to stop and search vehicles and respond to the potential threat the roadblock can reveal. Initially stop cars at a checkpoint well short of the main search area to minimize the effect of car bombs.

(3) Construction and Layout. Set up the roadblock so it is visible to traffic flow once there is no egress except through the roadblock. The layout should force the vehicle to slow and stop short of the search area. Allow vehicles to either pass through the roadblock or direct into the search area. Position covering forces with clear fields of fire of both the initial checkpoint and search area.

(4) Manning. Manning requirements depend on the threat and expected volume of traffic. Specialized personnel may be required (civil police, female searchers, interpreters, and explosive ordnance disposal [EOD] personnel).

(5) Equipment. In addition to the equipment identified at the beginning of section II, the following equipment is recommended for units conducting roadblocks.

Portable lamps/lights	Marker lights
Car puncture chains	Traffic signs
Lightweight barriers	Traffic cones
Directional arrow	Mirrors
Visor sleeves	

(6) Surveillance. Early warning and night observation devices should be available to roadblock personnel.

(7) Communications. External and internal communications are essential. Maintain communications with the parent unit commander, reaction force, and host nation's military and civilian police at all times.

(8) Legal Issues. Personnel manning roadblocks must be aware of their legal authority, duties, and limitations regarding search, arrest, and use of force. ROE are commensurate with the threat and clearly understood by every Marine.

i. Observation Posts in Urban Areas. OPs provide prolonged, covert observation of areas, people, or buildings. OPs allow observation of an area for possible enemy activity (avenue 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. Personnel from the scout/sniper platoon can be used for OP duty.

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/clothes, and using deception. Report compromise immediately.

Urban areas afford the use of derelict and occupied houses, shops, and schools as OPs. Derelict houses are excellent OPs. Clear derelict houses of boobytraps before occupation. Occupied houses pose danger of compromise. Use occupied houses only in the owner's absence if possible. Use shops during nonbusiness hours and do not occupy for more than 12 hours. Use schools during weekends and holidays. Due to the inquisitiveness of children, special care is required when using schools.

(1) Planning. To be effective, carefully plan OPs. Planning addresses the mission, terrain, friendly disposition and routines, enemy situation, and local situation. Reconnoiter the area and select a site with good observation; concealment; and covered approaches, entries, and exits. Teams and equipment (e.g., binoculars, special observation equipment, seismic devices,

cameras, weapons, radios) should be appropriate to the task. Teams should have experienced leadership, unit cohesion and confidence, patience and endurance, and restraint. OP planning addresses time and method of occupation, relief, and closure (e.g., personal camouflage, screens, inspection by passing patrols); watch routine; concealment and protection; ROE; administration and support requirements (e.g., food, water, batteries, head arrangements, record of event log); and communications needs (e.g., radio, telephone, call signs, codewords, passwords, challenges, pyrotechnic signals, radio discipline).

(2) OP Orders. OP orders follow the typical five-paragraph format with unique inclusions identified in figure 4-3.

4202. Searches

a. Vehicles. Figure 4-4 depicts areas to thoroughly examine during vehicle searches. FMFRP 7-37, *Vehicle Bomb Search*, provides excellent information on vehicle bomb search procedures. Vehicle searches also follow the guidelines in setting up roadblocks (par. 4201h) and personnel searching (par. 4202b). Always have someone covering the searchers and those being searched.

b. Personnel. Conduct searches in a professional, cautious manner. Limit conversation to instructions necessary to conduct the search. Extend appropriate respect to persons being searched. The aim is to provide security without creating animosities. Be courteous but firm, and maintain total control of the situation. Whenever possible, women search women and men search men. If a female searcher is unavailable, another person is present to observe the searching of women by male Marines.

Searchers should work in pairs, and search each individual separately. Use two searchers with one searching and the other covering. Searchers always work from behind. Position the person being searched in front of a wall (or car) with legs apart and hands against the wall in a leaning position. Position the individual in such a way that he cannot move without falling down or being easily knocked down. Watch for facial reactions, nervousness, or sweating. There are two types of searches: quick body search or frisk and detailed body search.

(1) Quick Body Search or Frisk. Use the frisk as a preliminary search to detect weapons or as a usual form of search in a low-risk area.

1. Situation
   a. Ground. (Determine required maps, aerial photographs, sketches, models required.)
   b. Enemy Forces. (Identify suspects, local inhabitants, pattern of life, weapons, cars, dogs, etc.).
   c. Own Forces. (Identify actions of the parent command, reaction force, other OPs, and patrols.)
2. Mission. (Identify specific OP tasks.)
3. Execution.
   a. General Outline. (Summarize the operation and composition of OP.)
   b. Occupation of OP. (Identify routes and methods.)
   c. Operations Routine.
      - Position each man in the OP.
      - Locate field of view and target areas.
      - Detail watches.
      - Position equipment.
      - Record information in a log.
      - Administrative routine.
      - Reaction to a suspect or target.
      - Orders for compromise.
   d. Withdrawal Method and Route.
4. Administration and Logistics. (Identify individual and special equipment, food, water, batteries, dress, weapons, and medical.)
5. Command and Signal. (Identify chain of command, passwords, codewords, nicknames, call signs of reaction force, and other patrols and orders if communications breakdown.)

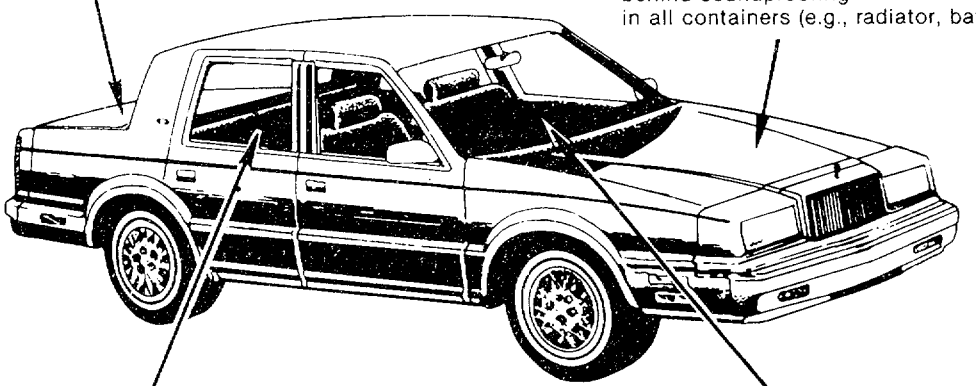
Figure 4-3. Observation Post Orders.

TRUNK

Have driver open and identify contents.
Places to check: under and around spare wheel
in tool boxes
in luggage
use gauge to check air in spare tire
in spare wheel housing
between rear seat and trunk partition.

HOOD

Have driver open hood.
Look for items taped to bulkhead or hood.
Places to check: oil and air filters
front grill
heater
behind soundproofing
in all containers (e.g., radiator, battery).



PASSENGER COMPARTMENTS

Methodically check vehicle compartments from front to rear.
Be suspicious of strong-smelling perfume/deodorant.
Places to check: behind dash
fittings (e.g., radio/cassette)
glove compartments
behind panels
under floor mats
in, under, and between seats and cushions
open windows
stuffed toys and decorative animals
ashtrays.

OCCUPANTS

Search drivers and passengers.
Search loose baggage.

NOTE

Search the following areas of commercial vehicles:
driver's cab
space between body and cab
external storage areas/bins
wooden bodies
false floors and sides
space between rear double wheels
wheel chocks

Figure 4-4. Vehicle Search Areas.

Follow a logical search sequence from head to toe. Use both hands and stroke (rather than pat) all clothing. If possible, use a metal detection system. Check the following areas carefully:

- Hair.
- In and under hats.
- Armpits.
- Inside legs.
- Half-clenched hands.
- Medical dressings or bandages.
- Bags or cases.
- Walking sticks, umbrellas, or crutches.
- Shoes, boots, or socks.

(2) Detailed Body Search. If possible, set aside a specific room or area for detailed body searches. A corpsman and a female searcher should be in attendance. The following sequence should be used:

- Establish identity.
- Establish ownership to baggage.
- Direct individual to turn out all pockets.
- Direct individual to remove all clothes, jewelry, watches.
- Inspect body from head to foot. Pay attention to hair, ears, mouth, teeth, body orifices, crotch, and between toes.
- Examine clothing. Pay attention to linings, seams, buttons, belts, shoe or boot soles, and heels.
- Examine contents of pockets.
- Examine baggage and other articles (sticks, umbrellas).

c. Houses. Figure 4-5 depicts places in a house used to conceal contraband. Pay special attention to these areas.

When searching, search and reposition furniture to allow freedom to search floor, walls, and baseboards; remove floor coverings; check for trap openings in floors and loose floorboards and baseboards; check ceilings for trap doors or false ceilings; and check and clear walls visually, by tapping, and by using a metal detector. To conduct a thorough search, the following equipment may be required:

Ladders	Flashlights
Picks, shovels	Wrecking bars
Magnets	Telescopic mirror
Axe	Mine markers
Helmets	White tape
Mine detectors	Eye shields
Measuring tape	Metal cutting tools
Chisels	Knives
Safety harness	Rope
Hand tools (hammers, pliers, screwdrivers)	Saws Mine probes

(1) Occupied

(a) Approach, Entry, and Search. Search teams enter quickly and assemble home's occupants in one room. Search occupants to ensure safety of team. Team leader searches team in front of occupants to prevent accusations. Draw plan of house and search from top to bottom and left to right. Head of household accompanies search team while the remainder of the household remains in one room. Report to the team leader as each room is cleared. To avoid accusations of theft, search in pairs.

(b) Exit Procedures. Leave the house in its original condition. Repair damage or team leader completes and signs a damage claim form. The team leader searches team members in front of the head of the household to ensure there has been no theft.

(2) Unoccupied

(a) Approach, Entry, and Search. Search the furnishings and interior of an unoccupied house in the same manner as an occupied house. Establish a command post outside the building. Assume unoccupied or derelict houses are boobytrapped, and clear boobytraps before beginning search. Make



ATTICS

Roof area, skylights
Between eaves and roofing
Gutters and drain pipes
Water tanks
Heat/air ducts
Rafters, insulation
Storage boxes

BASEMENTS

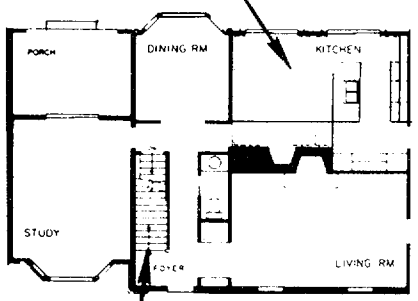
Water heaters
Furnaces, stoker, coal bins
Overhead joists and ducts
Floors, drains, walls

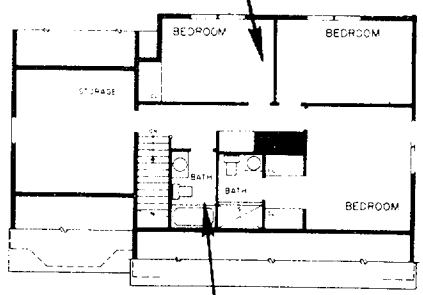
KITCHEN

Walls, cabinets, closets
Refrigerator, stove, domestic appliances
Food containers, pots, utensils

ROOMS

Doors, windows, outside ledges
Furniture, interior fittings, lights
Walls, air vents, paneling, bookcases, ceilings
Fireplaces and chimneys
Floors and floor coverings, baseboards
Closets





STAIRWAY

Staircase frame and step treads
Panels

BATHROOM

Around sinks, toilet tanks, bathtubs
Walls, windows, floors
Mirrors

NOTE

Other areas of particular concern are tubular systems, false letter boxes, bedding, behind mirrors, toys, suitcases, air inlet systems, sewer, drainage systems, electric boxes, garages, root cellars, haystacks, and sheds.

Figure 4-5. House Search Areas.

a visual reconnaissance of the building's exterior for suspicious signs (e.g., wires, signs of fresh digging, explosive wrappers, footprints). Detail a pair of searchers to make initial entry. Do not enter through a door. Check windows for boobytraps before entry. Ideally, holes in walls or roofs should be used. AVOID THE OBVIOUS.

Searchers never open doors until both sides are cleared of boobytraps. Searchers use hand lines to open doors or cupboards, move furniture, or other tasks which may endanger safety. Leave all doors, drawers, and cupboards open after inspection. Clearly mark routes cleared of boobytraps with white tape. Once the house is cleared of boobytraps, the team leader assigns pairs of searchers to each room and continues to search as with an occupied house.

(b) Boobytraps. Boobytraps are concealed in unlikely places. Be wary of attractive items in the open; loose floorboards; window ledges; stair treads; fresh nails or screws; lumps or bulges under carpets or chairs; and dirt, wrappings, sawdust, pegs, wires, or cording in unlikely places. Boobytraps can be activated by more than one method. The most common methods of activation are—

- **Pulling** open a drawer.
- **Pressure** created by standing on a floorboard or sitting in a chair.
- **Release/antilift** created by picking up a book or bottle.
- **Tilting** an object on its side.
- **Trembling** vibration or movement.
- **Collapsing a circuit** in an electrically initiated device by cutting or breaking the circuit.
- **Light sensitive** device that functions when exposed to or blocked from light.
- **Antisubmerge** device placed in water.
- **Antiprobe** reacts to contact by search probe.

Forward descriptions of all boobytraps to adjacent and higher headquarters for dissemination. If time permits, indicate that the building has been cleared by marking the building or posting a sign with the date and time. Never consider a building free of boobytraps—even if it is marked.

d. Search Operation Orders. Obtain legal authorization before executing a search. Search operation orders follow the typical five-paragraph format with unique inclusions (see fig. 4-6).

e. Military Working Dog Teams. Military working dog (MWD) teams are valuable assets to security operations. There are four types of MWD teams used in security operations: explosives/patrol, drug/patrol, patrol, and scout.

Explosives/patrol and scout MWD teams search for previously fired AA&Es in buildings, vehicles, and open areas. Use explosives/patrol MWD teams to clear building of explosives. Report the presence of AA&Es to EOD. If EOD is not available and search teams must move on, either destroy the AA&E or post signs for follow-on patrols. Use patrol and scout MWD teams to detect and search for people. Patrol MWD teams attack on the handler's command. Scout and explosives/patrol MWD teams are trained for passive response. Contact military police for in-depth explanations of MWD team capabilities.

4203. Tactical Responses

a. Ambushes. Ambushes in combating terrorist operations are similar to ambushes in any other phase of war. Like patrolling, ambushes demand patience, skill, and outstanding warrior ability. Planned ambushes are primarily defensive measures.

(1) Urban Ambushes. Ambushes in urban security operations differ from their conventional counterparts in two ways. First, the aim is to arrest targeted individuals, not to kill them. Second, security is more difficult because of concentrated population.

1. Situation
   a. Ground. (Describe the area. Use maps and air photographs.)
   b. Enemy Forces. (Determine terrorist activity, reason for search, high- or low-risk area, type of search, and intelligence background.)
   c. Friendly Forces. (Determine troops involved, extent of task, and other required operations.)
   d. Attachments and Detachments. (Identify engineer teams, dogs, EOD, and others.)
2. Mission
3. Execution
   a. Concept of Operation
      (1) Description of the whole operation, including deployment of search teams and cordon troops in the area.
      (2) Description of cordon operations.
      (3) Description of search operation.
   b. The Cordon
      (1) Area to be cordoned (inner and outer cordons).
      (2) Vehicle pickup and dismount points (location, routes, timings).
      (3) Positions of individual cordon members.
      (4) Areas of observation/fire of each cordon member.
      (5) Time to be in position.
      (6) Vehicle assembly areas at search area.
      (7) Location of reaction forces, command and control element, supporting agencies, and search advisors.
   c. The Search
      (1) Aim and extent of search.
      (2) Composition of teams and allocation of attachments.
      (3) Order of priority of search tasks.
      (4) Exact task for each team.
      (5) Specialist tasks.
      (6) Damage (limitations must be given).
      (7) Assistance from police, female searchers, dogs, and EOD.
      (8) Guard/escort.
4. Administration and Logistics
   a. Ammunition and weapons.
   b. Messing.
   c. Uniform.
   d. Medical. (Identify casualty evacuation plan.)
   e. Special equipment to be taken.
5. Command and Signal
   a. Use and allocation of radios, including search net and command net.
   b. Call signs.
   c. Location of control point or search headquarters.
   d. Nicknames and codewords.
   e. Electronic countermeasures constraints.

Figure 4-6. Search Operation Orders.

It may not be possible to site an ambush in the most tactically sound position. The site is frequently dictated by the area or house frequented by targeted individuals. Information about the target's movement is essential. It is vital to know the movement patterns of local inhabitants and to have an intimate knowledge of the area (e.g., short cuts, gaps in walls and fences, sewer systems). Troops familiar with the area set ambushes.

Cover occupation of an ambush site by normal operations (e.g., house searches, roadblocks), flooding an area with patrols to disguise the actual occupation, and using civilian vehicles/clothes to establish the ambush party. An ambush can consist of one or more OPs used to watch for targeted individuals. Once spotted, OP personnel can react or call in prepositioned snatch parties. If the target is moving into or out of the area, deploy hasty roadblocks as a form of ambush or reinforce existing roadblocks to act as surprise snatch parties. Because of security problems, urban ambushes usually occur at night. The employment of night observation devices is essential to identify the target. Street lights cause a problem for night observation devices and it may be necessary to arrange for a blackout with the host nation or to eliminate as much artificial background light as possible.

(2) Causes for Failure. After analyzing almost 5,000 operational ambushes, failures resulted due to the following:

- Footprints in the vicinity of the ambush alerted the target.
- Lack of all-round observation allowed the target to out flank the ambush.
- Noise of cocking weapons or safety catches alerted the target.
- Poorly sited ambush lacked view of the area.
- Lack of clear orders for springing resulted in premature firing and allowed the target to escape.
- Lack of fire control led to ragged and ineffective engagement.
- Misfires and stoppages prevented full engagement by the ambush party.
- Tendency to shoot high in poor lighting.
- Several weapons engaged the same target and did not fully cover the target area.

(3) Ambush Orders. Ambush orders follow the standard 5-paragraph format with the execution paragraph containing the information emphasized in figure 4-7.

1. Situation
   a. Enemy Forces
   b. Friendly Forces
2. Mission
3. Execution
   a. Action at Place of Ambush.
      (1) Method of entry into ambush position.
      (2) Position in ambush.
      (3) Sectors of fire.
      (4) Signal for ambush.
      (5) Signals in general.
      (6) Time from_____to_____.
   b. Action at Approach of Enemy
      (1) Warning by sentry.
      (2) Signals to fire.
      (3) Illumination.
      (4) Cease firing signal.
      (5) Search party/follow up.
   c. Withdrawal
      (1) Signal to end ambush and move out.
      (2) Order of march.
      (3) Handling instructions for casualties and prisoners.
      (4) Rendezvous point.
4. Administration and Logistics
5. Command and Signal

Figure 4-7. Ambush Orders.

b. Riot Control. Crowd violence is 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 an event. Crowd violence may also be intramural which involves clashes within the crowd or from opposing forces. Crowd violence is characterized by excitement and violence; both are highly contagious. Riot control aims to restore order with minimum use of force. The general approach is to reduce or disrupt the crowd's unifying influences, and reorient the participants to concerns for personal vulnerability and welfare. FM 19-15, *Civil Disturbances*, and FMFM 6-4, *Marine Rifle Company/Platoon*, provide additional information.

Remember the principles of riot control using the term FRACASS.

F lexibility in changing tactics to meet the situation.

R ehearsals ensure success.

A ppearance of being able to do damage is often more effective then having to resort to force.

C ontrol by positioning Marines and presenting the image of having and maintaining full control even if the situation deteriorates.

A ll-round defense of assigned sectors of observation and fire. Able to observe and fire 360 degrees around control force.

S peed in deployment, arrest, and reaction to change.

S urprise keeps the crowd off balance.

Disrupt rioters by threat of force, arrest of leaders, and breaking the mob into smaller groups. Make it clear that further rioting will result in physical discomfort to lawbreakers. Always leave an escape route open to allow rioters to disperse. Use the following procedures in ascending order to disperse rioters.

(1) Talk. Have police officers try to talk down the situation with group's leaders. Keep troops in riot gear out of sight.

(2) Deploy. If talking fails, move riot troops quickly into position. The sudden sight of well-disciplined, armed troops often affects a crowd's resolve, causing hesitation and sometimes dispersal.

(3) Give Warning. Instruct the crowd to disperse, that no further unlawful behavior will be tolerated, that force will be used as necessary if the area is not cleared at once, and that those remaining will be liable to arrest.

(4) Take Pictures. Use TV and photographic cameras to collect a pictorial record of the group, especially leaders. This can be used for prosecution evidence and tends to remind participants that they can be individually identified and prosecuted, thereby reducing resolve.

(5) Advance. Advance guard troops, in riot gear, advance in formation (e.g., skirmish line, wedge, echelon right/left). Advance guard troops drive the crowd into specific areas. Wherever possible, drive the crowd against obstacles (e.g., roadblocks) and force the crowd to split. Troop formation divides in accordance with the crowd and again drives the crowd against obstacles until the crowd loses cohesion and disperses. Supporting units follow in column behind the advance guard to support the advance and to pick up independent advanced guard duties as the crowd splits. Advancing forces employ riot batons, fixed bayonets, riot control agents, and water hoses (dyed water) as appropriate. Equip vehicles (LAVs, trucks) with people pushers (wood platforms or concertina rolls affixed to vehicle front). Unit commanders employ snipers in life-threatening situations and in accordance with ROE. Intramural situations are handled by interposing troops (advancing from side streets) advancing against both factions.

(6) Make Arrests. Make arrests in conjunction with the advance. Snatch squads follow the advancing line and pull people for arrest swiftly and efficiently. Snatch squads contain at least four men: a leader, two snatchers, and a cover man. Snatch squads are lightly equipped and armed only with a riot baton. They must not be drawn too far into a crowd.

(7) Dominate the Area. Once the crowd begins to disperse, deploy troops to dominate the area. The goal is to allow rioters escape routes while preventing rioting in other areas.

(8) Withdraw and Return Control to Civil Authorities. Once the crowd has dispersed and all is quiet, troops return to the assembly area and control is returned to local police.

c. Urban Shootings. A shooting can be a single sniper, several weapons from one firing point, or a series of shots from several firing points. A single sniper can entice security forces into a larger ambush. When entering an area under fire, anticipate your reaction and be prepared to kill or capture the assailant.

The immediate reaction when coming under fire is to fire at and suppress the assailant or his suspected position. Report where you are, location where you came under fire, and whether or not there are casualties. Move directly towards the firing point or locate it if not already seen. Use caution in approaching firing points, ambushes, mines, and boobytraps may be in place. Maneuver other units to cut off likely escape routes. Quickly estimate the civilian situation on-scene. Send a full contact report containing time of the incident, exact location with grid reference, actions taken, and assistance needed. Once the initial situation is contained and reinforcements arrive, begin a deliberate follow up. A deliberate follow up involves—

- Selecting a new incident control point, if required.
- Establishing roadblocks on likely escape routes.
- Deploying a cordon if necessary.
- Searching suspicious houses within 1 hour of the incident (coordinate with local authorities).
- Questioning local inhabitants.
- Cordoning firing point to protect evidence.
- Employing support from MWD teams and local authorities in order to search the scene, collect evidence, and search caches.
- Analyzing evidence.
- Supervising the handling of weapons or caches discovered during follow up. Leave the weapons and caches undisturbed. Mount an OP to observe or task EOD or police to clear and collect evidence.

d. 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 entering a bomb site, proceed with extreme caution and contact the EOD team immediately. Appendix O contains additional explosives device procedures. The EOD team will need the following information:

- Where is the bomb?
- What does it look like?
- When was it placed?
- What warning was given?
- Are witnesses available?
- Are any suspects available for questioning?
- Who is securing the area?
- Are there any hostile crowds or sniping?

The following is a list of do's and don'ts when discovering an unexploded bomb or when arriving at the scene of a bombing incident.

DO

- Establish a control point.
- Establish coordination with civil authorities.
- Clear the area of people for at least 200 yards from the bomb.
- Divert traffic away from the scene.
- Assemble witnesses, suspects, and house owners at the control point.
- Send for an EOD team.
- Alert firefighters and emergency medical teams, as required.
- Obtain as much information as possible.
- Secure the area against snipers.
- Dominate possible firing points.
- Use one man to approach or check suspicious areas or objects.
- Follow EOD commander instructions upon arrival.
- Treat the press with tact, but keep them from the scene during the search and disarming.

DON'T

- Touch or approach a bomb.
- Assume that one explosion means the area is safe.
- Permit anyone to approach the bomb except authorized EOD personnel.
- Allow the press or anyone else to hurry the EOD team.
- Reveal the names of the EOD team or permit photographs of the team.
- Disclose the construction of the bomb.
- Reveal any reasons for the bomb's failure.
- Identify techniques used to disarm the bomb.

Chapter 5

Crisis Management Planning

Combating terrorism programs are keyed to the preventive and defensive measures outlined in chapters 3 and 4. These measures provide security and prevent terrorist incidents. However, a dedicated enemy might still mount an operation after comparing potential gain to possible risk. Installations must prepare to provide immediate initial response to a terrorist situation and manage the resources required to counter a prolonged terrorist situation. This chapter outlines terrorist crisis management planning procedures.

5001. Incident Response Phases

Incident response is predicated on terrorist activity, availability and ability of civilian law enforcement agencies and military forces, and location of incident (CONUS or OCONUS). Incident response is divided into phases I, II, and III. Phases II and III require identification of reactive capability. Reactive capability is identified by types A, B, C, or D. When occurring OCONUS, types B, C, and D require guidance from the NCA and involve one or more United States military Services. Regardless of the nature of the incident and the available reaction force, tailor the use of force to the situation.

a. CONUS. Figure 5-1 illustrates CONUS incident response.

(1) Phase I. Phase I involves immediate response to a terrorist situation. Military police or interior guard provide the initial response. Initial responders determine the type of incident, resolve or contain the incident if possible, and gather intelligence. If the incident appears to be terrorist-related, notify the installation/unit commander as soon possible.

(2) Phase II. Phase II manages resources required to counter a prolonged terrorist situation. The commander activates the CMT and CMF. If the incident is terrorist-related, notify the FBI, service command center, and higher headquarters. The FBI has primary jurisdiction for domestic terrorism and either assumes or declines jurisdiction based on federal interest. The military supports the FBI under current DOD and DOJ MOUs. Installation personnel remain under direct control of the military. If the FBI does not assume jurisdiction and the incident is beyond the installation's ability, installation commander's may request additional military forces through appropriate Service channels.

(3) Phase III. Phase III continues to manage resources required to counter a prolonged terrorist situation. The NCA intercedes if the FBI or installation cannot resolve the terrorist incident. The NCA provides specially-trained civilian and military forces to resolve the incident. If the FBI assumes initial jurisdiction, submit requests for assistance from the NCA through DOJ under current DOD and DOJ MOUs. If the NCA commits military forces, the Secretary of Defense directs military operations according to law enforcement policies determined by the Attorney General.

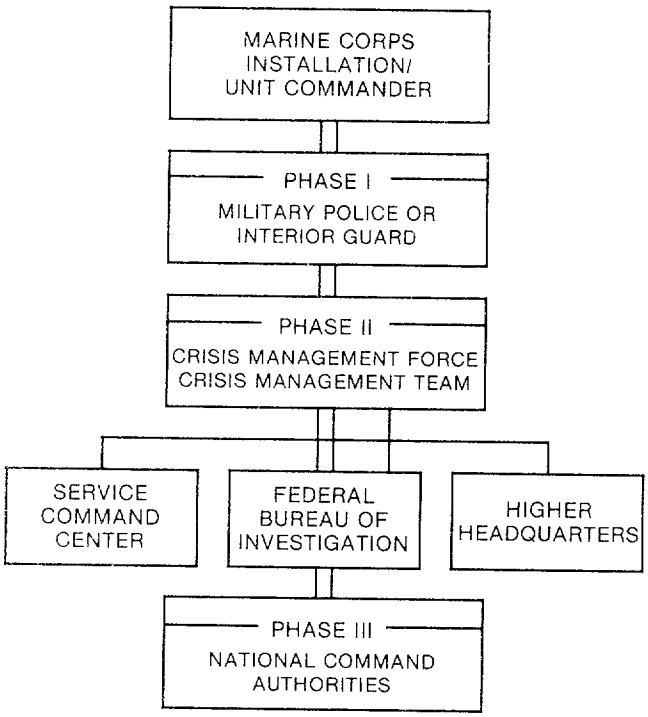


Figure 5-1. CONUS Incident Response Phases.

b. OCONUS. Figure 5-2 illustrates OCONUS incident response.

(1) Phase I. OCONUS phase I response is basically the same as CONUS phase I response found in paragraph 5001a(1). Notify the host nation under applicable status-of-forces agreements and Marine Corps regulations.

(2) Phase II. Phase II begins when United States forces from outside the installation or host nation forces respond to the incident. The host nation either assumes or declines jurisdiction based on status-of-forces agreements. Obtain host nation consent before committing follow-on United States forces. Status-of-forces agreements provide guidelines for interaction between United States and host nation forces.

(3) Phase III. Phase III begins when the host nation or NCA commits specially-trained forces. Obtain permission before committing United States forces. Status-of-forces agreements provide guidelines for interaction between United States and host nation forces.

c. Reactive Capability. Within the current United States force structure, a variety of terrorist operational reactive capabilities exist. Reactive capabilities within an individual unit or installation determine the initial reaction. Reactive ability can be limited to the reaction force of the commander's interior guard, the reaction force assets located within a tenant unit, or the installation's CMF capabilities. Depending upon the scope and nature of the incident, operations may involve the employment of general purpose forces in certain areas of special operations. Determine need for this form of employment in phase II or III response operations.

(1) Type A. Type A incidents require a reactive force trained in specialized operations. These forces require expertise and skill; e.g., hostage rescues. National forces are available from the United States military. Civil forces are drawn from the FBI's Hostage Rescue Team and Special Weapons and Tactics Teams (SWAT) organized by local police departments.

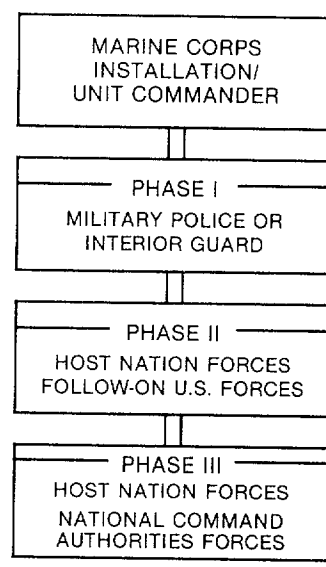


Figure 5-2. OCONUS Incident Response Phases.

(2) Type B. Type B is similar in nature to type A except the required force is larger and trained in raid operations. The reactive force conducts forced entry, seals off the objective area, and conducts assaults. Overseas missions can require task organization of type A forces into a Marine expeditionary unit (MEU) or utilization of a Marine expeditionary unit (special operations capable (MEU[SOC]).

(3) Type C. Type C incidents require a coordinated combined arms raid capability. This response inflicts damage against strongholds or training areas. Sea-based MEUs can be used for these operations.

(4) Type D. Type D incidents require aviation strikes or naval gunfire bombardment. This response inflicts damage against terrorist facilities. The Marine Corps air/naval gunfire liaison company (ANGLICO) provides terminal guidance for air or naval gunfire bombardment from ground or airborne platforms.

5002. Crisis Management Team

The CMT plans, coordinates, and controls procedures, techniques, and policies during heightened THREATCONs, special threats, acts of terrorism, and disruptions on government installations. The team is pre-established at installations in high-risk areas. The CMT considers local, national, and international implications of a major disruption. The CMT establishes contact with the MCCC. At installation level, establish the CMT at or in proximity to the operations center. The CMT location becomes the command and control center during an incident.

a. Specific Duties. The CMT's purpose is to—

- Resolve the incident without casualties, if possible.
- Influence and manage information flowing between military and civilian law enforcement and intelligence agencies.
- Resolve the incident without additional reinforcements.
- Manage multiple and diversionary incidents.
- Handle political, media, and public reactions.
- Receive, analyze, use, and disseminate intelligence and information at all levels of command and control.
- Provide timely intelligence and information to the installation commander and CMF.
- Manage rapidly shifting series of encounters including mobile incidents.
- Coordinate the duties of the interior guard.

b. Procedures. In CONUS, the installation commander/CMT leader and provost marshal work closely with the FBI. The CMT coordinates with the local FBI office. At a minimum, invite the FBI Special Agent in Charge (SAC) to reconnoiter the installation. The FBI SAC should know key personnel, have an opportunity to review plans and discuss scenarios, and know the location of the operations center and CMT. The installation commander and FBI SAC clarify responsibility and jurisdiction.

OCONUS, status-of-forces agreements establish authority and jurisdiction of on-post terrorist incidents. The civil affairs officer and/or staff judge advocate determines authority and jurisdiction and assists in the preparation of an MOU if required. DOS and host nation representatives agree upon any decisions.

Typically, the senior officer of the CMT is the installation commander or appointed representative. Representatives are specialists and advise and support the CMT commander and CMF. The CMT representatives can include:

- S-1/G-1/personnel.
- S-2/G-2/intelligence.
- S-3/G-3/operations.
- S-4/G-4/logistics.
- S-5/G-5/civil affairs.

- Special staff sections
  - PMO.
  - Staff judge advocate.
  - Public affairs.
  - Transportation.
  - Aviation.
  - Communications.
  - Engineers/utilities.
  - Medical activity/Red Cross.
  - Chaplain.
  - EOD section.
- Major tenant commands.
- Local NIS field office.
- Civilian authorities/representatives.
- State and local police.

Control the number of personnel physically located within the CMT. The CMT should not become too large to be effective. Use key people only. Staff agencies should consider sending a liaison to work with the CMT while key personnel remain at their duty stations. This procedure streamlines the management and operation of responsibilities and reduces the number of people within the CMT.

For example, the staff judge advocate keeps key personnel at the law office and sends a liaison to work with the CMT. This allows key personnel to research and discuss ideas in a calm environment. The liaison then transmits guidance to the CMT from the staff judge advocate.

Locate the CMT near or in the operations center. Maintain direct communications between the CMT and operations center during a crisis situation. Never place the CMT inside the outer perimeter established by the CMF. Remember, the CMT serves as a special staff element in support of the operations center. Locate the CMT in a room used for other duties. This room becomes the CMT facility only during exercises and actual incidents. Modify the room with phone jacks and outlets to allow quick conversion from office or conference rooms to the CMT.

5003. Crisis Management Force

The CMF contains or curtails terrorist incidents. The installation establishes and maintains the CMF. CMF elements provide adequate security during heightened terrorist THREATCONs. The billet of CMF commander is provisional in nature and typically occupied by the provost marshal. Activate the CMF during a terrorist threat, terrorist incident, or other crisis (e.g., natural disaster, civil disturbance).

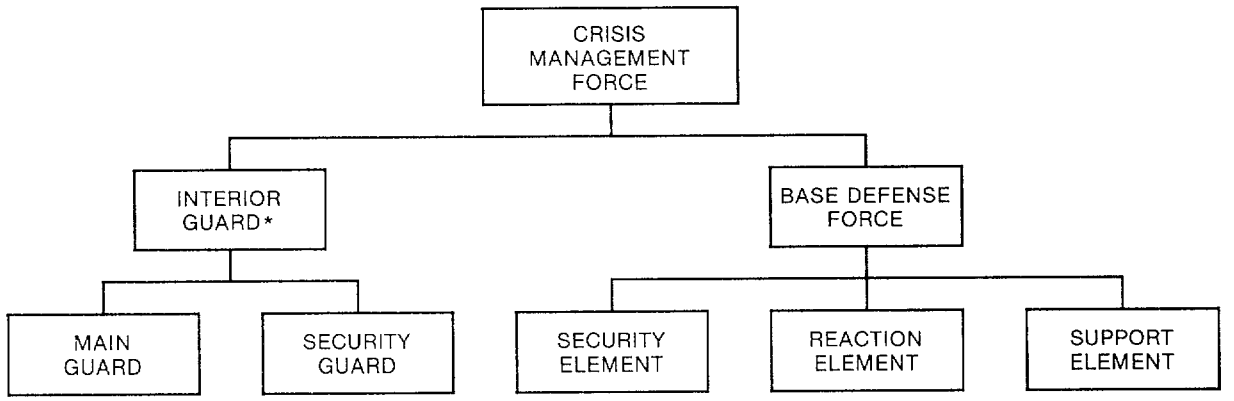
During heightened THREATCONs, all permanent security and safety elements on Marine Corps installations are organized into a single organization. The CMF includes military police, augmentation force (base personnel), fire department, EOD, medical, and other emergency services (e.g., transportation, communications) assets as needed. At a minimum, the CMF includes security, support, and reaction elements. Typically, the CMF is organized as depicted in figure 5-3. Organize and train the CMF as a team and evaluate its capabilities annually.

The relationship between the CMF and a tenant command's interior guard is coordination and reinforcement. Tenant command interior guards should not fall under the operational control of the CMF commander. The interior guard provides security for their command, including key assets and infrastructures. Additionally, they are capable of reacting to and containing an incident until the installation's reaction force assumes operational control.

a. Security Element

(1) Organization. The security element consists of military police and an augmentation force. The augmentation force consists of installation personnel trained in guard duties and attached to the security element. The augmentation force assists and expands the military police's operational capabilities.

(2) Mission and Responsibilities. The security element provides security to the installation, including key assets and infrastructures. The security element is responsible for initial response and containment of the incident.



*Coordinated through the CMT.

Figure 5-3. Typical Crisis Management Force.

b. Reaction Element. The installation establishes the reaction force. The reaction force responds to, contains, and resolves special threat situations. Typically, reaction forces cannot conduct hostage rescue operations involving multiple hostage-takers and hostages. The reaction force is organized, trained, and equipped to—

- Establish and maintain inner and outer perimeter cordons.
- Conduct limited hostage negotiations.
- Collect criminal intelligence concerning the terrorists.
- Collect evidence.
- Conduct limited assaults to free hostages.
- Use force to overcome the terrorist.

Commanders must be acutely aware of the capabilities and limitations of their reaction force. At a minimum, the reaction force includes headquarters, assault, operations, and negotiations and investigations elements (see fig. 5-4). The reaction force is organized mostly from military police assets. However, personnel from outside the PMO may be used (e.g., outer perimeter and support personnel). For this reason, periodic training is important to the reaction force's effectiveness.

(1) Headquarters Element

(a) Organization. The headquarters element consists of the reaction force commander, a recorder, and communication personnel as required. The CMF commander selects the reaction force commander.

(b) Mission and Responsibilities. The headquarters element's mission is the successful resolution of threat situations requiring deployment of the reaction force. The only exception is when the FBI or host nation assumes tactical control of the incident and the reaction force is supporting the tactical movement of those forces. Regardless of whether or not the reaction force commander has tactical control of the incident or is supporting another force, he operates the installation's on-scene command post and directs the actions of the reaction force's subordinate elements.

(2) Assault Element

(a) Organization. The assault element contains the special reaction team (SRT). The SRT reacts tactically to resolve hostage and barricade situations and combating terrorism

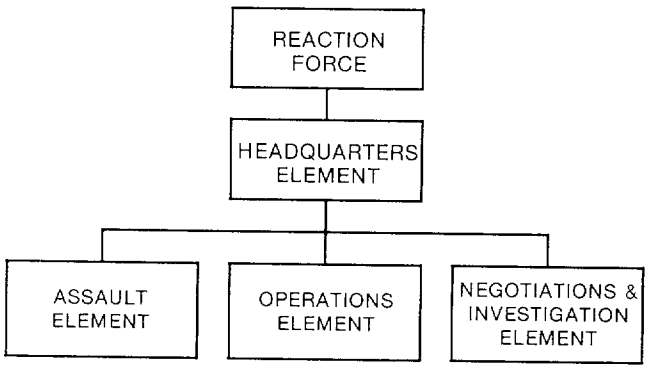


Figure 5-4. Reaction Force Organization.

operations. The CMF commander authorizes tactical use of the SRT. To be effective, the SRT trains together frequently. Training requirements include—

- Assault planning, preparation, and execution (e.g., intelligence gathering, blueprint reading, security).
- Terrorist tactics (e.g., history, psychology, methodology).
- Weapons and explosives (e.g, terrorist and SRT).
- Communications (e.g., audio and visual).
- Special tactics (e.g., air, water, ground).
- Special equipment (e.g., protective gear, ropes, vehicles).
- First aid.

Military police personnel comprise the SRT. The SRT includes an SRT commander and one or more five-man entry teams and four-man cover teams. All SRT members should have completed a formal SRT course. Smaller installations may elect to obtain such support from other federal/civilian agencies, military Services, state and local governments, or host nations. If exercising this option, establish a formal MOU and test the capabilities of forces in mock situations.

(b) Mission and Responsibilities. The assault element's mission is to respond tactically and successfully resolve special threat situations using minimum force. Situations include, but are not limited to, countersniper operations, barricade suspect operations, barricade captor/hostage operations, violent suspect apprehensions, and terrorist incidents. Terrorist incidents requiring SRT employment usually involve more than one of the operations mentioned. The installation commander exercises caution when employing an SRT. If the SRT's mission exceed its capabilities, request outside support using the forces identified in paragraph 5001.

(3) Operations Element

(a) Organization. The perimeter element consists of a commander, inner and outer cordon forces, and support personnel. Military police personnel comprise the inner and outer cordon forces. If the perimeter size becomes unmanageable, attach personnel from the augmentation force to provide support. Because the SRT cover team normally positions itself along the inner perimeter, maintain a strict chain of command. The SRT cover team normally reports to the SRT commander even if functioning as the inner cordon force. Support personnel include medical, transportation, communication, legal, and public affairs representatives as required by the on-scene commander.

(b) Mission and Responsibilities. The inner cordon force's mission is to contain the incident using the minimum force necessary. The outer cordon force's mission is to establish a cordon far enough from the incident to prevent injury to and observation by unauthorized personnel. The outer cordon force may also be responsible for evacuating personnel from areas within the outer cordon. Support personnel provide the on-scene commander with the required support.

(4) Negotiations and Investigations Element

(a) Organization. The negotiations and investigations element consists of the PMO investigations officer or staff noncommissioned officer (NCO), hostage negotiations team (HNT), and a command investigator from Criminal Investigation Division (CID). Organize the HNT using CID personnel trained at the U.S. Army Military Police School's hostage negotiations course and NIS agents trained as hostage negotiators. The local NIS SAC instructs NIS agents employed as negotiators to report to the on-scene commander through the investigations officer or staff NCO. Employ other personnel (e.g., psychiatrists, psychologists, bilingual translators) as required.

(b) Mission and Responsibilities. The negotiations and investigations element gathers intelligence and negotiates with the suspects. It is critical to open communications quickly and establish terrorist identities, personalities, motives, habits, and abilities. Information helps the negotiator relate to the terrorists on a personal level. If identities are unknown, check license plates in the vicinity. This can produce names of persons, terrorist or hostage, involved in the incident. Physical descriptions of the terrorists and other persons inside the barricade are important. The HNT receives information from interviews with initial response personnel, witnesses, escaped and released hostages, and captured terrorists. Use information obtained by the HNT for intelligence purposes. Make information readily available to the CMF commander.

Hostage negotiators attempt to resolve the situation through nonviolent means. Hostage negotiators attempt to gain the tactical advantage to gain the release or rescue of hostages and contribute to the apprehension of the terrorists. The CMF commander activates the HNT. Use only one negotiator at a time. Ideally, the HNT includes—

- Officer in charge.
- Primary hostage negotiator who has completed formal hostage negotiator training.
- Backup hostage negotiator who has completed formal hostage negotiator training.
- CID or NIS investigator.
- Counterintelligence agent knowledgeable in international terrorism.
- Bilingual translator, if required.
- Explosives expert (EOD or similarly qualified person).
- Mental health professional (e.g., psychiatrist, psychologist, or similarly qualified person).

The CMF commander selects team members who have the characteristics of successful negotiators. Characteristics of a successful negotiator are maturity, mental and emotional stability, listening ability, sincerity, articulate, flexibility, and physically fit. Negotiators are not decision makers. The negotiator establishes rapport with the terrorists. The negotiator is a neutral who must appear able to consider the interests of the terrorists and the interests of society equally. This permits the negotiator to defer decisions and maintain rapport while demands are delayed or refused. The psychological concept of transference (ability to identify and sympathize with each other) between hostage-taker and negotiator occurs frequently; therefore, change negotiators regularly. Negotiators strive to—

- Be a mediator, not an arbitrator.
- Allow terrorists to set the pace, mood, and topic of conversation.
- Listen to the terrorists' views and express neither approval nor disapproval.
- Maintain a dialogue with the terrorists.

c. Support Element

(1) Organization. The support element consists of base activities necessary to support overall security. At a minimum, the support element includes the fire department, EOD, medical, and other supporting activities as needed.

(2) Mission and Responsibilities. The support element provides combat support and combat service support to the CMF.

5004. Interior Guard

On a day-to-day basis, every installation/unit throughout the Marine Corps maintains a viable interior guard posture. The interior guard provides security for the command area, including key assets and infrastructures. Additionally, they can react to and contain an incident until the installation's reaction force assumes operational control. All interior guards (e.g., fire watches, duty NCO, watchstanders, sentries, patrols) are under one authority. When an installation/unit has more than one interior guard, a senior officer retains overall control. The relationship between the CMF and tenant command's interior guard is coordination and reinforcement. A tenant command interior guard should not fall under the CMF commander's operational control. At a minimum, interior guard procedures address—

- A daily guard mount and inspection of personnel.
- A guard school to train guard personnel.
- Off-duty watches centrally billeted and readily available.
- Roving patrols who vary their routes.
- Qualification and ability of personnel to carry assigned weapon.
- Physical inspection of every guard's relief.
- Availability of emergency backup communication procedures.

5005. Crisis Management Plan

a. Planning, Objectives, and Responsibilities. The crisis management plan is part of the installation's physical security plan. The crisis management plan includes responsive measures for various types of crisis situations and applies to all levels of command. The crisis management plan complements and supports the installation's disaster preparedness plan with regard to recovery procedures. The crisis management plan outlines specific duties and responsibilities of the installation's CMT and CMF. It provides notification procedures, establishes operational procedures, identifies members and alternates, and defines duties. Although most terrorist attacks against military installations are bombings, the installation must prepare to counter other terrorist threats. The crisis management plan and all collateral plans consider the worst possible scenario—a prolonged hostage/barricade situation. To assist in the development of a crisis management plan, see appendixes P and Q.

The operations officer should have primary responsibility for the development of the crisis management plan in coordination with the installation command staff. The crisis management plan is thoroughly reviewed by the installation command staff, PMO, and CMT members. Next, key personnel evaluate plans and procedures using basic scenarios to track potential problems. This simulation is an important step and can solve many problems without committing resources other than the planners. Crisis management plan implementation should complement normal operating procedures.

For example, the operations center is under the cognizance of the operations officer, remains under his control during a crisis management operation, and continues to function as the operations center.

b. Contingency Planning. Installations prepare contingency plans for various terrorist incidents. These contingency plans form part of the physical security plan (see app. C). These plans include

responses to bombings, ambush/attack, hijacking/skyjacking, kidnapping, hostage/barricade situation, and arson.

(1) Bombings. If terrorists plant one bomb, respond as if there are others. Alert the bomb search teams and EOD personnel. The initial response force removes everyone from the scene and into a safe area. Interview anyone near the scene at the time of the explosion. Keep in mind that one of the people being interviewed may be the terrorist who planted the bomb.

(2) Ambush/Attack. Always assume terrorists are still in the area. The initial response force gives aid to the victims and establishes a defensive perimeter. When reinforcements arrive, the initial response force clears the area of people before the investigation begins. Use available resources to clear the area, including aircraft.

(3) Hijacking/Skyjacking. The initial response force attempts to contain the situation and prevents terrorists from escaping. Once activated, the reaction force continues to contain the incident. The main objectives are to contain the situation, negotiate with the terrorists, or end the incident through successful assault. The reaction force can perform assaults on aircraft; however, it is best to allow a specialized team (e.g., FBI or host nation force) to make the assault. The reaction force makes the assault only if specialists are unavailable.

(4) Kidnapping. In most cases, knowledge of a kidnapping is not known until it has occurred and the terrorists have secured the victim. Immediately dispatch military police to patrol the area and provide protection for other possible targets, including members of the victim's family. Activate the CMT and contact the NIS. The CMT coordinates military support, makes reports to higher headquarters, develops news releases, and recommends possible courses of action. The NIS investigates the kidnapping. The reaction force is available if the victim or terrorists are located on the installation. At this point, the HNT assumes an active role and can be dedicated directly to the operations center.

(5) Hostage/Barricade Situation. The most difficult contingency is a prolonged hostage/barricade situation. Another agency or the host nation may assume jurisdiction for the incident. The installation continues inner and outer perimeter security missions, gate security missions, and similar security functions. The installation operations center, CMT, and CMF continue to function under the control of the installation commander even after transfer of jurisdiction.

Because of the sensitive nature of hostage situations, establish and follow a preplanned course of action until trained negotiators arrive at the scene. Every installation should develop its own hostage situation SOP. Within CONUS, coordinate hostage situation SOPs with the FBI. OCONUS, coordinate hostage situation SOPs with the U.S. Embassy's regional security officer. Any further coordination depends upon the regional security officer's recommendations.

(a) Hostage Intelligence. Hostage intelligence has two purposes. First, it helps police and combating terrorist forces ensure hostage safety. Second, it helps theorize what might happen inside a barricade before the siege ends. As well as knowing the number of hostages, their identities, and their descriptions, make every effort to obtain the following hostage information:

- Sex and age.
- Relationship to other hostages.
- Personality traits.
- Special training or skills.
- Degree to which they are being threatened.
- Susceptibility to hysteria or other adverse reactions to extreme excitement or stress.
- Health condition.

(b) Physical Surroundings. Hostage intelligence addresses the immediate space in which hostages are being held, structure

enclosing the space, and surrounding neighborhood or environment. Pinpoint and monitor the terrorist's and hostage's location. Limit activities in surrounding areas. Carefully study the design of the incident site (building, aircraft, or ship). If possible, obtain blueprints of the site (building, aircraft, or street layout) and use a similar structure for rehearsal. Locate and interview persons with intimate knowledge of the incident site. Consider every detail of the inside of the site. Pinpoint all entrances and exits. Determine the location of telephones and their numbers; the location of water, gas, and electrical connections; and if there are time devices on the premises (e.g., alarms, lights, sound systems, locks). Other considerations include:

- Do normal operations continue at other areas on the installation?
- Which assets should be committed to managing the incident?
- How will that affect other operations?

(c) Organization of Information. Intelligence information concerning terrorists has high priority. Perform an investigation to obtain information if necessary. CID and NIS agents under the direction of a senior agent could perform the investigation. A representative of the staff judge advocate can serve as advisor. The investigation compiles data during the incident and conducts post incident criminal investigation. Answers to the questions presented in figure 5-5 provide the CMT with pertinent information in order to identify and classify the terrorist.

(6) Arson. Incendiary devices are often used during an organized civil disturbance (e.g., throwing a fire bomb) or against a specific target. As with bombs, time-delay mechanisms allow escape from the area before the fire occurs. Boobytrapped buildings increase casualties among firefighters responding to the scene. Firefighters and military police must be aware of the potential for boobytraps and act accordingly (see app. O). Secure the area during fire suppression and inspection by bomb search teams and EOD personnel.

5006. Communication Requirements

Establishing and maintaining communications during a crisis is critical. The crisis management plan considers all communication requirements and necessary backup systems. Planning and testing communications during operational exercises prevent problems during an incident.

After activating the CMT, secure communications are needed to higher headquarters and among team members as quickly as possible. Maintain intelligence channels to provide a continuous flow of information. Communications equipment used by the negotiator should have a one-way, secure monitoring capability and be capable of hands-free use. Audio monitors with a recording capability should be available for use by other HNT members and officials.

Terrorists have access to radio communication frequencies and the ability to monitor transmissions. They may boobytrap an incident area with explosive devices set to detonate when keying a nearby radio to a known local frequency. Prepare the SRT and other operational units of the reaction force to use arm-and-hand signals when communicating within the incident perimeter.

The HNT must be able to communicate directly with the terrorists. The operations center and CMT monitor but do not interfere with these communications. Secure communication channels are preferred. It is important that the CMT control radio and telecommunication channels. This keeps the terrorists from coordinating activities with outside groups.

5007. Public Affairs

Public affairs officers assist in terrorist operations. When requested, the public affairs office acts as a point of contact and a single voice to the news media. If primary responsibility for coordinating media activities during a terrorist incident does not rest with another agency (e.g., FBI or DOS), the public affairs office assumes this function. Public affairs officers respect the jurisdiction and interests of United States agencies (e.g., DOJ and FBI) responsible for primary coordination of public affairs activities concerning domestic acts of terrorism. Appendix R provides additional guidance for public affairs personnel in the event a terrorist incident occurs.

Do the hostage-takers have criminal records? If so, a wealth of personal information may be derived from their records.

Do the terrorists possess special skills and knowledge?

Are the terrorists trained in explosives or sniper tactics?

Do the hostage-takers have any special affiliations?

Are the hostage-takers members of any religious sect or group which can dictate or influence some of their behavior?

What habits, deviations, or addictions do they have which could influence their behavior? This knowledge could be used to predict their actions and responses.

What are their immediate problems? Their need for transportation, medical care, food, water, and other basic concerns are negotiable.

If recognized as terrorists, what are their previous methods of operations? Do they shoot hostages?

Figure 5-5. Terrorist Classification Sheet.

(reverse blank)

Chapter 6

Crisis Management Employment

The final antiterrorism measure is employment of tactical measures by the installation's/unit's security forces to contain and counter terrorist incidents. Employing of the CMF justifies the extensive preparation, planning, and response measures required. This chapter presents a summary of the procedures presented in this book.

6001. Initial Response

Either on-duty military police patrols or the interior guard usually provide initial response to a terrorist attack. The initial response force is under the control of the on-scene senior officer or NCO who has assumed responsibility. Once the initial response force has responded to the incident, the installation commander activates required forces.

a. Initial Response Force. The initial response force immediately identifies and reports the nature of the situation, isolates the incident, and contains the situation until relieved by the reaction force commander. Initial response force actions are critical. It is vital that each security force has trained personnel who are aware of the threat and capable of reacting. The on-scene commander directs the initial response force. Upon activation of the initial response force, the senior Marine on duty notifies the installation commander.

If the attack is a bombing, ambush, assassination, or arson attempt, the terrorists may escape before patrols arrive. In these cases, the initial response force provides medical aid, seals off the crime scene, and secures other potential targets in case the initial attack was a diversionary tactic. If the event is a hostage/barricade situation, the initial response force seals off and isolates the incident scene. No one enters or leaves the incident scene. The intial response force records witnesses names and directs them to a safe location for debriefing.

b. Installation Commander. The installation commander, depending upon established procedures, activates the installation's CMT and CMF. In CONUS, report any terrorist incident to the MCCC and the FBI. OCONUS, report incidents to the appropriate military command operations center, DOS, host nation, and MCCC.

c. Crisis Management Team. The CMT assembles at or near the operations center. The operations center serves as the command post for the CMT. The CMT/installation commander maintains command over the CMT. The CMF arrives at the incident scene and the CMT commander, or other appointed authority, assumes responsibility for supervising the CMF.

Communications are critical to establishing the initial response and maintaining the situation. Establish communications between the CMF, higher headquarters, and tenant unit interior guards, if required. If possible, communications are in a secure mode. There are usually three communications circuits: command net (administrative matters, support, routine traffic), tactical net (operations), and intelligence net.

6002. Confirmation

Since jurisdiction depends on whether the crime is a terrorist incident, it is important to identify the

incident as quickly as possible. If the FBI or host nation assumes control, coordinate the passage of lines. Prepare to manage the entire event if the FBI or host nation does not assume control.

Always prepare for the worst possible contingency. If a bombing has occurred, assume there are other bombs. Activate bomb search teams and alert EOD personnel while securing sensitive areas. If a hostage/barricade situation is in progress, assume it will last at least 7 days and prepare to isolate and contain the area during the 7-day period. Coordinate with relief forces for replacement of CMT and CMF personnel.

6003. Use of Force Options

The CMT guides and recommends appropriate force options to the installation commander. Usually, the first option is immediate assault, but this is often not the preferred choice. Accurate intelligence may not be available and time is usually on the side of response forces. At some point assault may be necessary, but it is usually not required immediately.

The second option is to contain and stabilize the incident. This usually is the preferred approach in a hostage situation. Hostage negotiators help the commander manage the incident by buying time and providing information. Skilled negotiators know how to probe terrorist weaknesses and vulnerabilities. They also obtain information on the hostages. Negotiators can persuade terrorist elements to give up. Information obtained during the negotiation process is invaluable when exercising the third option.

The third option is a planned assault. Assign responsibility for this assault to the SRT or other terrorist-trained force. The element of surprise is usually more important than size. If exercising the third option, the preferred course of action is—

- Contain and stabilize the area of the incident until the CMF is in place.
- Negotiate with the terrorists to gather intelligence and secure time.
- Make a planned, well-rehearsed assault if it is decided that negotiations are futile or that hostages are in imminent danger.

History indicates the longer a hostage/barricade situation lasts, the greater the probability of retrieving the hostage safely. The more time and intelligence the negotiator can obtain, the more likely he is to effect a positive outcome. Experience shows there is an exception when hostages are hooded. Hoods prevent emotional bonds from developing between the hostage-takers and their hostages (Stockholm Syndrome—see FMFRP 7-14A, *The Individual's Guide for Understanding and Surviving Terrorism*). Hoods permit the terrorists to remain impersonal and increase the hostages chance of being killed. In this situation, the force option might neutralize the terrorists through controlled fire (snipers) or quick assault.

6004. Preparation

a. Multiple Incidents. Terrorists often execute several incidents in quick succession. This increases casualties and reduces public confidence in security forces.

For example, bombs are planted with different delay mechanisms so secondary devices explode when the initial response force arrives.

The initial response force must be aware of this tactic and alert to the possibility of secondary devices. The initial response force secures the scene and evacuates casualties. They restrict all other activities until EOD personnel clear the area.

Initial attacks are often diversionary tactics. The crisis management plan addresses securing sensitive areas and high-risk personnel, regardless of where the initial incident occurs. While this decreases the number of persons available at the incident scene, its main objective is to keep the terrorists from accomplishing their goal.

b. Prolonged Incident. Never assume that the incident will be resolved quickly, especially if it involves a hostage/barricade situation. Give special consideration to the normal operation of other activities on the installation during the incident. Replacements for CMT and CMF members must be available.

6005. Response

Military personnel respond to a terrorist incident in three phases. Resources are used continuously and overlap from one phase to another.

a. Phase I. Phase I commits available local resources. This includes the regular military police patrol and any available backup units. Ideally, every military police shift includes at least two persons trained in terrorist operations. These forces secure and contain the scene until phase II.

> **NOTE:** Two-thirds of all terrorist incidents use bombs. Response forces should be alert to this fact while securing and containing the incident scene.

b. Phase II. Phase II enhances the initial response force with CMF, CMT, FBI, or host nation tactical units. This phase begins when the installation commander is notified and the CMT is activated. The FBI or host nation assumes control during this phase. If the FBI or host nation assumes control, the installation CMF provides support. Within CONUS, the FBI has discretionary authority to assume jurisdiction. OCONUS, the host country usually has that authority.

c. Phase III. Phase III commits DOD or host nation combating terrorism forces. This phase involves ending the incident. Incident termination may be the result of successful negotiations, assault, or other actions, including the surrender of the terrorists. Of course, the terrorists may decide to exercise the extreme option of killing their hostages and committing suicide.

6006. Typical Response to a Terrorist Incident

A terrorist hostage/barricade incident on a Marine Corps installation in CONUS might evolve as follows: (See fig. 6-1.)

- Installation commander activates the CMT and CMF.
- CMF musters at a designated assembly area and deploys on order.
- Installation operations center activated.
- Mission-essential personnel arrive at appointed locations.
- CMF contains the incident and reports intelligence from the incident scene.
- FBI notified. FBI forwards SAC to the incident.
- Incident jurisdiction established (see app. A).
- FBI SAC assumes jurisdiction after consulting with the Attorney General. In the event the FBI declines jurisdiction, the military commander takes the necessary steps to resolve the incident.
- FBI SAC establishes a joint command center with the military commander.
- FBI SAC, coordinating with the military commander and FBI headquarters, determines FBI assets needed to resolve the situation.
- FBI combating terrorism assets arrive at assembly area.
- FBI SAC directs agents to the incident scene to reconnoiter and validate intelligence provided by the military.
- FBI SAC determines force options based on circumstances.
- Military personnel provide inner and outer perimeter cordons and other support as requested. Military personnel remain under the command of the installation commander while supporting the FBI.
- FBI SAC determines if the incident requires additional force and advises the Attorney General.
- Attorney General coordinates use of additional forces from available military and national resources.
- Appropriate actions continue until the terrorist incident is resolved.

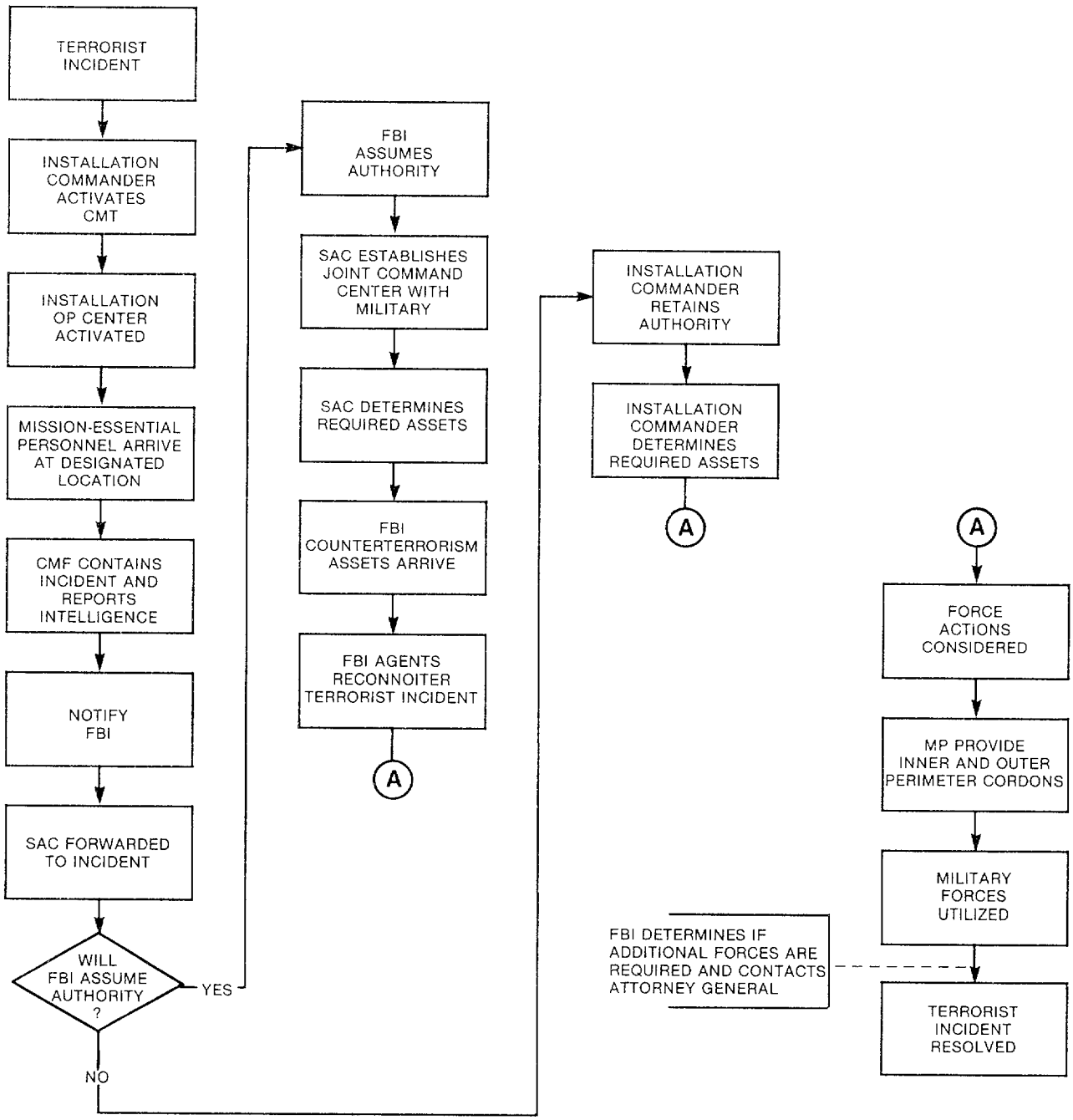


Figure 6-1. Response to a Terrorist Incident.

6007. Identify Inconsistencies

Information and intelligence gathering begin as soon as the initial response forces arrive at the scene. Report inconsistencies in the physical situation and terrorist's demands and claims to the CMT commander. These include inconsistencies in reports made by witnesses and hostages who escape or are released.

For example, criminal hostage-takers claim to be political activists because they believe their demands will be more readily accepted. If they claim to be politically oriented and their demands are monetary their motive is more criminal than political.

Crusaders conduct suicide missions—criminals do not. Knowing the adversary is a criminal rather than a crusader influences strategy. Criminals usually surrender after a period of negotiations. If the perpetrators are crusaders, the SRT assault option may be needed.

6008. Establish Communications

One of the most important aspects of implementing the crisis management plan is establishing secure communications among the incident area forces, CMT, and CMF. Once forces are established, activate all other elements of the communication plan. Communication personnel must be able to respond to changing needs and to maintain communication channels identified in the crisis management plan. Assuming a 7-day scenario, plan backup communications for all channels.

6009. Obtain Evidence

Although the foremost goal is ending a terrorist incident without injury, another goal is the successful prosecution of terrorists. Witness testimony, photographic evidence, etc., play an important part in achieving successful prosecution. Maintain the chain of evidence during an incident. To maintain the chain of evidence, document 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. Establish and maintain the chain by recording who initially took custody of the evidence (e.g., who took the photograph or picked up the weapon); immediately tagging the evidence with data on who found it, exact time, and exact date; and recording disposition of the evidence (e.g., to who, what, were, and why it was given). Types of evidence for which the chain must be established include—

- Photographs taken during the incident.
- Physical evidence, including AA&E parts used by terrorists.
- Tape recordings of conversations between terrorists and hostage negotiators.
- Reports prepared by military police initially responding to the scene.
- Eyewitness testimony.
- Demand notes or other written messages prepared by the terrorists.

The CMF commander begins the chain of custody for evidence collected in the incident area. This responsibility may be delegated to an NIS agent. The CMT commander is responsible for evidence collected and forwarded to the CMT. The evidence may be collected by, or turned over to, the FBI or appropriate host nation agency. Regardless of who maintains operational responsibility, document the incident and establish and maintain the chain of custody for evidence. This is critical if successful prosecution is to occur.

6010. Disposition of Apprehended Personnel

Handle apprehended United States military personnel according to current Marine Corps regulations and installation SOP. Release civilian detainees to the FBI or United States federal marshals. OCONUS, process civilian detainees under current status-of-forces agreement.

6011. After-Action Report

The CMT commander ensures that required reports are submitted during and after a terrorist incident. Situation monitoring does not end until the incident is terminated and all after-action reports are completed. Commanders are encouraged to submit a "lessons learned" analysis to MCCDC, MAGTF Warfighting Center, Quantico, Va. This analysis summarizes the incident, responses by military personnel, and positive and negative lessons learned.

Appendix A

United States Policy and Legal Considerations

The United States has made clear its policy regarding terrorism. That policy is as follows:

- All terrorist actions are criminal and intolerable, whatever their motivation, and should be condemned.
- All lawful measures to prevent such acts and to bring to justice those who commit them will be taken.
- No concessions to terrorist blackmail will be made, because to do so will merely invite further demands.
- When Americans are abducted overseas, the United States will look to the host government to exercise its responsibility under international law to protect all persons within its territories, including the safe release of hostages.
- Close and continuous contact with host governments will be maintained during an incident. Intelligence and technical support will be offered to the extent practicable but advice will not be offered on how to respond to specific terrorist demands.
- International cooperation to combat terrorism remains a fundamental aspect of U.S. policy, since all governments, regardless of structure or philosophy, are vulnerable; and all avenues to strengthen such cooperation will be pursued.

At the national level, the Department of State is the lead agency for response to terrorist incidents which take place outside the United States. The Department of Justice is the lead agency for domestic terrorism, with the exception of acts which threaten the safety of persons aboard aircraft in flight or which involve nuclear weapons. These are the responsibilities of the Federal Aviation Administration and the Nuclear Regulatory Commission, respectively. All Federal agencies which have resources for responding to terrorism are linked together through agency command centers and crises management groups to ensure effective coordination of the U.S. response.

1. General Considerations Affecting the Military Response to Acts of Terrorism

Restrictions on the use of military personnel in the United States or its possessions is contained in the Posse Comitatus Act (Title 18 U.S. Code, Seciton 1385). It does not apply in foreign countries nor to actions aboard military bases or in military contracted buildings or spaces, or in guarding military property in transit. Outside the United States, the host country has primary authority as set forth in the applicable Status-of-Forces Agreement (SOFA).

The act has been interpreted as a general prohibition against the use of the uniform services of the Department of Defense, either as part of a Posse Comitatus or in a military role other than provided by statute, to assist local law enforcement officers in carrying out their duties. The same prohibition runs against the use of troops to execute federal laws. See Vol. 41 Op. Atty. Gen. p. 330 (1957); Vol. 16 Op. Atty. Gen. p. 162 (1878). The purpose of this restrictive legislation was to restore congressional control over the manner and circumstances under which military power could be used in domestic affairs; however, there are certain exceptions to this prohibition, as explained below:

a. Constitutional. The constitutional authority which applies to these exceptions is based upon the inherent legal right of the United States Government to ensure the preservation of public order and continued governmental functioning within its territorial limits, by force if necessary. These exceptions include:

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

(2) Protection of Federal Property and Functions. This authorizes federal actions, including use of military forces, to protect federal property and functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection. See DOD Directive 3025.12, par. V.C., 19 August 1971, as amended.

b. Statutory. Congress, pursuant to its constitutional authority, has provided a broad range of legislation authorizing the President to use regular and federalized forces to execute the laws. To illustrate, the President is currently empowered to use military forces:

(1) To Restore and Maintain Public Order

(a) To respond to requests for aid from state governments (Title 10, U.S. Code, Section 332). Whenever the President considers that unlawful obstructions, combinations, assemblages, or rebellion against the authority of the United States make it impracticable to enforce the laws in a state or territory by the ordinary course of judicial proceedings, he may utilize federal armed forces as he deems necessary to enforce those laws, or to suppress the rebellion under the statute.

(b) To protect the constitutional rights under certain conditions (Title 10, U.S. Code, Seciton 333). The Fourteenth Amendment to the Constitution forbids any state to deny equal protection of the laws to any person within its jurisdiction. Congress has implemented this provision by providing that whenever insurrection, civil violence, unlawful combinations, or conspiracies in any state so oppose, obstruct, or hinder the execution of the laws of the state, and any of the United States, as to deprive any of the population of that state of rights, privileges, and immunities named in the Constitution and secured by laws, and the authorities of that state are unable, fail, or refuse to provide such protection, it will be deemed a denial by that state of the equal protection of the laws. Thereupon it becomes the duty of the President to take such measures, by intervention with federal armed forces, or by other means, as he deems necessary, to suppress such disturbances. Whenever the President considers it necessary to use a national guard or federal armed forces under the authority of the intervention statutes discussed above, he must immediately issue a proclamation ordering the insurgents to disperse and retire peaceably to their abodes within a limited time (Title 10, U.S. Code, Section 334). If the proclamation is not obeyed, an executive order is then issued directing the Secretary of Defense to employ federal military forces

as are necessary to restore law and order. See DOD Directive 3025.12, par. V.C.2a, 19 August 1971, as amended.

(c) To protect federal property and functions (Title 18, U.S. Code Section 231 and 1361 and Title 50, U.S. Code, Section 797). The latter prohibits participation in civil disorders affecting commerce or federal functions.

(2) To Meet Specified Contingencies

(a) To assist the U.S. Secret Service in protection of the President, Vice President, major political candidates, and foreign dignitaries (HR Res 1292; Title 18, U.S. Code, Section 3056).

(b) To assist federal magistrates in carrying out magisterial orders relating to civil rights violations (Title 42, U.S. Code, Section 1989).

(c) To assist the Attorney General in the enforcement of drug abuse prevention and control (Title 21, U.S. Code, Section 873[b]).

(d) To assist the administrator of the Environmental Protection Agency in water pollution control functions (Title 33, U.S. Code, Section 1362).

(e) To assist the FBI in investigations of congressional assassination, kidnapping, and assault (Title 18, U.S. Code, Section 351[g]).

(3) To Cope with Domestic Emergencies and to Protect Public Safety

(a) By furnishing aid to civilians in time of natural disasters (Title 42, U.S. Code, Section 4401-84).

(b) By rendering humanitarian or emergency assistance in case of national disasters (Title 42, U.S. Code, Section 1855).

(c) Emergency Rule: When the calamity or extreme emergency render waiting for instructions from the proper military department dangerous, a commander may take whatever action the circumstances reasonably justify. However, he must comply with the following:

- Report the military response to higher headquarters.
- Document all the facts and surrounding circumstances to meet any subsequent challenge of impropriety.
- Retain military response under the military chain of command.
- Limit military involvement to the minimum demanded by necessity.
- Emergency situations include, but are not limited to, the following:
  - •• Providing civilian or mixed civilian/military fire fighting assistance where base fire departments have mutual aid agreements with nearby civilian communities.
  - •• Providing emergency explosive ordinance disposal service.
  - •• Using working dog teams in an emergency to aid in locating lost persons (humanitarian acts) or explosive devices (domestic emergencies).
  - •• Emergency use of military aircraft in air piracy or aircraft hijacking cases may be authorized by the National Military Command Center (NMCC) (Deputy SecDef Memo, Subject: Support of Civil Authorities in Airplane Hijacking Emergencies, 29 June 72). Military aircraft may be committed for use as chase planes. Use of military personnel to apprehend skyjacking and the use of any type of military aircraft as platforms for weapons against suspected skyjackers are prohibited by the above cited memorandum.

2. Jurisdiction/Authority for Handling Terrorists Incidents

There are several federal criminal statutes that may apply to terrorist activities. Some deal with conduct which is peculiarly terroristic, while others prescribe conduct which is only criminal, but in which the terrorist may engage to accomplish his purposes. The federal law contains no special prohibition against terrorist acts or threats, as do some state codes. The Federal Government has investigative and prosecutorial jurisdiction over a wide range of criminal acts. Once the violation of federal law triggers jurisdictional authority, the investigative and law enforcement resources of the FBI and other federal enforcement agencies become available, and prosecution for the offense may proceed through the office of the United States Attorney. Many of these acts are also violations of state law. Depending upon the particular circumstances of the case, a terrorist incident could involve either the violation of state criminal laws or the violation of federal criminal laws. Violation of state criminal law invokes the police power of the state; violation of the federal law, the federal law enforcement authority. More commonly, however, a terrorist incident will involve violation of both state and federal criminal law, creating concurrent jurisdiction between state and federal authorities over the offense. In this situation, both state and federal enforcement authorities have power under their respective criminal codes to investigate the offense and to institute criminal proceedings. Whether concurrent jurisdiction arises can only be determined on a case-by-case basis. Two relevant factors regarding law enforcement responsibility for a given incident are:

- The capability and willingness of state or federal authorities to act.
- The importance of the state or federal interest sought to be protected under the criminal statute.

If concurrent jurisdiction is present, the Federal Government can either act or defer to state jurisdiction, depending on the nature of the incident and the capabilities of local authorities. Even where state jurisdiction prevails, the Federal Government can provide law enforcement assistance and support to local authorities on request. The choice between federal or state action is made by the prosecuting authority. However, successive prosecutions are possible, even where federal and state law prescribe essentially the same offense, without contravening the Fifth Amendment prohibition against double jeopardy. Obviously, if an incident occurs on a federal enclave (which would include most Marine Corps Bases or installations), the Federal Government would have exclusive jurisdiction for prosecution. However, Marine and/or naval installations may provide, under certain agreements, for state jurisdiction as well. In those cases an evaluation must be made as to which jurisdiction is appropriate.

a. State Responses to Terrorism. All states have developed response capabilities to combat terrorism. However, a discussion of those capabilities are beyond the scope of this Appendix. State requests for military assistance to respond to terrorist acts are discussed in paragraph 3.

b. Federal Agency Programs that Provide Antiterrorism Assistance. The primary federal organizations dealing with terrorism management are the Department of State's Committee to Combat Acts of Terrorism, the National Security Council (NSC), and the Department of Justice. The Committee to Combat Acts of Terrorism was reorganized in 1977 to coordinate, through its working group executive committee, the activities of 31 federal organizations. This group focuses primarily on the protection of foreign diplomatic personnel in the United States and American officials working and traveling abroad. The 31 member agencies, including the Department of Defense, may provide assistance in the form of terrorist incident information, technical assistance about security precautions, public information, and participation in education seminars. In addition to the above, major organizations with jurisdictional authority to combat terrorism include:

(1) Department of Justice. The Department of Justice is responsible for overseeing the federal response to acts of domestic terrorism. The Attorney General of the United States, through

an appointed Deputy Attorney General, makes major policy decisions and legal judgments related to each terrorist incident as it occurs.

(2) Federal Bureau of Investigation. The FBI has been designated as the primary operational agency for the management of terrorist incidents. When one occurs, the first reaction is generally from the special agent in charge of the incident area. The Special Agent in Charge is under the supervision of the Director of the FBI. The FBI maintains a liaison with each governor's office and renews it with each change of administration. There is a Special Agent in Charge of 59 field offices throughout the United States. Due to the presence of concurrent jurisdiction in many cases, the FBI cooperates with state and local law enforcement authorities on a continuing basis. In accordance with the Atomic Energy Act of 1954, the FBI is the agency responsible for investigating a threat made involving the misuse of a nuclear weapon, special nuclear materials, or dangerous radioactive material. In this effort, they cooperate with the Departments of Energy and Defense, the Nuclear Regulatory Commission, and the Environmental Protection Agency, as well as several states which have established nuclear threat emergency response plans.

(3) Department of Defense. In accordance with a DOD, DOJ, and FBI Memorandum of Understanding (5 Aug 83) (see app. B), all military preparations and operations, including the employment of military forces at the scene of a terrorist incident, will be the primary responsibility of the Secretary of Defense. In discharging these functions, he will observe such law enforcement policies as the Attorney General may determine. The responsibilities of the Department of Defense will be carried out principally through the Department of the Army, inasmuch as the Secretary of the Army is assigned primary responsibility for such matters as DOD Executive Agent. However, the Attorney General through the FBI will remain responsible; (1) for coordinating the activities of all federal agencies assisting in the resolution of the incident and in the administration of justice in the affected area, and (2) for coordinating these activities with those state and local agencies similarly engaged.

Upon notification of a Presidential approval to use military force, the Attorney General will advise the Director of the FBI who will notify the Special Agent in Charge (SAC), and the Secretary of Defense will advise the military commander. The military commander and the SAC will coordinate the transfer of operational control to the military commander. Responsibility for the tactical phase of the operation is transferred to military authority when the SAC relinquishes command and control of such operation and it is accepted by the on-site military commander. However, the SAC may revoke the military commitment at any time prior to the assault phase if he determines that military intervention is no longer required, provided that the military commander agrees that a withdrawal can be accomplished without seriously endangering the safety of military personnel or others involved in the operation. When the military commander determines that he has completed the assault phase of the operation, command and control will be promptly returned to the SAC.

The respective roles of the Defense Department, Justice Department, and the FBI with respect to a terrorist incident on a military reservation are essentially the same as described above. However, the installation commander is responsible for the maintenance of law and order on a military reservation and may take such immediate action in response to a terrorist incident as may be necessary to protect life and property.

The FBI will be notified as soon as possible of all terrorist incidents. It will exercise jurisdiction if the Attorney General or his designee determines that such incident is a matter of significant federal interest. When the FBI assumes jurisdiction, the Attorney General will coordinate the federal response. Should military assistance be required, it will be furnished according to the procedures described in the MOU. If the FBI declines to exercise its jurisdiction, military authorities will take appropriate action to resolve the incident.

3. Requests by Civilian Authorities for Use of Marine Corps Resources to Combat Domestic Terrorist Incidents

Requests for military assistance by civilian authorities to combat terrorist acts off-base are guided by the legal considerations discussed in paragraph 1 and the following regulations and instructions:

OPNAVINST 3440.16A provides procedures for processing and approving subject requests. Military resources are classified into three groups:

- Group 1: Personnel, arms, ammunition, tank-auto equipment, and aircraft.
- Group 2: Riot control agents, concertina wire and other equipment employed in control of civil disturbances.
- Group 3: Fire fighting resources, protective equipment (mask, helmets, etc.), other equipment such as clothing, communication equipment, and use of naval facilities.

If a request is made for Group 1 or Group 2 resources, the cognizant Marine commander will report the request in accordance with OPNAVINST 3100.6E, Special Incident Reporting, to CMC (POC). That request is forwarded to the Director of Military Support (DOMS), Department of Army, for approval. Group 2 resources may be granted by the Regional Planning Agent (designated by the principal planning agent and defined in OPNAVINST 3440.16A) when approved by the military task force on-site commander. In such cases, the request and action taken is forwarded to CMC with an informational copy sent to the principal planning agent (CINCPACFLT, CINCLANTFLT, CHNAVRES).

In the case of a request for Group 3 resources, the regional planning agent may grant authority for the loaning of these resources to civilian law enforcement agencies for their use. The request and action taken is transmitted to the principal planning agent with an information copy to CMC (POC).

Other applicable regulations and instructions concerning request for military assistance and/or cooperation with civilian law enforcement agencies in terrorist situations include the following:

- DOD Dir. 3025.1, Use of Military Resources During Peacetime Civil Emergencies Within the United States, Its Territories and Possessions (USDP).
- DOD Dir. 3025.10, Military Support of Civil Defense (USDP).
- DOD Dir. 3025.12, Employment of Military Resources in the Event of Civil Disturbances (USDP).
- DOD Dir. 5525.5, DOD Cooperation with Civilian Law Enforcement Officials (FMFP).
- DOD Dir. 2000.12, Protection of DOD Personnel and Resources Against Terrorists Acts (SO/LIC).
- SECNAVINST 5820.7B, Posse Comitatus Act.
- SECNAVINST 3850.1A, Protection of DOD Personnel and Resources Against Terrorist Acts.
- SECNAVINST 3050.32, Employment of Naval Resources in National Disasters, Emergencies Within the United States, Its Territories and Possessions.
- MCO 5720.60, Marine Corps Public Affairs Manual, Vol. 1, Community Relations.
- MCO 5720.61, Marine Corps Public Affairs Manual, Vol. 2, Organization, Mission, and Functions.
- MCO 3000.8B, Employment of Marine Corps Resources in Civil Disturbances.

Depending on the situation or circumstance, the applicable regulation or order should be reviewed and must be adhered to when responsive action is taken.

4. Response to Terrorist Acts Overseas

In the event of a threat or the use of force against U.S. forces based or stationed in a foreign country, the commanding officer, if the circumstances permit, should advise the host country of the situation and request appropriate assistance consistent with the applicable status of forces or station agreement (if a SOFA exists). If possible, foreign police/military forces should first be used to contain the threat or repel an attack. However, primary responsibility for the protection of Marine personnel, assets and/or installations remains with the commanding officer.

Appendix B

Memorandum of Understanding Between the Department of Defense, the Department of Justice, and the Federal Bureau of Investigation

SUBJECT: USE OF FEDERAL MILITARY FORCE IN DOMESTIC TERRORIST INCIDENTS

I. Purpose. This memorandum sets forth the responsibilities of the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Department of Defense (DOD); and the procedures to be followed by each of these agencies with respect to the use of military force in a domestic terrorist incident. These procedures are based on the Interdepartmental Action Plan for Civil Disturbances, dated April 1, 1969.

II. Responsibilities. The responsibility for the management of the Federal response to acts of terrorism in the United States rests with the Attorney General. As the chief law enforcement officer of the Federal Government, the Attorney General coordinates all Federal Government activities during a major terrorism crisis and advises the President as to whether and when to commit military forces in response to such a situation. Within the Department of Justice, the lead agency for the operation response to such incidents is made by the FBI Special Agent in Charge (SAC) at the scene, under the supervision of the Director of the FBI, who has overall responsibility for ongoing operations to contain and resolve the incident.

All military preparations and operations, including the employment of military forces at the scene of a terrorist incident, will be the primary responsibility of the Secretary of Defense. In discharging these functions, he will observe such law enforcement policies as the Attorney General may determine. To the extent practical, such law enforcement policies will be formulated during the early stages of the terrorist incident to insure that military planning and operations are consistent with administration policy and the requirements of the law.

The responsibilities of the Department of Defense under this memorandum will be carried out principally through the Department of Army, inasmuch as the Secretary of the Army is assigned primary responsibility for such matters as DOD Executive Agent.

III. Responding to Early Stages of Terrorist Incident. The Department of Justice will immediately notify DOD when a terrorist incident has occurred with potential for military involvement and will keep DOD advised of developments. The Department of Defense will dispatch military observers to the incident site upon mutual agreement by DOD and FBI to appraise the situation before any decision is made to commit federal military forces. Although the Posse Comitatus Act does not permit military personnel to actively engage in the law enforcement mission unless expressly authorized, the Act does not prohibit military observers from reporting to the Department of Defense; nor does it generally prohibit the preparation of contingency plans for lawful military intervention; advice to civilian officials; sharing intelligence information collected during the normal course of military operations, including operations relating to the incident; the loan of specialized equipment or weaponry; the use of military personnel to deliver and maintain equipment for civilian use, provided those personnel do not operate that

equipment; * or the use of military personnel to train civilian law enforcement officials in the operation and maintenance of military equipment. See 10 USC, Sec 371-78 (Supp. 1981); DOD Directive 5525.5, DOD Cooperation with Civilian Law Enforcement Officials; 47 Fed. Reg 14899 (April 7, 1982). Application of the Posse Comitatus Act may differ depending on the particular factual situation presented, and advice should be obtained whenever possible from appropriate officials.

Precautionary steps, such as the prepositioning of troops near the incident site may be undertaken with the approval of the DOD and the SAC. Prepositioning must, of course, be undertaken with discretion. The prepositioning of more than a battalion-sized unit (approximately 500 men) by order of the Secretary of Defense will be undertaken only with the informal approval of the President. Such approval will be sought by the Attorney General, and, ordinarily, only if there appears to be a substantial likelihood that such forces will be required.

When the SAC anticipates that federal military assistance will shortly become necessary, he will promptly notify the Director, who will advise the Attorney General. After consultation with the Director of the FBI and the Secretary of Defense on the gravity of the situation, the Attorney General will advise the President whether the conditions would warrant employment of military forces at that particular time. The FBI shall disseminate information concerning the incident and its participants to military authorities as though such authorities were operating in a law enforcement capacity. Such information may be retained by appropriate military components in accordance with procedures agreed upon by the Department of Justice and the Department of Defense.

IV. Employment of Military Forces. If the President decides to approve the use of military force, the Attorney General will, where necessary, furnish the President with an appropriately drawn proclamation and executive order, or other documents needed to implement his decision. Although the Attorney General has statutory authority to request the assistance of military forces for certain law enforcement purposes, military forces will not be committed in such circumstances without Presidential approval.

When the use of military force is approved, the Secretary of Defense will conduct military operation subject to law enforcement policies determined by the Attorney General. The Secretary of the Army, as Executive Agent for the Secretary of Defense, is responsible for the necessary military decisions and for issuance of the appropriate orders to the military task force commander. The established law enforcement policies may require revision or elaboration during the actual military operation; in that event, the Secretary of the Army will refer to such matters, military exigencies permitting, to the Attorney General, with his recommendation.

The Attorney General through the FBI will remain responsible for: (1) coordinating the activities of the federal agencies assisting in the resolution of the incident and in the administration of justice in the affected area, and (2) coordinating these activities with those state and local agencies similarly engaged.

Upon notification of a Presidential approval to use military force, the Attorney General will advise the military task force commander. The military commander and the SAC will coordinate the transfer of operational control to the military commander.

Responsibility for the tactical phase of the operation is transferred to military authority when the SAC relinquishes command and control of such operation and it is accepted by the on-site military task force commander. However, the SAC may revoke the military commitment at any time prior to the assault phase if he determines that military intervention is no longer required, provided that the military commander agrees that a withdrawal can be accomplished without seriously endangering the safety of military personnel or others involved in the operation. The military commander may utilize FBI personnel as hostage negotiators, translators, sniper/

*In the event the incident involves certain violations of federal law relating to controlled substances, immigration and nationality matters, or tariff and customs offenses, additional authority may be available permitting the use of military personnel to operate and maintain military equipment. See 10 USC, Sec 374 (Supp. 1981).

observers, and in other similar support roles, but FBI personnel may not participate in the tactical assault unless expressly authorized by the SAC.

When the military task force commander determines that he has completed the assault phase of the operation, command and control will be promptly returned to the SAC.

V. Post-Incident Responsibilities. Upon termination of the incident and return of command to the FBI, all military personnel will be evacuated immediately to a relocation site mutually agreed upon by the SAC and the military commander. However, certain key military personnel may be requested to remain briefly at the site if the SAC determines that their continued presence is necessary to protect the integrity of the investigative process. The FBI will make every reasonable effort to expedite interviews of military personnel and will afford such constitutional and procedural safeguards, including the presence of military counsel, as may be appropriate to the inquiry. To the extent permitted by law, the FBI will protect the identity of the such personnel and any sensitive methods or techniques used during the operation from public disclosure. All such information will be handled in accordance with the requirements of Executive Order 12356 or any successor order or regulations, where appropriate. In addition, procedures will be established to ensure that any forensic examination of weapons or other equipment used by military personnel that may be necessary will be conducted as expeditiously as possible.

VI. Terrorist Incidents on a Military Reservation. The respective roles of the Defense Department, the Justice Department and the FBI with respect to a terrorist incident on a military reservation may take such immediate action in response to a terrorist incident as may be necessary to protect life and property. The FBI will be promptly notified of all terrorist incidents and will exercise jurisdiction if the Attorney General or his designee determines that such incident is a matter of significant interest. Unless otherwise specified, the SAC of the appropriate region acting under the supervision of the Director shall be the Attorney General's designee in such matters. The Attorney General may request military assistance without Presidential approval in such circumstances, but such assistance shall be furnished in a manner consistent with the provisions of this memorandum of understanding. If the FBI declines to exercise its jurisdiction, military authorities will take appropriate action to resolve the incident.

VII. Terms of Agreement. This agreement will become effective immediately upon signature by all parties and shall continue in effect unless terminated by any party upon notice in writing to all other parties.

Amendments or modifications to this agreement may be made upon written agreement by all parties to the agreement.

(Signed)	5 Aug 83
John O. March, Jr. Secretary of the Army	(Date)

(Signed)	16 Jun 83
Jeffrey Harris Acting Associate Attorney General U.S. Department of Justice	(Date)

(Signed)	23 Jun 83
William H. Webster Director Federal Bureau of Investigation	(Date)

Appendix C

Physical Security Plan Format

CLASSIFICATION

Copy no._____of_____copies
Issuing Headquarters
Location
Date/time group

1. PURPOSE

(State plan's purpose.)

2. AREA SECURITY

(Define the areas, buildings, and structures considered critical. Establish priorities for their protection.)

3. CONTROL MEASURES

(Define and establish restrictions on access to and movement into critical areas.)

a. Personnel Access. (Establish control pertinent to each area or structure. Determine access authority. Provide access criteria for unit personnel, visitors, maintenance or support personnel, contractor personnel, and local police/armed forces. Describe the system used in each area. If a badge system is used, provide complete descriptions to disseminate requirements for identification and control of personnel. Identify application of the control system for unit personnel, visitors to restricted or administrative areas, vendors, tradesmen, contractor personnel, and maintenance or support personnel.)

b. Material Control. (State incoming and outgoing material control requirements. Identify material admission requirements, inspection procedures, special controls on delivery of supplies and/or personnel shipments in restricted areas, and required documentation.)

c. Vehicle Control. (Identify vehicle registration policy, search policies, parking regulations, and controls for entering restricted and administrative areas. Procedures must address privately-owned, military, and emergency vehicles.)

(Page number)

CLASSIFICATION

CLASSIFICATION

4. AIDS TO SECURITY

(Identify the installations's security procedures for protective barriers, protective lighting system, intrusion detection system, and communications. Define the protective barrier's clear zones [criteria and maintenance], signs [type and posting requirements], and gates [hours of operation, security requirements, and lock security]. State the protective lighting system's use and control, inspection procedures, response to commercial power failure, response to alternate source of power failure, and emergency lighting system [stationary and portable]. State the intrusion detection system's security classification, inspection procedures, use and monitoring, response to alarm conditions, maintenance requirements, alarm logs or registers, sensitivity settings, fail-safe and tamper-proof provisions, and monitor panel location. State communication locations, use, tests, and authentication procedures.)

5. INTERIOR GUARD PROCEDURES

(Include general instructions for interior guard personnel [fixed and mobile]). Detailed instructions (e.g., special orders and SOPs) are attached as annexes. Incorporate randomness into procedures. Address composition and organization; tour of duty; essential posts and routes; weapons and equipment; training; use of MWD teams; method of challenging with sign and countersign; ROE; and alert force's composition, mission, weapons, equipment, location, and deployment concept.)

6. CONTINGENCY PLANS

(Identify emergency response. Attach detailed plans [e.g., counterterrorism, bomb threats, hostage negotiation, disaster, fire] as annexes. Address individual actions, alert force actions, and security alert status.)

7. SECURITY ALERT STATUS

(Determine current security alert status.)

8. USE OF AIR SURVEILLANCE

(State whether or not air surveillance is to be exploited.)

9. COORDINATING INSTRUCTIONS

(Identify integration plans of host nation or nearby military installations. State liaison and coordination instructions for local civil authorities, federal agencies, and other military organizations.)

/s/ Commander

ANNEXES as applicable

(Page number)

CLASSIFICATION

Appendix D

THREATCON System

Section I. Basic THREATCON Procedures

The THREATCONs outlined below describe the progressive level of terrorist threat to all United States military facilities and personnel under MCO 5500.13. As approved by JCS, the terminology, terms, and definitions are recommended security measures designed to ease inter-Service coordination and support of United States military antiterrorism activities. The purpose of the THREATCON system is accessibility and easy dissemination. The declaration, reduction, and cancellation of THREATCONs remains the exclusive responsibility of the commanders specified in the order. While there is no direct correlation between threat information (e.g., ATAC 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.

THREATCON NORMAL exists when there is no known threat.

THREATCON ALFA exists when there is a general threat of possible terrorist activity against installations and personnel. The exact nature and extent are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO. However, it may be necessary to implement selected THREATCON BRAVO measures as a result of intelligence or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

THREATCON BRAVO exists when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing hardship, affecting operational capability, and aggravating relations with local authorities.

THREATCON CHARLIE exists when an incident occurs or when intelligence is received indicating that some form of terrorist action is imminent. Implementation of this measure for longer than a short period of time will probably create hardship and affect peacetime activities of a unit and its personnel.

THREATCON DELTA exists when a terrorist attack has occurred or when intelligence indicates that a terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

Once a THREATCON is declared, the following security measures are mandatory and implemented immediately. Commanders are authorized to supplement these measures.

THREATCON ALFA

Measure 1 At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of United States installations. Watch for abandoned parcels or suitcases and any unusual activity.

Measure 2 Have the duty officer or personnel with access to building plans and plans for area evacuations available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

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

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

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

Measure 6 As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO individually or in combination.

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

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

Measure 9 Spare.

THREATCON BRAVO

Measure 10 Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

Measure 11 Keep all personnel involved in implementing antiterrorist contingency plans on call.

Measure 12 Check plans for implementation of the next THREATCON.

Measure 13 Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

Measure 14 Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

Measure 15 At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

Measure 16 Examine mail (above the regular examination process) for letter or parcel bombs.

Measure 17 Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

Measure 18 Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

Measure 19 Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

Measure 20 At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

Measure 21 Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers.

Measure 22 Operate random patrols to check vehicles, people, and buildings.

Measure 23 Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or driving.

Measure 24 Implement additional security measures for high-risk personnel as appropriate.

Measure 25 Brief personnel who may augment guard forces on the use of deadly force.

Measures 26-29 Spare.

THREATCON CHARLIE

Measure 30 Continue or introduce all measures listed in THREATCON BRAVO.

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

Measure 32 Limit access points to absolute minimum.

Measure 33 Strictly enforce control of entry. Randomly search vehicles.

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

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

Measure 36 Increase patrolling of the installation.

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

Measure 38 Erect barriers and obstacles to control traffic flow.

Measure 39 Spare.

THREATCON DELTA

Measure 40 Continue or introduce all measures listed for THREATCONs BRAVO and CHARLIE.

Measure 41 Augment guards as necessary.

Measure 42 Identify all vehicles within operational or mission support areas.

Measure 43 Search all vehicles and its contents before allowing entrance to the installation.

Measure 44 Control access and implement positive identification of all personnel.

Measure 45 Search all suitcases, briefcases, packages, etc., brought into the installation.

Measure 46 Control access to all areas under the jurisdiction of the United States.

Measure 47 Make frequent checks of the exterior of buildings and of parking areas.

Measure 48 Minimize all administrative journeys and visits.

Measure 49 Coordinate the possible closing of public and military roads and facilities with local authorities.

Measure 50 Spare.

Section II. Aviation Facility THREATCON Procedures

In addition to basic THREATCON procedures, a variety of other tasks need to be performed at aviation facilities under MCO 5500.14.

THREATCON ALFA AND BRAVO

Planning

Review THREATCON ALFA and BRAVO.

Update THREATCON ALFA and BRAVO as required.

Briefing and Liaison

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

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

Ensure that duty officers are always available by telephone.

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

Be prepared to receive and direct aircraft from other stations.

Precautions Inside Air Stations

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

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

Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area.

Search all vehicles, briefcases, packages, etc., entering the area.

Erect barriers around potential targets if possible.

Maintain firefighting equipment and practice drills.

Hold practice alerts within barrack perimeters.

Precautions Outside Air Stations

Carry out regular inspections of perimeters, especially adjacent to flight paths, in conjunction with local police.

Advise the local police of any areas outside the perimeter where attacks could be mounted and which cannot be avoided by aircraft on takeoff or landing.

Warn air crews to report any unusual activity near approach and overshoot areas.

THREATCON CHARLIE

Planning	Review THREATCON CHARLIE.
	Update THREATCON CHARLIE as required.
Briefing and Liaison	Brief all personnel on the increased threat.
	Inform local police of increased threat.
	Coordinate precautionary measures taken outside airfield perimeters with local police.
	Implement appropriate flying countermeasures laid down in SOPs as directed by air traffic controllers.
Precautions Inside Air Stations	Consider replacing civilian guards with military guards at access points.
	Inspect all vehicles and buildings regularly.
	Detail additional guards to be on call at short notice and consider augmenting firefighting details.
	Carry out random patrols within airfield perimeters and maintain continuous observation of approach and overshoot areas.
	Reduce flying to essential operational flights only. Cease circuit flying if appropriate.
	Escort all visitors.
	Close relief landing grounds where appropriate.
	Check airfield diversion state.
Precautions Outside Air Stations	Be prepared to react to requests from major Marine commands.
	Provide troops to assist local police in searching approaches outside the perimeter of military airfields for terrorists.

THREATCON DELTA

Planning	Review THREATCON DELTA.
	Update THREATCON DELTA as required.
Briefing and Liaison	Brief all personnel on the very high level of threat.
	Inform local police of increased threat.

Precautions Inside Air Stations

Cease all flying except for specifically authorized operational sorties.

Implement appropriate flying countermeasures if necessary.

Be prepared to accept aircraft diverted from other stations.

Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

Precautions Outside Air Stations

Close military roads allowing access to the air station.

Appendix E

Installation Vulnerability Assessment

The installation vulnerability assessment (IVA) provides the installation commander with a tool to assess installation/unit vulnerability. The IVA must stand on its own and be supported by valid considerations. Typically, a small group of knowledgeable individuals develops the IVA and forwards it to the command group upon completion. Use the IVA and available hard intelligence information as tools to determine potential vulnerability. When a specific threat is proven, the IVA aids in developing measures to counter the threat. Compare the results of your IVA with those of other installations to determine relative vulnerability.

It is important that the evaluator record assigned points. Installations with a low vulnerability score can still be primary terrorist targets because of one or more of the criteria used. For example, your installation may have a very low score, but scored high on one category (e.g., installation characteristics and sensitivity). Terrorists may target the installation specifically to obtain nuclear or chemical weapons. Consider each of the IVA categories separately. If your installation scores high on any of the categories, consider yourself at risk. Even if you score low on all categories, you may still be at risk if potential terrorist activity exists in your area.

No factor is a determinant by itself. Consider the overall relationship between factors. The IVA uses a scale of 0-100 points. The higher the value, the higher the vulnerability. Each category has a paragraph for narrative assessment. The narrative paragraph provides a thorough understanding of why and how scores were determined. It is important that the commander fully understand scoring rationale, and why certain areas are high risk. The last step involves totalling the points. Review the high scoring areas when determining allotment of resources in order to decrease an installation's vulnerability. Upon completion of the IVA, total the points in all categories and compare the total to the scale below.

Vulnerability Range	Points
Very low	0-10
Low	11-30
Medium	31-60
High	61-80
Very High	81-100

Installation Characteristics and Sensitivity
(16 Points Maximum)

Installations are capable of establishing and maintaining barrier integrity, especially in emergency situations.

_____ VIPs. (1 point per celebrity, 3 points foreign personnel) **(6 points maximum)**

_____ Mission sensitivity. If more than one of the following categories applies to your installation, assess maximum point value. **(6 points maximum)**

Nuclear, chemical, or intelligence facility (6 points)
Research and development facilities (5 points)
Marine Corps base, air station, or air facility (4 points)
Training facility (2 points)

_____ Current threat analysis by military police/intelligence investigators. (available 0 points/unavailable 3 points)

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

NARRATIVE ASSESSMENT:

Geographic Region
(8 Points Maximum)

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

_____ West Coast/Florida/Outside CONUS (8 points)

_____ East (6 points)

_____ Southwest (4 points)

_____ South, Northwest, Central, Northeast, and Mid-Atlantic (2 points)

NARRATIVE ASSESSMENT:

Status of Training
(12 Points Maximum)

Consider establishing, equipping, maintaining, and testing operations and other special threat personnel. Trained installation personnel refers to SRTs, hostage negotiators, CMTs, communication specialists, etc.

_____ Operations center inactive and no terrorism-trained installation personnel. (12 points)

_____ Operation center active, but no terrorism-trained installation personnel. (9 points)

_____ Operation center active, terrorism-trained installation personnel present, but required equipment not fully available. (7 points)

_____ Operation center active, terrorism-trained installation personnel present, and required equipment available. (3 points)

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

NARRATIVE ASSESSMENT:

Distance from Urban Areas
(8 Points Maximum)

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

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

NARRATIVE ASSESSMENT:

Availability of Communications
(11 Points Maximum)

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

_____ Communications with lower elements only. (4 points)

_____ Communications with lower and lateral elements only. (3 points)

_____ Communications with higher, lower, and lateral elements. (0 points)

_____ Landline telephone.
Nondedicated (2 points)
Dedicated (1 point)
Secure dedicated (0 points)

_____ Radio.
Nondedicated (2 points)
Dedicated (1 point)
Secure dedicated (0 points)

NARRATIVE ASSESSMENT:

Time and Distance from Other U.S. Military Installations
(7 Points Maximum)

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

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

NARRATIVE ASSESSMENT:

Availability of Nonmilitary Law Enforcement Resources

(8 Points Maximum)

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

	Response Time Points			
	1 Hour	2 Hours	3 Hours	+3 Hours
Trained federally* and locally	1	2	3	4
Trained federally*	2	3	4	5
Trained locally	3	4	5	6
Not trained locally	4	5	6	7
Not available	8	8	8	8

*Federally refers to United States and host nation governments.

NARRATIVE ASSESSMENT:

Terrain

(5 Points Maximum)

Analyze terrain in conjunction with a review of installation sensitivity, adequacy of barrier defense, and routes of access/egress.

_____ Built-up area (5 points)
_____ Mountainous, forested, or areas conducive to concealment (4 points)
_____ Open areas (2 points)

NARRATIVE ASSESSMENT:

Access to Installation
(8 Points Maximum)

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

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

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

_____ Waterways
- Navigable (2 points)
- Nonnavigable (1 point)
- None (0 points)

NARRATIVE ASSIGNMENT:

Unity of Security Effort
(8 Points Maximum)

_____ Single Service installation and existing crisis management plan and organization (0 points)

_____ Multi-Service installation and existing crisis management plan and organization (4 points)

_____ Single Service installation and no crisis management plan or organization (6 points)

_____ Multi-Service installation and no existing crisis management plan or organization (8 points)

NARRATIVE ASSESSMENT:

Proximity to Foreign Borders
(8 Points Maximum)

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

_____ Mexican border
- 0-100 miles (8 points)
- 101-500 miles (6 points)
- Over 500 miles (2 points)

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

NARRATIVE ASSESSMENT:

Appendix F

Individual Security Precautions in High-Risk Areas

Military personnel and their families must know and understand the area's threat level, appropriate protection plan and their role, and what to do in an emergency. If possible, avoid establishing a routine schedule. Past incidents show that terrorists keep their victim under surveillance for a substantial period of time in order to discover travel patterns and to arrange a suitable time and place for kidnappings or assassinations. Unpredictability is one of the best defensive weapons. The following list provides a heightened awareness of individual security measures.

Personal Security Measures

Avoid wearing a uniform if possible.

Avoid using rank, especially in a civilian environment.

Keep a low profile.

Be sensitive to the possibility of surveillance. Before leaving, check up and down the street for suspicious cars or individuals.

Be aware of the possibility that you are being followed. If you suspect you are being followed, move as quickly as possible to preselected safe havens (e.g., police station); report the incident; identify the vehicle or person if possible; contact your base security officer as soon as possible.

Do not eat at the same restaurant twice in a row.

Do not dress in a fashion that clearly identifies you as American; e.g., cowboy.

Do not go to the office when no one else is there.

Avoid civil disturbances and disputes with local citizens.

Immediately summon local police if a dispute occurs or if there is an accident.

Do not divulge your home address, telephone number, or family information unnecessarily.

Watch for unexplained absences of local citizens as early warning of possible terrorist action.

Learn certain key phrases of the host nation's language (e.g., I need a policeman. Take me to a doctor. Where is the hospital? Where is the police station? Help!).

Learn to use local commercial telephones.

Learn emergency telephone numbers (e.g., military police, fire department, unit headquarters, etc.).

Carry the exact change needed for pay telephones.

Receive all mail through a U.S. facility.

Inspect mail and packages for possible letter bombs or other devices.

Do not accept unsolicited packages.

Vary the time and place of personal fitness routines.

Avoid walking/jogging on country roads or down deserted streets.

Walk in well-populated areas at the height of rush hour.

Always carry identification documents. Carry a card stating blood type and allergies to particular medication. The card should be bilingual: English and the language of the host nation.

Do not flash large sums of money.

Security During Travel

Vary mode of transportation and dress.

Use unmarked vehicles.

Vary routes, departure time, arrival times, and entrances and exits if you walk to and from work and around town.

Keep co-workers and family aware of schedules.

Check in before departure and after arrival.

Report any unexpected changes in schedule.

Travel with a group of people.

Travel on busy, well-travelled thoroughfares. Stay away from isolated country roads.

Know where dangerous areas are located and avoid them.

Drive toward the center of the road on single lane highways.

Keep doors locked and windows closed or opened only partially when travelling in an automobile.

Park cars off the street at night.

Park in a safe, lighted area.

Lock car when it is unattended.

Search car before entering to ensure there are no suspicious objects or unexplained wires or strings outside, underneath, or inside. Immediately report any suspicious wires or objects to the proper authority.

Do not permit taxi drivers to deviate from known and desired routes.

Do not use the same taxi service or bus stop.

Do not take the first available cab.

Never pick up hitchhikers.

Avoid going out alone.

Appendix G

Senior Officer's Security Measures

Unless targeted as a primary target, military personnel must ensure their own security in a high-risk area. Develop personal security programs to reduce risk. Do not under estimate the seriousness of the threat. Discuss the threat to your personal security with your security staff and principle assistants. Brief your personal staff and driver on their responsibilities. Discuss appropriate measures with your family.

An individual's military training includes self-protection training, weapons training, hostage survival training, OPSEC training, awareness of current status-of-forces agreements, and awareness of special equipment needs (e.g., armor-plated vehicles). However, each individual should develop his own security plan. The following list identifies areas to consider when developing a personal security plan.

Security at Home

Evaluate home security requirements.

Check persons entering the premises; e.g., electricians, plumbers, telephone maintenance personnel. If in doubt, call their office.

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

Ensure all door locks/window clasps are working.

Consider installing a door security chain, spy glass, or visitor intercom.

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

Consider installing security lights to aid in identification of visitors outside the home.

Draw curtains in a room before switching on lights.

Consider fitting windows with either venetian blinds or thick curtains.

Have reserve lighting handy; e.g., flashlight, lamps.

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

Investigate household staff (especially temporary staff).

Always be on the lookout for the unusual.

Ensure home is locked and secure if leaving the resident unattended for several days. Be cautious upon return.

Arrange for visits to be made by police and neighbors if the house is left unattended.

Have telephone numbers of police, PMO, and local Marine guard forces readily available.

Arrange for the observation of all mail, parcels, and local trade deliveries.

Keep in touch with neighbors.

Do not hesitate to call the police.

Take vehicle numbers if you are suspicious.

Note and report suspicious persons.

Strictly control house keys.

Ensure car is never left unattended.

Place car in a locked garage.

Be on the alert for the unusual; e.g., the movement of furniture or the placing of unusual wires.

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

Consider an alarm to a neighbor's house.

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

Security to and from Work

Vary daily pattern as much as possible. Leave and return at different times. Use alternative routes.

Be discreet in forecasting movements.

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

Use defensive and evasive driving techniques.

Drill with your driver by watching for suspicious cars and taking evasive action.

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

Park car in a safe area.

Keep the trunk locked.

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 under cars.

Do not leave personal items exposed in the car; e.g., items of uniform, service issue maps, official briefcases.

Security at Official Functions

Discuss security requirements with the person planning the function.

Travel to and from the function with escorts.

Choose the route carefully.

Do not publicize planned attendance at official functions unless required.

Attempt to sit away from public areas.

Security at Private Functions

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

Have your personal staff assist a civilian host if required.

Arrange that visitors be subject to adequate security control.

Screen the issuance of invitations if possible.

Vary times at sporting activities; e.g., golfing, jogging.

Security During Travel

Restrict the use of rank or title.

Do not see unknown visitors in hotel room or suite.

Book airline seats at the last moment or use an alias.

Security of Children

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

Instruct children never to admit strangers to the house.

Teach children when and how to alert police or neighbors.

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

Instruct children to refuse gifts or approaches from strangers.

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

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

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

Encourage children to report suspicious incidents to you.

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

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

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

Appendix H

Office Procedures

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

Office Accessibility

Offices most likely to be terrorism targets should not be directly accessible to the public.

Do not locate executive office areas on ground floor levels.

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

If office windows face public areas, curtain and reinforce with bullet resistant materials.

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

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

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

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

Depending upon the nature of the organization's activities, draw attention away from the location and function of the office.

Physical Security Measures

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

If feasible, add a high perimeter fence or wall and a comprehensive external lighting system.

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

Position light fixtures where tampering would be difficult and noticeable.

Check grounds to insure there are no covered or concealed avenues of approach for terrorists, especially near entrances.

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

Lock manhole covers near the building.

Cover, lock, or screen outdoor openings such as coal bins, air vents, or utility access points.

Screen windows (particularly those near the ground or accessible from adjacent buildings) to prevent a terrorist from throwing an explosive device into the building or placing one on the ledge.

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

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

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

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

Mailboxes should not be close to the building.

Seal tops, voids, and open spaces above cabinets, bookcases, and display cases.

Keep janitorial closets, service openings, telephone closets, and electrical closets locked at all times.

Protect communication closets and utility areas with an alarm system.

Remove names on reserved parking spaces.

Empty trash receptacles daily (preferably twice a day).

Periodically check fire extinguishers to be sure they are in working order and readily available. Recharge as necessary.

Personnel Procedures

Stress heightened awareness of personnel working in the office. The security of an office depends largely on the actions and awareness of its personnel.

Develop and disseminate clear instructions on personnel security procedures.

Hold regular security briefings for building occupants.

Personnel should understand security measures, appropriate response, and who to contact in an emergency.

Drill if appropriate.

Senior personnel should not work late on a routine basis. Never work alone.

Give switchboard personnel and secretaries special training in handling bomb threat and extortion telephone calls.

Insure communications between senior personnel, secretaries, and security personnel with intercoms, telephones, and duress alarm systems. Conceal these communication lines if possible.

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

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

Have mail room personnel trained in bomb detection, handle and inspect all suspect items.

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

Maintain tight control of keys.

Lock cabinets and closets when not in use.

Lock all office rest rooms when not in use.

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

Keep janitors under observation when cleaning.

Secure official papers from unauthorized viewing.

Update security clearances of employees (especially foreign nationals).

Do not reveal the location of office personnel to callers unless they are positively identified.

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

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

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

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

Be alert to people disguised as public utility crews, road workers, vendors, etc., who might station themselves near the office to observe activities and gather information.

Note parked or abandoned vehicles near the entrance or walls.

Note the license number of suspicious vehicles and occupant's descriptions and report to your supervisor, security officer, or local police.

Controlling Entry

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

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

Consider the installation of metal detecting devices at controlled entrances.

Prohibit the introduction of boxes and parcels by nonorganizational members.

Arrange office space so unescorted visitors are under the receptionist's visual observation and they follow stringent access control procedures.

Do not make exceptions in an office's access control system.

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

Policing the Area

Determine if the local or military police patrol the area.

Request patrol by local or military police.

Know the capabilities and limitations of local and military police.

Use private guards if appropriate.

If using private guards, perform background checks.

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

Brief guards on appropriate response in case of a terrorist incident.

Preparation for Emergencies

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

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

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

The safe room should have a sturdy door with a lock and an emergency exit if possible. Bathrooms on upper stories work well as safe rooms.

Store emergency and first aid supplies in the safe room.

Bars or grill work on safe room windows should be locked from the inside to ease escape.

Keep keys to locks, a rope or chain ladder to ease escape, and a means of communication (e.g., telephone or radio transmitter) in the safe room.

Select and identify emergency exits.

Determine evacuation and escape routes and brief personnel.

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

Maintain a set of written emergency and contingency procedures in the security office.

Emergency procedures should include bomb threat and bomb search techniques.

Public Areas

Remove all potted plants and ornamental objects from public areas.

Empty trash receptacles frequently.

Lock doors to service areas.

Lock trap doors in the ceiling or floor, including skylights.

Empty wastebaskets frequently to prevent an accumulation of trash which would hide an explosive device.

Keep the premises clean and neat so it is easier to observe anything out of place. (Do not allow parcels, boxes, cases, or bundles of books or magazines in public areas.)

Insure construction or placement of furniture and other items would not conceal explosive devices or weapons.

Keep furniture away from walls or corners.

Raise, tie back, or remove curtains, drapes, or cloth covers.

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

Exercise particular precautions in public rest rooms.

Install springs on stall doors in rest rooms so they stand open when not locked.

Equip stalls with an inside latch to prevent someone hiding a device in a locked stall.

Fasten down or install a fixed covering over the covers on commode water tanks.

Use open mesh baskets for towels. Empty frequently.

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

Appendix I

Lock Security

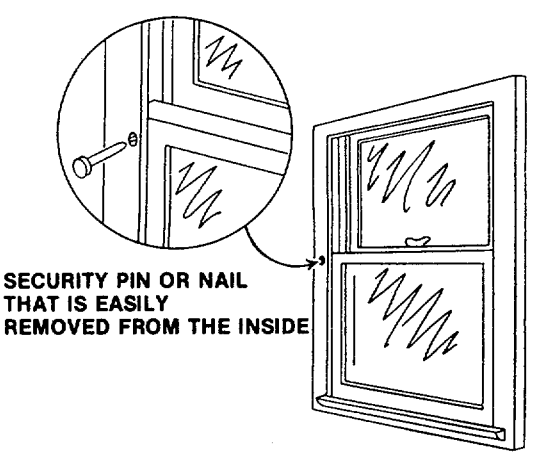
The first line of defense in any security system are locks or locking devices. Residence, office, or vehicle security rely heavily upon locking devices. Locking devices vary in appearance, function, and application. Locks are delaying devices of perimeter security. Locking devices can be effectively integrated into other security and protection systems (e.g., alarms, electronic controls). Intruders cannot risk creating loud noises in an attempt to defeat or break locks, nor can they afford the time.

How much should you spend for a lock? Security increases in proportion to the amount of money spent on quality locking devices. The stronger the locks and the more sophisticated its mechanisms, the greater degree of security. With normal usage and care, quality locks will last 30 to 40 years. The five major categories of locks used in residences or offices are cylindrical, mortise, cylinder dead bolt, rim, and cylindrical lock sets with dead bolt functions.

Entryway Safety Factors

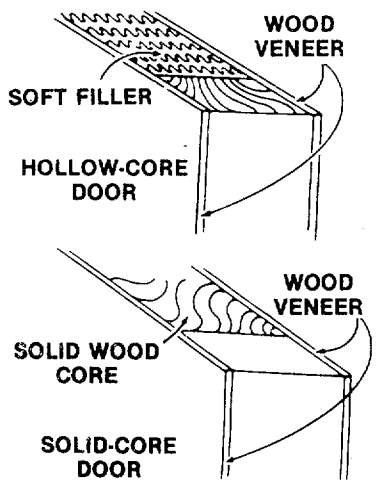
Windows

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



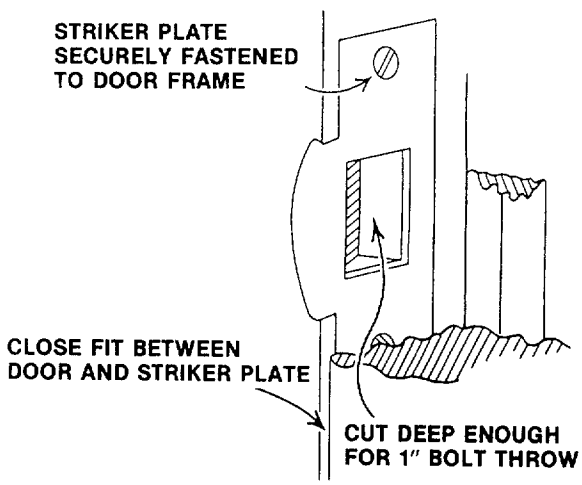
Employ the following techniques to upgrade window security. The simplest measure is to drill one or more holes through the sash and frame and insert a pin or nail to prevent the window from being opened. Key-operated locks are also available, but they pose a safety hazard in the event that the window is needed for escape in an emergency. Other methods of window security include the installation of steel bars, mesh, or grillwork.

Doors



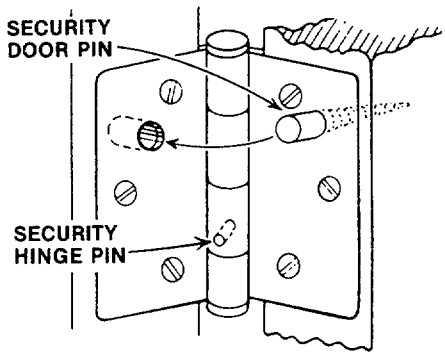
As important as the locking device is, the security afforded is only as good as the construction of the door and frame. There are three major types of doors: flush wood doors, stile and rail (panel) wood doors, and metal doors. There are two types of flush doors: hollow-core and solid-core. A hollow-core door is made of two sheets of thin veneer overlaying hollow cardboard strips. A solid-core door is made of two sheets of wood veneer overlapping a solid wooden core. Solid-core doors provide a substantial security advantage over hollow-core doors. Solid-core doors add sound insulation and fire resistance. From a security perspective, a metal door is superior to any wooden door.

A door's vulnerability (as opposed to its frame, hinges, or other accessory parts) is defined in terms of penetrability (How easy is it to break through? How long does it take to break through?). However, breaking through a door is not the most common method in defeating a door system. A far more significant hazard is a door that fits loosely to the frame, thereby allowing it to be pried or forced open. Most wooden door frames have solid wood, 3/4 inch to 1 inch in depth. Beyond this, there is usually a 4-inch to 6-inch gap of air between the frame and the first stud. This construction provides very little resistance to forced entry. Strengthen the door frame by securing 2-inch by 4-inch studs directly behind the door frame's facing. Another method uses long wood screws that will reach and fasten to the first stud in the wall.



Striker Plates. A secure lock is only as effective as the striker plate it engages. 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.

Hinges. The security value of the door hinge is often overlooked. A well secured hinge prevents forcing a door out of its frame.

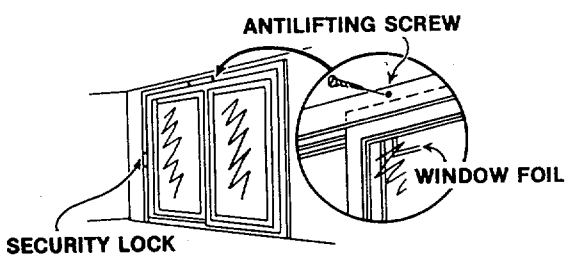


From a security standpoint, the most important feature of a hinge is whether it is located on the inside or outside of the door. If the hinge pins are on the outside, they can be removed and the door removed from the frame. There are several solutions to this problem. One is to weld the pins to the hinge or between the two ends. This method is effective, but permanent. Another technique (see the illustration) requires drilling a small hole through the hinge and into the pin and inserting a second pin or small nail flush with the hinge surface. Another technique requires inserting two large screws in the door (or jamb) and leaving the screw head exposed 1/2 inch. Drill a matching hole on the opposite side so the screw head fits into the hole when the door is shut.

Sliding Glass Doors

Sliding glass doors present easy access to a residence and pose complex security problems. Sliding glass doors are available in a variety of styles and sizes. Sliding glass doors are designed with little or no thought to security.

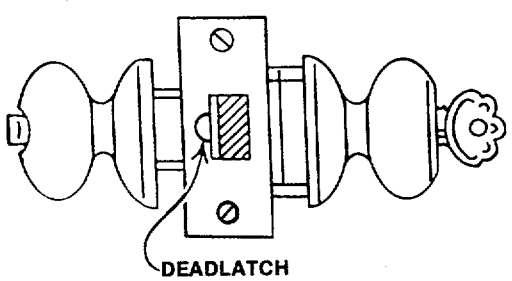
Many factors affect the ability to secure this type of entrance. It is not enough to prevent the door from being moved horizontally, it must also be secured vertically. The channel in which the door rides provides wide tolerances and facilitates vertically lifting the door out of its channel. Most locks designed for sliding glass doors take into consideration both types of movement and prevent the door from being lifted out of the channel. The simplest measure is to drill a hole through the channel and the frame. Insert a pin or nail to prevent the door from being opened. Also, insert sheet metal screws into the upper channel and allow them to protrude far enough to prevent the door from being lifted out of the channel.

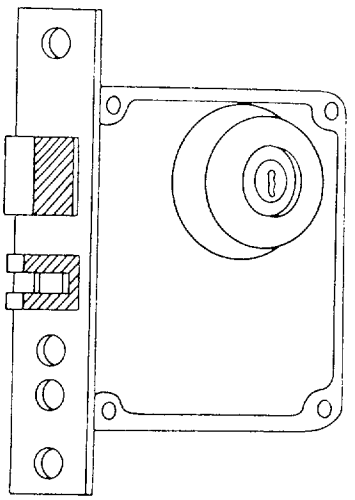


Locking Mechanisms

Cylindrical Locks

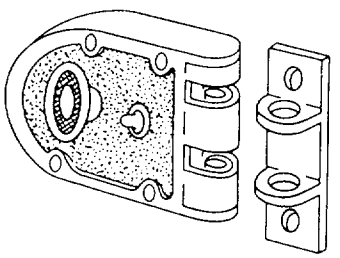
Cylindrical locks (key-in-knob locks) are the most widely used lock in residential construction. Cylindrical locks are both inexpensive and simple to re-key. Cheaper cylindrical locks have serious shortcomings. Cheap cylindrical locks may not have a dead latch and may be slipped with a credit card or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





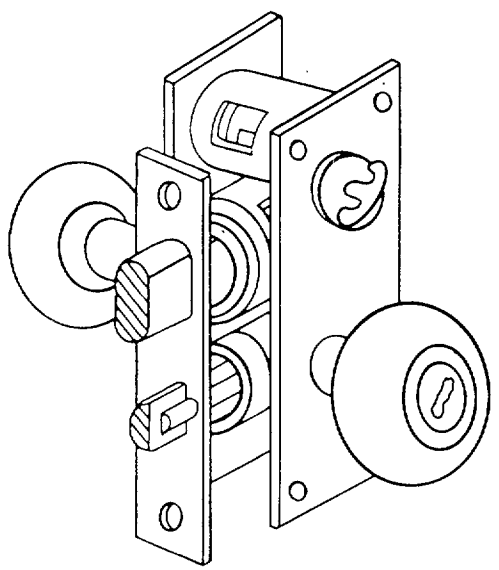
Mortise Locks

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



Rim Locks

Rim locks are erroneously referred to as jimmy proof. Do not be misled by the use of the word proof—these locks can be compromised. However, rim locks are one of the most secure surface-mounted locks. Usually, rim locks are not used as the primary lock. Install rim locks on the inside of the door above vulnerable primary locks. Assuming the striker is properly installed on the jamb and that a vertical dead bolt is used, the rim lock makes an excellent auxiliary lock and is very difficult to defeat. Rim locks are far less expensive than replacing the primary lock.

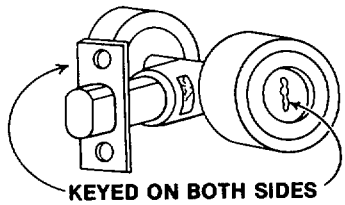


Cylindrical Lock Sets With Dead Bolt Functions

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.

Cylinder Dead Bolt Locks

Single-cylinder dead bolt locks are rapidly becoming the most popular auxiliary lock. Install these locks 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. Fire officials are concerned that the need to find a key delays escape in an emergency.



Lock Selection Guidelines

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

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

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

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

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

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

- A heavy shackle—at least 9/32 inch of hardened steel.
- A double locking mechanism that locks the heel and toe.
- A minimum five-pin tumbler on tumbler locks.
- A key retaining feature that prevents removing the key unless the padlock is locked.

Use rim locks to provide additional protection.

Lock all vulnerable windows and doors at night.

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

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

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

Fill hollow metal door frames behind the striker plate with cement to prevent forcing the frame.

Restrict home and office keys.

Restrict distribution and duplication of keys.

Keep spare keys in a locked drawer or filing cabinet.

Incorporate heavy-duty, double-cylinder door locks on office entrance doors if fire and safety regulations permit.

Appendix J

Soft Target Procedures

Soft targets provide easy access and little risk to the terrorist. Predetermining soft targets is extremely difficult, if not impossible. Therefore, hard and fast guidance is not available. However, commanders should use the guidelines provided in this appendix to develop security plans or advise personnel. If unable to follow the guidelines given in this appendix, follow the intent as closely as possible. Minimize the risk of attack and its effect on soft targets by taking sensible precautions. Examples of soft targets include—

- Open garrisons, stations, barracks, or establishments where access is not strictly controlled. Potential targets within these areas are sleeping accommodations, administrative buildings, and communal areas.
- Military buildings in civilian environments.
- Establishments unmanned during nonworking hours.
- Unattended vehicles.
- AA&Es and other military stores in transit.
- Military events (e.g., displays, exhibitions, open days) open to the public, both on and off Marine Corps property.
- Places of entertainment frequented by troops.
- Off-duty personnel.
- Dependents.

Those responsible for the security of property should assess on a day-to-day basis whether authorization for the use of their premises by civilian organizations is compatible with the maintenance of security. Consider the premises, units occupying the premises, and civilian usage when making the assessment. Security considerations always outweigh financial factors. In cases where it is necessary to temporarily withdraw authority for public use of premises, civilian organizations usually cooperate willingly and military/civilian relationships do not suffer. If the public has access to military premises, the commanding officer places a responsible member of his unit in attendance to ensure security is maintained.

1. Installations/Units

a. Responsibility. Although the installation commander is responsible for overall area security, individual units are responsible for their own local protection. The installation/unit prepares, updates, and practices the installation/unit security plan; establishes liaison with the local police; and continuously monitors the local threat. The continuous application of security procedures provides the best protection for soft targets.

b. Installation/Unit Security Plan. Periodically practice an installation/unit security plan. A command's senior officer oversees the drill. Cooperate with local police. A typical security plan might include—

- Arranging security of communal areas; e.g., clubs, places of entertainment.
- Organizing installation/unit emergency operations center.
- Providing an installation/unit reserve force during an alert or period of increased threat.
- Patrolling the perimeter of military installations.
- Guarding and controlling entry/exit points to military installations.

- Protecting married quarters inside and outside U.S. Marine Corps property.
- Warning systems which alert units (on and off duty) of changes in the security situation.
- Identifying assistance procedures for units with limited manpower resources.
- Securing large functions inside or outside the military installation.
- Identifying security role of the PMO and interior guard personnel.
- Establishing liaison with local police.

c. Unit Security. Unit security plans vary from unit to unit. Plan composition depends on local circumstances and a unit's role, size, and location. Base unit security procedures on the installation's overall security plan. Supplement these security procedures with unit instructions, knowledge of local circumstances, and advice from security staff and local police. Unit security plans should address the following:

- Alert measure application within the unit.
- Response to discovery or suspicion of an IED.
- Evacuation plan.
- Search plan.
- Immediate reaction plan addressing first-aid, cordoning the affected area, alerting emergency services, personal security advice and measures, etc.

d. Liaison. Liaison with local police and nearby property owners is essential. Unit commanders communicate with nearby property owners to ensure the individual Marine's protection, heighten civilian threat awareness, and dispel rumors. Do not mislead property owners into thinking that the U.S. Marine Corps is responsible for the protection of civilians. Units notify local authorities and the installation commander of any training outside recognized training areas.

2. Individuals

It is not the intention of these instructions to suggest that military personnel and their dependents should live in a constant state of worry about their personal security. Vigilance and caution relevant to the current situation ensure safety. Responsibility for the protection of personnel living off base normally rests with local police and personnel living on base rely on installation security. Take the following measures to minimize risk. There may be times when the following measures have an added significance because of increased terrorist activity. If increased terrorist activity is present, commanders should remind personnel of the measure applicable to the situation.

a. Security in Public Places. If Marines congregate in a specific place of entertainment and the threat level is high, discuss with local police the possibility of organizing joint patrols. Improve security in public places by selecting a member of the group to be a lookout. The lookout remains alert to any suspicious event inside the establishment and looks outside from time to time.

Do not leave the security of formal, organized gatherings to an improvised lookout system. Take proper security precautions to organize interior guard capabilities.

b. Married Quarter's Security

(1) Householders. Each householder acts as the security officer for his home and immediate area. Remain alert and inquisitive towards strangers and anything unusual. Keep house surroundings tidy. Make it difficult to hide an IED. Ensure dependents know how to report anything suspicious if the householder is away from the house.

(2) Military Warden Scheme. If there are large numbers of separated families, it may be necessary to implement a military warden scheme (similar to a civilian neighborhood watch).

Divide the area into areas of responsibility and assign units. Each unit selects a military warden for its area. The duties of a military warden include—

- Being at his quarters during his tour of military warden duty.
- Displaying a military warden sign outside his quarters.
- Receiving reports of prowlers, suspicious persons, or unusual occurrences from separated families.
- Transmitting reports as fast as possible to the appropriate authority.
- Assisting a separated family in cases of emergency.

3. Transportation

Transportation risks include theft and placement of bombs. Stolen military vehicles present the terrorist with a convenient way to access military installations unchecked. Military vehicles carrying passengers, contract hire vehicles, and civil transport vehicles used extensively by service personnel are prime targets for bomb placements. General officer and staff cars for VIPs are attractive targets and require special attention.

a. Parking Passenger-Carrying Military Vehicles. Use the following guidance to park passenger-carrying military vehicles:

- House military vehicles in protected or guarded locations when not in use.
- Examine storage space, racks, battery and tool lockers, spare wheel, and engine compartments before using a vehicle.
- Vary halts on regular runs.
- Do not leave vehicles unattended in public places if there is more than one passenger.
- If a driver is unaccompanied, halt where the vehicle can be left in military, local police, or other secure custody. If this is not possible, lock the vehicle and parked where it will be under the observation of the driver. Search the vehicle before resuming the journey.
- Never leave vehicles carrying AA&Es or classified material in unguarded places.
- Search any vehicles exposed to risk before resuming the journey.
- Drivers and passengers cooperate to ensure that all baggage is identified before loading and that those presenting baggage travel on the vehicle.
- Do not leave baggage unattended prior to loading.
- Check passenger lists or ID cards as appropriate.

b. Contract Hire Transport. The term contract hire transport addresses transport hired exclusively for military use and under military control during contract period. Security precautions are the same as those used for military transport.

c. Civil Transport. When civilian firms provide transportation for the use of servicemen and their families, discuss security arrangements with local police. Advise personnel to be alert and vigilant while traveling on civilian transportation, particularly upon returning to major United States installations after recognized breaks such as weekends and holidays. Do not use military rank if making advance bookings.

4. Military Events Open to the Public

Military events open to the public (e.g., displays, tours, open house) either on or off U.S. Marine Corps property are attractive targets. These events afford the terrorist the opportunity to embarrass the military in front of the public. Typical threats include bomb hoaxes to disrupt proceedings, actual bomb attacks, and demonstrations directed against the military. Take special precautions to check the bags of those entering permanent displays (e.g., museums).

The installation physical security council issues a threat assessment and identifies possible countermeasures each time a military open house is planned. All military events open to the public have a security plan. The security plan is discussed with the security staff and local police. The security plan's scope and detail depend upon the size and circumstances of the event and the prevailing threat. Consider the following:

- Establish a joint military/local police security control headquarters.
- Divide the area into sectors and man each sector with a sector control force.
- Inform the PMO, officer of the day, interior guard, and local police of security details.
- Command and local police coordination requirements.
- Search the location before and during the function.
- Brief selected senior ranks and other personnel on the need for vigilance and allocation of security tasks.
- Parking arrangements.
- Safe area in case evacuation is necessary.
- Guard the area before the event's opening, at night, and during the event.
- Control access. Obviously this is difficult when the general public is invited, but spot checks on vehicles and hand-carried articles are generally accepted by the public and act as a deterrent.
- Ensure the security of static displays is normally the responsibility of the organization providing and manning individual displays. Any display of arms or ammunition must be properly secured and guarded.
- Contingency plans for potential demonstrations, evacuations, and the possibility of the threat condition being raised.
- Closing activities and clearing the public in time for a thorough search to be made before dark.

All publicly announced military events (e.g., recruiting activities, band concerts, sports events, social functions, reunions) attended by regular, reserve, cadets, or retired Service personnel should have the prior knowledge and approval of local police. This applies to military events on or off United States property, events open or closed to the public, and events the public may know of in advance. Event sponsors provide advance notice to higher headquarters. This notice includes all relevant details and the name and telephone number of the sponsor. Headquarters informs local police and obtains required approval. This procedure does not apply to military events which are not publicly announced.

Appendix K

Postal Bombs

Warning Signs

Suspicious postmark or return address.
Unusual or foreign handwriting.
Lopsided or unbalanced package or letter.
Excessive weight in comparison to package size. Effective postal bombs weigh more than 2 ounces and require additional postage.
Protruding wires.
Small hole in the package or envelope.
Grease marks (from the sweating of explosives).
Smell of almonds or marzipan.
Completely sealed envelope flap (usually there is an ungummed gap of about 1/8 inch).
Touching indicates stiffening material or metal.
Unusually thick letters; e.g., 3/16 inch or more.
If upon opening an envelope, another personally addressed or tightly sealed envelope is found.

Upon receipt of a suspicious package/letter, place the package/letter on the nearest horizontal, firm surface. Keep face and body shielded. Place the package/letter behind a substantial object (e.g., steel filing cabinet) or use a wall as a barrier and place the item gently on the floor around the corner of a door. Keep the movement of any suspicious package/letter to a minimum to reduce premature detonation. Under no circumstances should a suspicious package/letter be tampered with by untrained personnel.

WARNING

Do not take a suspicious package/letter to local police or security officer. Do not place the package/letter outside in the street, in a bucket of water, or cover with sand. These actions can increase the probability of detonation.

Upon receipt of a suspicious package/letter, order all personnel to leave the room as quickly as possible, Make no attempt to open the package/letter, and leave the room. If possible, open the windows before leaving but do not endanger yourself. Leave the door open and unlocked to assist EOD personnel upon their arrival. Call local police or PMO immediately. Prevent personnel from entering the room until local police or PMO take control of the situation.

Appendix L

Telephone Call Procedures

Upon receiving an anonymous telephone call:

Try to keep a word for word record of the conversation.

Attempt to obtain the name of the caller, address, and telephone number or a contact point. Point out to the caller that by giving these details he is indicating that it is a genuine warning.

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

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

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

If the threat contains a codeword, verify the codeword with local police or the PMO immediately.

During the call, try to obtain answers to the questions listed on the telephone threat information sheet located on the back of this page.

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?

After providing the duty officer/PMO with details of the telephone call, 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 PMO or local police.

Telephone Threat Information Sheet

Which unit or installation is involved? _____

_____

Nature of the threat. _____

_____

Time or period of the threat. _____

_____

Who made the threat? _____

_____

Voice characteristics:

Was the tone normal? _____

Did it sound disguised or muffled? _____

Was it high-pitched or stuttering? _____

Did it sound nervous? _____

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

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

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

Did the voice have a pronounced or recognizable accent? _____

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

Were there background noises? _____ If so,

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

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

Did the caller display a detailed knowledge; e.g., role or layout of the unit or establishment? _____

Appendix M

Procedures for Drivers

Drivers in high-risk areas must be alert and able to respond skillfully if confronted. Prepare for explosive devices or firearm attacks while on the move. Remember, if the passenger is a target, then so is the driver. The best defense is common sense, alertness, and skill.

Preventive Tactics

Lock the car when not in use.

Do not leave parcels and other items in the car.

Lock the trunk and gas cap.

Avoid leaving the car unattended in the open.

Do not sit in the car while waiting. Observe the car from a distance so there is a complete view of the area.

Avoid using the same route and daily schedule.

Avoid isolated roads.

Detour suspicious cars.

Continually check to ensure you are not being followed. Warn the passenger if detouring to check on suspicious cars.

Be vigilant when stopped.

Be alert to unknown persons standing or working and occupied cars parked near the journey's starting point.

Note description of suspicious people and vehicles (registration number, type, color, etc.).

Stop short of any unusual object or incident.

Searching the Car

If the car is left for any length of time, search before using. Suspicions should be aroused by unusual objects in the car; objects out of place; outward signs of tampering; loose wiring, string, or tape; packages left under the vehicle; or ground disturbed around the vehicle. Perform the following full search procedures before entering a vehicle:

- Look carefully around the outside of the vehicle.
- Look through all windows.
- Check around and behind each wheel.
- Remove hub caps and examine.
- Look under the car (particularly exhaust and behind gas tank) using an angled mirror on a stick if available.
- Open the driver's door.
- Check the driver's seat, floor, and controls.
- Check all doors before opening.
- Examine seats and floors.
- Open and inspect the trunk.
- Examine the spare wheel.
- Check all tools.
- Open hood carefully and examine the engine compartment.

If the driver finds a suspicious device, do not touch it or attempt to start or move the car. Call the PMO or local police. Remember that boobytraps are set with more than one means of detonation. Common methods of vehicle detonation include—

- Pressure switch under a wheel, seat cushion, or pedal.
- Trembler switch activated by movement.
- Tilt switch (also called a mercury switch) activated by rotary motion (e.g., braking) or inclination.
- Heat switch attached to the exhaust manifold or exhaust pipe.
- Peg switch attached to a door or throttle.
- Cable switch attached to a mechanical trigger.
- Timing device.
- Remote-control device.

FMFRP 7-37, *Vehicle Bomb Search*, contains additional information. FMFRP 7-37 should be located in every Marine Corps vehicle.

Attacked While on the Move

If attacked while on the move, safe driver training may have to be forgotten. Protecting the passenger's life is paramount. Damage to the car is trivial when compared to the possibility of being taken hostage or losing lives. If followed:

- Drive to a police station or service establishment.
- Remain on busy streets.
- Do not get boxed in.
- Keep distance from obstacles.
- Ensure adequate space for fast getaway.

If threatened, close all windows, switch on the headlights and hazard warning lights, use the horn to draw attention, and hide important papers. The advantages and disadvantages of various courses of action may have to be balanced during critical situations. For example, it may be better to accelerate out of danger and then stop suddenly followed by a quick turn in order to outwit a terrorist. It is essential that the driver can accurately judge the car's dimensions, know the extent of damage the car can sustain, and know how to exploit the car's acceleration and turning capabilities.

Appendix N

Assassination Threat Procedures

Personnel in high-risk areas may be the object of attack or receive threats. To ensure safety, personnel in high-risk areas must be aware of the threat level and the appropriate response. Responsibility for individual protection depends on the location, the threat, and the individual involved. If CONUS, local police provide protection to the individual. If OCONUS, United States military and host nation forces provide protection to the individual. If the individual is a member of the military, provide protection with a combination of local and military forces. The following procedures provide guidance when responding to a terrorist threat.

Warning Typically, threats against individuals are received by either local police, Marine Corps intelligence and security sources, or directly from the terrorist.

Reaction to Warning Upon receipt of threat, contact the proper authorities. Take protective measures. Proper authorities check the validity of the threat through normal security channels, perform an assessment, determine responsive actions, provide armed escorts and sentries.

Control of Movement If possible, threatened individuals travel outside their place of duty by helicopter or civilian car. Protective escorts accompany any travel movement. If a staff car is used, change vehicles frequently and do not display flags. Examine vehicles before use.

Physical Security Personnel identified as high-risk are afforded the maximum security measures available to protect the individual and the family.

Publicity Typically, assassination threats recede with time if the threatened individual maintains a low profile and avoids all forms of publicity; e.g., authorship of books, lectures, public appearances.

Appendix O

Explosive Device Procedures

Response to a Suspected Improvised Explosive Device

Suspicion

Suspicion that an improvised explosive device (IED) is within an establishment often stems from a threatening anonymous telephone call. Take these calls seriously even though subsequent investigation proves it to be a false alarm or hoax. Appendix L provides advice on handling anonymous telephone calls.

Immediate Action

Upon receiving an anonymous warning or threat, notify the PMO or police immediately. Local SOPs determine subsequent actions. Immediate action includes search without evacuation, movement of personnel within the establishment, partial evacuation, or total evacuation.

Factors favoring a search before movement of personnel:

- High incidence of hoax telephone threats.
- Establishment has effective security arrangements.
- Information in the warning is imprecise or incorrect.
- Caller sounded intoxicated, amused, or very young.
- Prevailing threat of terrorist activity is low.

Factors favoring movement of personnel before searching:

- Establishment is comparatively open.
- Information in the warning is precise as to matters of location, description of device, timing, and motive for attack.
- Prevailing threat of terrorist activity is high.

Searching for a Suspected IED

Types

Use a nominated persons search when the threat's credibility is very low. The search is superficial. Predesignated individuals search assigned areas. The search can be achieved covertly.

Use an occupant search when the threat's credibility risk is low. Occupants search their own areas. The search is completed quickly because occupants know their area and are most likely to notice anything unusual.

Use a team search when the threat's credibility is high. The search is thorough and places the minimum number of personnel at risk. Completely evacuate the area. The area remains evacuated until the search is complete. Search teams make a systemic search of the area. The search is slow, but the results are accurate.

Search Procedures

Make an audio check, listen for unusual sounds.

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

Perform a thorough and systematic search in and around containers and fixtures.

Pass search results as quickly as possible to the leader responsible for controlling the search area.

Search Organization

The person controlling the search should possess a means of tracking and recording the search results; e.g., diagram of the area. Delegate areas of responsibility to search team leaders. Search team leaders report to the person controlling the search when their areas have been cleared. Pay particular attention to entrances, toilets, corridors, stairs, unlocked closets, storage spaces, rooms and areas not checked by usual occupants, external building areas, window ledges, ventilators, courtyards, and spaces shielded from normal view.

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.

Alarm System

Bomb threat alarm systems should be easily distinguished from the fire alarms.

Assembly Areas

Assembly areas are preselected and well-known to personnel. Establish a clearly defined procedure for the controlling, marshalling, and checking personnel within the assembly area. If buildings or establishments are in a public area, coordinate assembly areas with local police.

Assembly areas are chosen with the following considerations:

- Assembly areas should be 200 meters, and not less than 100 meters, from the likely target or building if possible.
- Locate assembly areas in areas where there is little chance of an IED being hidden. Open spaces are best. Avoid car parking areas because IEDs can easily be hidden in vehicles.
- Select alternate assembly areas in the case of inclement weather. Search the assembly area before personnel occupy the space.
- Assembly areas should not be near expanses of plate glass or windows. Blast effects can cause windows to be sucked outward rather than blown inward.

Routes to Assembly Areas

Choose routes to the assembly area so personnel do not approach the IED at any time. Preselect routes to the assembly area, but devise a system to inform personnel of the location of the suspected IED and alternate routes. Routes prevent confusion and bunching and avoid potential hazards (e.g., plate glass, windows, likely locations of additional IEDs).

Personnel Evacuation Response

Upon hearing the alarm, personnel secure all classified documents, carry out a quick visual search of their immediate working area, open windows wherever possible, leave the building, take personal belongings, leave doors open, and proceed to the assembly area.

Building and Area Clearance

Establish procedures to ensure threatened buildings and areas are cleared and no one re-enters. Establish a cordon to prevent personnel from entering the danger area. Establish an initial control point (ICP) as the focal point for PMO and military police control.

Evacuation Drills

Practice evacuation and search drills periodically under the supervision of the installation's/unit's senior officer. Hold drills in cooperation with local police if possible. Avoid unnecessary alarm to personnel and civilians in adjacent premises.

Incident Control Point and Cordon

Cordon suspicious objects to a distance of at least 100 meters. Cordon suspicious vehicles to a distance of at least 200 meters. No one is permitted to enter the cordon. Establish an ICP on the cordon to control access. Relinquish ICP responsibility to the PMO or local police upon arrival. Maintain the cordon until the PMO or local police have completed their examination or state that the cordon may stand down.

Discovery of a Suspected IED

Do not touch or move a suspicious object. If it is possible that an occupant can explain the object's presence, ask them to identify it with a verbal description. This should not be done if it entails bringing evacuated personnel back into the area.

Take the following actions if an object's presence remains inexplicable:

- Evacuate buildings and surrounding areas, including the search team.
- Evacuated areas must be at least 100 meters from the suspicious object.
- Establish a cordon and ICP.
- Inform the ICP that an object has been found.
- Keep person who located the object at the ICP until questioned.

Reaction to an Exploded IED

Explosion without Casualties

Maintain the cordon. Allow only authorized personnel into the explosion area. Fight any fires threatening undamaged buildings if this can be achieved without risking personnel. Report the explosion to the PMO or local police if they are not yet in attendance. Report the explosion to the installation operations center even if an EOD team is on its way. Give the maximum detail; e.g., time of explosion, number of explosions, color of smoke, speed and spread of fire. Ensure clear passage for fire and ambulance vehicles and personnel. Refer media inquiries to the public affairs office at the operations center. Establish information center to handle inquiries from the next of kin.

Explosion with Casualties

Casualties can be inflicted by an explosion which occurs with little or no warning. The first consideration is the effective, organized search for and evacuation of casualties. Witnesses naturally approach the explosion area to aid in searching for casualties. The senior officer must coordinate the search and keep the number of searchers to a minimum due to the threat of IEDs and secondary effects (e.g., falling masonry, fires). Attempt to prepare an accurate casualty list for notification of next of kin. Remember, it is better to release an accurate list of casualties a little later than an incorrect list quickly. Arrange for unaffected personnel to contact their next of kin quickly.

Assisting the Threat Management Team

Reporting

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:

- Was a warning received? If so, how was it received?
- Who discovered the device?
- How was the device discovered (e.g., casual discovery, organized search)?
- Identify location of the device. Give as much detail as possible.
- Time of discovery.
- Estimate the length of time the device has been in the discovered position.
- Describe the device in as much detail as possible.
- Safety measures taken.
- Suggested routes to the scene.
- Any other pertinent information (e.g., background history).

Access

Upon arrival, ensure PMO, local police, and EOD vehicles are not impeded from reaching the ICP.

During evacuation, leave doors and windows of buildings.

Obtain diagrams of building if possible. If available, obtain detailed plans of the public service conduits (e.g., gas, electricity, central heating). If unavailable, a sketch can be drawn by someone with detailed knowledge of the building.

Witnesses are invaluable and should be on hand when military and local police arrive. Witnesses include the person who discovered the device, witnessed the explosion, or possess detailed knowledge of the building or area.

Appendix P

Crisis Management Plan Format

CLASSIFICATION

Copy no._____of_____copies
Issuing Headquarters
Location
Date/time group

Ref: (a) Maps, charts, and other relevant documents.

Time Zone: X

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

1. SITUATION

(Identify essential information in order to understanding ongoing events.)

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

b. CMF. (Explain CMF abilities and responsibilities. CMF ability can influence the crisis management mission.)

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

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

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

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

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

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

(Page number)

CLASSIFICATION

CLASSIFICATION

2. MISSION

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

3. EXECUTION

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

b. Tasks. (Identify specific tasks for each element of the command charged with executing a crisis management mission. When giving multiple instructions, itemize and indicate priority or sequence [e.g., Commander, MP Company provides a one-platoon ready reaction force].)

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

4. SERVICE SUPPORT

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

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

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

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

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

(1) Maintenance of Unit Strength

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

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

(Page number)

CLASSIFICATION

CLASSIFICATION

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

(3) Development and Maintenance of Morale

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

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

(4) Maintenance of Discipline, Law, and Order. (Provided by PMO.)

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

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

5. COMMAND AND SIGNAL

(Provide instructions for command and operation of communications-electronics. Communications-electronics instructions may refer to an annex, but should list the index and issue number of the C^3 operation instructions in effect. If not already issued, give instructions for control, coordination, and establishment of priorities in the use of electromagnetic emissions. Command instructions include subordinate and higher unit command post locations and designated alternate command posts.)

ACKNOWLEDGEMENT INSTRUCTIONS

/s/Commander

ANNEXES as applicable

DISTRIBUTION:

(Page number)

CLASSIFICATION

Appendix Q

Crisis Management Plan Checklist

The installation/unit commander develops a crisis management contingency plan during the planning phase. Plan for a 7-day duration. The following checklist identifies considerations that should not be overlooked during planning.

Intelligence

Does the plan allow for the intelligence-gathering process (e.g., collection, evaluation, and dissemination of information) to aid in the identification of the local threat? ☐ Yes ☐ No

Does the plan consider restrictions placed on the collection and storage of information? ☐ Yes ☐ No

Does the plan indicate an awareness of sources of information for the intelligence-gathering effort (e.g., military intelligence, federal agencies, state/local authorities)? ☐ Yes ☐ No

Does the plan allow for liaison and coordination of information (e.g., establishing a threat committee)? ☐ Yes ☐ No

Threat Analysis

Does the plan identify the local threat (immediate and long-term)? ☐ Yes ☐ No

Does the plan identify other threats (e.g., national and international groups who have targeted or might target United States installations)? ☐ Yes ☐ No

Does the installation incorporate factors of the installation vulnerability determining system when assessing the threat? Does it address— ☐ Yes ☐ No

- Geography of the area concerned.
- Law enforcement resources.
- Population factors.
- Communication capabilities.

Does the plan establish a priority of identified weaknesses and vulnerabilities? ☐ Yes ☐ No

Security Countermeasures	Does the plan have specified THREATACONS and recommended actions (see MCO 5500.13)?	☐ Yes ☐ No
	Do security countermeasures include a combination of physical operations and sound-blanketing security measures?	☐ Yes ☐ No
OPSEC	Have procedures been established that prevent terrorists from readily obtaining information about plans and operations (e.g. , not publishing the commanding general's itinerary, safeguarding classified material)?	☐ Yes ☐ No
	Does the plan allow for in-depth coordination with the installation's OPSEC program?	☐ Yes ☐ No
	Has an OPSEC annex been included in the contingency plan?	☐ Yes ☐ No
Personnel Security	Has threat analysis identified individuals vulnerable to terrorist attack?	☐ Yes ☐ No
	Has an education process been started that identifies threats to vulnerable personnel?	☐ Yes ☐ No
Physical Security	Are special threat plans and physical security plans mutually supportive?	☐ Yes ☐ No
	Do security measures establish obstacles to terrorist activity (e.g., guards, intrusion detection systems, lighting, fencing)?	☐ Yes ☐ No
	Does the special threat plan include the threats identified in the threat statements of higher headquarters?	☐ Yes ☐ No
	Does the physical security officer assist in the threat analysis and corrective action?	☐ Yes ☐ No
	Is there obvious command interest in physical security?	☐ Yes ☐ No
Security Structure	Does the plan indicate that the FBI primary investigative and operational responsibility?	☐ Yes ☐ No
	Has coordination with the staff judge advocate been established?	☐ Yes ☐ No
	Does the plan allow for close cooperation between principle agents of the military and civilian communities and federal agencies?	☐ Yes ☐ No

	Does the plan clearly indicate parameters for use of force, including the briefing of any elements augmenting military police assets?	☐ Yes ☐ No
	Is there a mutual understanding between all local agencies (e.g., military, local FBI resident or senior agent-in-charge, and local law enforcement) that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction?	☐ Yes ☐ No
	Has the staff judge advocate considered ramifications of closing the post (e.g., possible civilian union problems)?	☐ Yes ☐ No
CMT Training	Has the CMT been established and exercised?	☐ Yes ☐ No
	Is the CMT based on the needs (e.g., recognizing manpower limitations, resource availability, equipment, and command) of the installation?	☐ Yes ☐ No
	Does the plan include a location for the CMT?	☐ Yes ☐ No
	Does the plan designate alternate locations?	☐ Yes ☐ No
	Does the plan allow for the use of visual aids (e.g., chalkboards, maps with overlays, bulletin boards) to provide situation status reports and countermeasures?	☐ Yes ☐ No
Reaction Force Training	Has the force been trained and exercised under realistic conditions?	☐ Yes ☐ No
	Has corrective action been applied to shortcomings/ deficiencies?	☐ Yes ☐ No
	Has the reaction force been formed and mission-specific trained (e.g., building entry and search techniques, vehicle assault operations, antisniper techniques, equipment)?	☐ Yes ☐ No
	Has the reaction force been tested quarterly (alert procedures, response time, overall preparedness)?	☐ Yes ☐ No
	Has responsibility been fixed for the negotiation team?	☐ Yes ☐ No
	Has the negotiation team been trained and exercised under realistic conditions?	☐ Yes ☐ No
	Does the negotiation team have the proper equipment?	☐ Yes ☐ No

General Observations

Was the plan developed as a coordinated staff effort?	☐ Yes ☐ No
Does the plan outline reporting requirements (e.g., logs, journals, after-action report)?	☐ Yes ☐ No
Does the plan provide for public affairs office support?	☐ Yes ☐ No
Does the plan address controlled presence of the media?	☐ Yes ☐ No
Does the plan include communications procedures/communications nets?	☐ Yes ☐ No
Does the plan consider the possible need for interpreters?	☐ Yes ☐ No
Does the plan consider the need for a list of personnel with various foreign backgrounds to provide cultural intelligence on foreign subjects and victims, as well as assist with any negotiation efforts?	☐ Yes ☐ No
Does the plan provide for and identify units that will augment military police assets?	☐ Yes ☐ No
Does the plan delineate specific tasking for each element of the command?	☐ Yes ☐ No
Does the plan provide for a response for each phase of counterterrorist activity (e.g., initial response, negotiation, assault)?	☐ Yes ☐ No
Does the plan note service support requirements (e.g., engineer, aviation, medical, communications, etc.)?	☐ Yes ☐ No
Does the plan make provisions for notification of nuclear assessment teams and nuclear accident/incident control officer?	☐ Yes ☐ No
Does the plan take into consideration the movement from various locations of civilian and military advisory personnel with military transportation assets, such as commercial airports?	☐ Yes ☐ No
Does the plan allow for the purchase and/or use of civilian vehicles, supplies, food, etc., if needed or as a hostage demand?	☐ Yes ☐ No
Does the plan make provisions for paying civilian employees overtime if they are involved in a special threat situation?	☐ Yes ☐ No
Does the plan take into consideration the messing, billeting, and transportation of civilian personnel?	☐ Yes ☐ No

Appendix R

Public Affairs Checklist

Because terrorists play to the media for recognition, the flow of information to the media must be in the best interest of the hostage and the situation. The staff judge advocate and the installation commander screen information to the media to ensure operational security and protect the command's legal position.

Never allow the media to become a vehicle for debriefing terrorists after an operation. Widespread dissemination of lessons learned and friendly operational procedures prepare the terrorist for his next attack. Make every effort to deny the terrorist the ability to manipulate the media to his own ends.

The following checklist contains the duties and responsibilities of the public affairs officer:

- ☐ Check with the G-3/S-3 upon entering the operations center.
- ☐ Establish a public affairs plan.
- ☐ Disseminate information to the news media in accordance with the established plan.
- ☐ Control press releases.
- ☐ Coordinate press releases with G-3/S-3.
- ☐ Control movement of news media personnel with press passes, escorts, etc.
- ☐ Obtain approval for the following items from the installation commander:
  - News releases.
  - News media personnel to enter outer perimeter.
  - Release of photographs of suspects, victims, and immediate scene.
  - Interviews with anyone other than the commander.
  - Direct communication with press personnel and suspect(s).

Appendix S

Glossary

Section I. Acronyms

AA&E ..... arms, ammunition, and explosives
ACE ..... aviation combat element
ANGLICO ..... air/naval gunfire liaison company
ATAC ..... Antiterrorism Alert Center
ATACSUM ..... ATAC Summary

CID ..... Criminal Investigation Division
CONUS ..... Continental United States
CMC ..... Commandant of the Marine Corps
CMF ..... crisis management force
CMT ..... crisis management team
CSSE ..... combat service support element

DOD ..... Department of Defense
DOJ ..... Department of Justice
DON ..... Department of Navy
DOS ..... Department of State

EEFI ..... essential elements of friendly information
EOD ..... explosive ordnance disposal

FAA ..... Federal Aviation Administration
FBI ..... Federal Bureau of Investigation
FMF ..... Fleet Marine Force

GCE ..... ground combat element

HEAT ..... high explosive antitank
HMMWV ..... high mobility multipurpose wheeled vehicle
HNT ..... hostage negotiations team
HQMC ..... Headquarters, U.S. Marine Corps

IAW ..... in accordance with
ICP ..... initial control point
IED ..... improvised explosive device
IVA ..... installation vulnerability assessment

JCS ..... Joint Chiefs of Staff

LAV ..... light armored vehicle
LVT97 ..... amphibious tractor

MAGTF ..... Marine Air-Ground Task Force
MCCC ..... Marine Corps Command Center
MCCDC ..... Marine Corps Combat Development Command
MCCRES ..... Marine Corps Combat Readiness Evaluation System
METT-T ..... mission, enemy, terrain, troops-time
MEU ..... Marine expeditionary unit
MEU(SOC) ..... MEU (special operations capable)
MOU ..... memorandum of understanding
MWD ..... military working dog

NBC ..... nuclear, biological, and chemical
NCA ..... National Command Authorities
NCO ..... noncommissioned officer
NIS ..... Naval Investigative Service
NISCOM ..... Naval Investigative Service Command
NISRA ... Naval Investigative Service Resident Agency
NMCC ..... National Military Command Center
NSC ..... National Security Council

OCONUS .... outside the Continental United States
OP ..... observation post
OPSEC ..... operations security

PMO ..... provost marshal office

ROE ..... rules of engagement

SAC ..... special agent in charge
SOFA ..... status-of-forces agreement
SOP ..... standing operating procedure
SRT ..... Special Reaction Team
SWAT ..... Special Weapons and Tactics Team

THREATCON ..... terrorist threat conditions

U.S. ..... United States
USA ..... United States Army
USAF ..... United States Air Force

VIP ..... very important person

Section II. Definitions

The use of and adherence to precise, approved, and understood military terminology is of paramount importance and of critical concern in all doctrinal publications. Unless identified as extracted from Joint Pub 1-02, terminology in this document is not standard within the Department of Defense and is applicable only in the content of this document.

A

antiterrorism — Defensive measures used to reduce the vulnerability of individuals and property to terrorism. (Joint Pub 1-02)

C

combating terrorism — Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) taken to oppose terrorism throughout the entire threat spectrum. (Joint Pub 1-02)

counterterrorism — Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT. (Joint Pub 1-02)

crisis management force — An installation's assets capable of reacting to an incident.

crisis management team — Team established at each Marine Corps installation. During heightened THREATCONS, the crisis management team becomes a temporary installation command element and initiates and coordinates all combating terrorism efforts aboard the installation and acts on behalf of the installation commander.

crusaders — Ideologically motivated terrorists.

D

deterrence — The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

H

high-risk personnel — Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.

hostage — A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Convention 1949). (Joint Pub 1-02)

I

initial control point — A designated point close to a terrorist incident where crisis management forces will rendezvous and establish control capability prior to initiating a tactical reaction.

in-flight — Period of time all external aircraft doors are closed and embarkation is complete, and continues until aircraft doors are opened for disembarkation.

initial response force — The first unit, usually military police, on the scene of a terrorist incident.

installation — A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

installation commander — The individual responsible for all operations aboard a military base or station.

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

insurgent — Member of a political party who rebels against established leadership.

K

kidnap insurance – Insurance purchased by corporations to insure key personnel working in high-risk, overseas areas.

N

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

negotiations – A discussion between authorities and a barricaded offender/terrorist to effect hostage release and terrorist surrender.

O

open sources of information – Unclassified information available to the public.

operations center – The facility or location on an installation used by the CMT commander to control and coordinate all antiterrorist and counterterrorist activities.

operations security – A process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.
b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Also called OPSEC. (Joint Pub 1-02)

P

physical security – That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

physical security council – A council at the installation, unit, or area level that acts as a permanent working entity to develop, perform, and update overall security plans and programs. The council is representative of the staff and chaired by the Chief of Staff or a unit executive officer.

prevention – The security procedures undertaken by the public and private sector in order to discourage terrorist acts.

primary targets – An object of high publicity value to terrorists.

proactive – Measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur.

R

reaction – The mounting of counterterrorism operations in response to specific acts of terrorism.

reactive – The counterterrorism response to an ongoing terrorist incident includes activation of EOD, deployment of special reaction team, etc.

rear area security – Rear area security includes those measures taken before, during, and/or after an enemy airborne attack, sabotage, infiltration, guerrilla action, and or initiation of psychological or propaganda warfare to minimize the effects thereof. Also called RAS. (FMFRP 0-14)

revolutionary – An individual attempting to effect a social or political change through the use of extreme measures.

S

saboteur – One who commits sabotage.

secondary targets – Alternative targets of lower publicity value. Attacked when primary target is unattainable.

security force – The detachment deployed between the main body and the enemy (to the front, flanks, or rear of the main body) tasked with the protection of the main body. The security force may be assigned a screening, guard, or covering mission. (FMFRP 0-14)

signal security – A generic term that includes both communications security and electronic security. (Joint Pub 1-02)

special reaction team – Any team of military/security personnel specially trained and equipped to tactically neutralize a special threat.

special threat – Any situation involving a sniper, barricade situation, or hostage-taker(s) that requires special reaction/response, manpower, and training.

status-of-forces agreement – An international agreement which determines the legal relationship between the Armed Services of one country and the host nation; determines a standard legal treatment; and provides a basis for solving legal problems raised by the presence of foreign forces abroad.

Stockholm Syndrome – The positive feelings of the hostages toward their captors accompanied by negative feelings toward the police.

T

tactical security – Those measures taken by commanders in a combat zone forward of the ground combat element rear boundary to protect their units from surprise, observation, detection, interference, espionage, and air or ground attack. This includes the integration of covering force, flank, and local security with the conduct of offensive and defensive operations, as well as the local security exercised by command, combat support, and combat service support units behind the lines.

terrorism – The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious or ideological objectives. (Joint Pub 1-02)

terrorist – An individual who uses violence, terror, and intimidation to achieve a result.

terrorist groups – Individuals affiliated by a common cause, usually classified as either crusaders, criminals, or crazies. All such groups unlawfully use threatened force or violence to obtain their objectives.

threat analysis – Analyzing of an installation's vulnerability to a terrorist threat to help uncover and isolate security weaknesses.

threat committee – An ad hoc group addressing threat analysis resulting in centralized efforts to eliminate weaknesses. The committee is made up of anyone possessing skills/knowledge in combating terrorism.

Appendix T

References and Related Technical Publications

Operational Handbooks

OH 3-5	Employment of Military Police in Combat (when revised, will become FMFM 3-5, Employment of Military Police in Combat)

Fleet Marine Force Manuals

FMFM 3-1	Command and Staff Action
FMFM 6-4	Marine Rifle Company/Platoon
FMFM 6-7	Scouting and Patrolling for Infantry Units

Fleet Marine Force Reference Manuals

FMFRP 7-14A	The Individual's Guide for Understanding and Surviving Terrorism
FMFRP 7-37	Vehicle Bomb Search

Marine Corps Orders

MCO 5720.60	Marine Corps Public Affairs Manual, Vol. 1, Community Relations
MCO 5720.61	Marine Corps Public Affairs Manual, Vol. 2, Organization, Mission, and Functions
MCO 3000.8B	Employment of Marine Corps Resources in Civil Disturbances
MCO 5500.14	FLS Prog
MCO 5500.13	Physical Security

Field Manuals

FM 19-15	Civil Disturbances

Joint Publications

Joint Pub 1-02	Department of Defense Dictionary of Military and Associated Terms
Joint Pub 0-2	Unified Action Armed Forces (UNAAF)

Miscellaneous Publications

OPNAVINST 3440.16A	Department of Navy Civil Disaster Assistance Program
OPNAVINST 3100.6E	Special Incident Reporting Procedures

Vol. 41, Opinion Attorney General, p. 330 (1957)
Vol. 16, Opinion Attorney General, p. 162 (1878)

House of Representatives Resolution 1292

Deputy SecDef Memo, Subject: Support of Civil Authorities in Airplane Hijacking Emergencies, 29 June 72

Memorandum of Understanding between the Department of Defense, the Department of Justice, and the Federal Bureau of Investigation (5 Aug 83)

Title 50, U.S. Code, Section 797
Title 49, U.S. Code, Section 1357(e)
Title 10, U.S. Code, Sections 331-334
Title 18, U.S. Code, Sections 112, 231, 351[g], 1361, 1385, 3056
Title 42, U.S. Code, Sections 1989, 4401-84, 1855
Title 21, U.S. Code, Section 873[b]
Title 33, U.S. Code, Section 1362

DOD Directive 3025.12	Employment of Military Resources in the Event of Civil Disturbances (USDP), pars. V.C. and V.C.2a, 19 August 1971
DOD Directive 5525.5	DOD Cooperation with Civilian Law Enforcement Officials (FMFP)
DOD Directive 3025.1	Use of Military Resources During Peacetime Civil Emergencies Within the United States, Its Territories and Possesions (USDP)
DOD Directive 3025.10	Military Support of Civil Defense (USDP)
DOD Directive 2000.12	Protection of DOD Personnel and Resources Against Terrorists Acts (SO/LIC)
SECNAVINST 3850.1A	Protection of DOD Personnel and Resources Against Terrorist Acts
SECNAVINST 5820.7B	Cooperation with Civilian Law Enforcement Officials; Posse Comitatus Act
SECNAVINST 3050.32	Employment of Naval Resources in National Disasters, Emergencies Within the United States, Its Territories, and Possessions

Index

	Paragraph	Page
A		
Assassination threat procedures	App. N	N-1
ATAC documents	Table 3-1	3-2
Authority, terrorist incident	App. A	A-4
C		
Civil requests for use of Marine Corps resources	App.A	A-6
Commandant of the Marine Corps	2004a	2-5
Commanding General, MCCDC	2004a	2-5
Crisis management		
After-action report	6011	6-6
Communication requirement	5006	5-10
Confirmation	6002	6-1
Establish communications	6008	6-5
Identify inconsistencies	6007	6-5
Initial response	6001	6-1
Initial response force	6001a	6-1
Installation commander	6001b	6-1
Obtain evidence	6009	6-5
Preparation	6004	6-2
Multiple incidents	6004a	6-2
Prolonged incidents	6004b	6-2
Public affairs	5007	5-10
Response	6005	6-3
Phase I	6005a	6-3
Phase II	6005b	6-3
Phase III	6005c	6-3
Terrorist incident	6006, Fig. 6-1	6-3, 6-4
Use of force options	6003	6-2
Crisis management force	2004c(2)(b), 5003, Fig. 5-3	2-7, 5-4, 5-5
Reaction element	5003b, Figs. 2-4, 5-4	5-5, 2-8, 5-6
Assault element	5003b(2)	5-5
Mission and responsibilities	5003b(2)(b)	5-6
Organization	5003b(2)(a)	5-5
Headquarters element	5003b(1)	5-5
Mission and responsibilities	5003b(1)(b)	5-5
Organization	5003b(1)(a)	5-5
Negotiations and investigations element	5003b(4)	5-7
Mission and responsibilities	5003b(4)(b)	5-7
Organization	5003b(4)(a)	5-7
Operations element	5003b(3)	5-6
Mission and responsibilities	5003b(3)(b)	5-6
Organization	5003b(3)(a)	5-6

	Paragraph	Page
Crisis management force—Continued		
Security element	5003a	5-4
Mission and responsibilities	5003a(2)	5-4
Organization	5003a(1)	5-4
Support element	5003c	5-8
Mission and responsibilities	5003c(2)	5-8
Organization	5003c(1)	5-8
Crisis management plan	5005	5-8
Contingency planning	5005b	5-8
Ambush	5005b(2)	5-9
Arson	5005b(6)	5-10
Attack	5005b(2)	5-9
Bombings	5005b(1)	5-9
Hijacking	5005b(3)	5-9
Hostage/barricade situation	5005b(5)	5-9
Hostage intelligence	5005b(5)(a)	5-9
Organization of information (*See also* terrorist classification sheet.)	5005b(5)(c)	5-10
Physical surroundings	5005b(5)(b)	5-9
Kidnapping	5005b(4)	5-9
Skyjacking	5005b(3)	5-9
Planning, objectives, and responsibilities	5005a	5-8
Crisis management plan checklist	App. Q	Q-1
Crisis management plan format	App. P	P-1
Crisis management team	2004c(2), 5002, 6001c	2-7, 5-3, 6-1
Procedures	5002b	5-3
Specific duties	5002a	5-3

D

Department of Defense, memorandum of understanding	App. B	B-1
Department of Justice, memorandum of understanding	App. B	B-1
Disposition of apprehended personnel	6010	6-5
Drivers, procedures	App. M	M-1
Attacked while on the move	App. M	M-2
Preventive tactics	App M.	M-1
Vehicle searches	4202a, App. M Fig. 4-4	4-13, M-1, 4-14

E

Entryway safety factors	App. I	I-1
Doors	App. I	I-2
Hinges	App. I	I-3
Sliding glass doors	App. I	I-3
Striker plates	App. I	I-2
Windows	App. I	I-1

	Paragraph	Page
Essential elements of information	3002	3-3
Explosive device procedures	App. O	O-1
Evacuation procedures	App. O	O-2
Incident control point and cordon	App. O	O-3
Suspected IED	App. O	O-1
Discovery	App. O	O-3
Response	App. O	O-1
Searching	App. O	O-1
Threat management team, assisting	App. O	O-4
F		
Federal Bureau of Investigation, memorandum of understanding	App. B	B-1
Fortification material	Table 4-3	4-7
I		
Incident response phases	5001	5-1
CONUS	5001a, Fig. 5-1,	5-1, 5-2
Phase I	5001a(1)	5-1
Phase II	5001a(2)	5-1
Phase III	5001a(3)	5-1
OCONUS	5001b, Fig. 5-2	5-2
Phase I	5001b(1)	5-2
Phase II	5001b(2)	5-2
Phase III	5001b(3)	5-2
Reactive capability	5001c	5-2
Type A	5001c(1)	5-2
Type B	5001c(2)	5-3
Type C	5001c(3)	5-3
Type D	5001c(4)	5-3
Individual security precautions in high-risk areas	App. F	F-1
Personal security measures	App. F	F-1
Security during travel	App. F	F-2
Installation vulnerability assessment	App. E	E-1
Intelligence indicators	Table 4-2	4-2
Intelligence support	3001	3-1
Expeditionary operations	3001c	3-3
Information sources	3001b, Table 4-1	3-2, 4-2
Criminal information	3001b(2)	3-3
Intelligence	3001b(3)	3-3
Open sources	3001b(1)	3-2
Subordinates, reports	3001b(4)	3-3
Organization sources	3001a	3-1
Adjacent headquarters	3001a(7)	3-2
Fleet or joint force intelligence	3001a(3)	3-1
Higher headquarters	3001a(7)	3-2
Host nation support	3001a(2)	3-1

	Paragraph	Page
Intelligence support—Continued		
HQMC, Intelligence Division, Counterintelligence	3001a(6)	3-2
Marine Corps Counterintelligence Teams/Representatives	3001a(5)	3-1
Naval Investigative Service Command (*See also* ATAC documents.)	3001a(4)	3-1
Subordinate headquarters	3001a(7)	3-2
U.S. Embassy	3001a(1)	3-1
Interior guard	5004	5-8
J		
Jurisdiction, terrorist incidents	App. A, Table 2-1	A-4, 2-2
L		
Legal considerations	App. A	A-1
Lock security	App. I	I-1
Lock selection guidelines	App. I	I-5
Locking mechanisms	App. I	I-3
Cylinder dead bolt locks	App. I	I-5
Cylindrical lock sets, dead bolt functions	App. I	I-4
Cylindrical locks	App. I	I-3
Mortise locks	App. I	I-4
Rim locks	App. I	I-4
M		
Marine Corps role	2004	2-5
Command antiterrorism program	2004b, Fig. 2-2	2-5, 2-6
Education and training	2004d	2-8
Installation commander	2004c, Fig. 2-3	2-6, 2-7
Crisis management team	2004c(2)	2-7
Crisis management force	2004c(2)(b), Fig. 2-4	2-7, 2-8
Operations center	2004c(2)(a)	2-7
Operational commander	2004c(3)	2-7
Physical security council	2004c(1)	2-6
Tenant commander	2004c(3)	2-7
Structure	2004a	2-5
Memorandum of understanding (*See also* Department of Defense, Department of Justice, and Federal Bureau of Investigation.)	App. B	B-1
Military responsibility	2003	2-4
CONUS off-base incidents	2003b	2-4
CONUS on-base incidents	2003a	2-4
OCONUS off-base incidents	2003d, App. A	2-4, A-6
OCONUS on-base incidents	2003c	2-4
N		
National response	Chapter 2	2-1
Nature of the threat	Chapter 1	1-1

	Paragraph	Page
O		
Office procedures	App. H	H-1
Controlling entry	App. H	H-3
Emergency preparation	App. H	H-4
Office accessibility	App. H	H-1
Personnel procedures	App. H	H-2
Physical security measures	App. H	H-2
Policing the area	App. H	H-4
Public areas	App. H	H-4
Operations security (*See also* intelligence indicators.)	4102	4-1
P		
Personnel security	4104	4-3
Individual protective measures	4104b	4-4
Prevention	4104a	4-4
Security precautions	4104c	4-4
High-risk personnel	4104c(1)	4-4
Individual travel	4104c(2)	4-5
Liberty parties	4104c(3)	4-5
Physical security	4103	4-3
Physical security plan format	App. C	C-1
Postal bombs	App. K	K-1
Preventive security measures	Section I	4-1
Protecting security operations	Section II	4-6
Air movement	4201f	4-10
Observation posts in urban areas	4201i	4-12
Orders	4201i(2), Fig. 4-3	4-13
Planning	4201i(1)	4-12
Rail movement	4201d	4-9
Road movement	4201c	4-8
Convoys	4201c(3)	4-9
Advanced guard	4201c(3)(a)	4-9
Convoy orders	4201c(3)(d), Fig. 4-2	4-9, 4-10
Main body escort	4201c(3)(b)	4-9
Reaction or strike group	4201c(3)(c)	4-9
Sea movement	4201e	4-9
Sentries in urban areas	4201b	4-8
Urban installations	4201a	4-6
Develop security plan	4201a(2)	4-6
Establish defense	4201a(3)	4-7
Estimate situation	4201a(1), Fig. 4-1	4-6, 4-7

	Paragraph	Page
Protecting security operations—Continued		
Urban patrolling	4201g	4-10
Foot patrols	4201g(1)	4-11
Covering fire	4201g(1)(b)	4-11
Formations	4201g(1)(a)	4-11
Hard targeting	4201g(1)(c)	4-11
Obstacle crossing	4201g(1)(d)	4-11
Vehicle patrols	4201g(2)	4-11
Urban roadblocks	4201h	4-11
Communications	4201h(7)	4-12
Concealment	4201h(1)	4-12
Construction and layout	4201h(3)	4-12
Equipment	4201h(5)	4-12
Legal issues	4201h(8)	4-12
Manning	4201h(4)	4-12
Security	4201h(2)	4-12
Surveillance	4201h(6)	4-12
Public affairs checklist	App. R	R-1
R		
Rear area security	4101	4-1
S		
Searches	4202	4-13
Houses	4202c, Fig. 4-5	4-15, 4-16
Occupied	4202c(1)	4-15
Approach	4202c(1)(a)	4-15
Entry	4202c(1)(a)	4-15
Search	4202c(1)(a)	4-15
Exit procedures	4202c(1)(b)	4-15
Unoccupied	4202c(2)	4-15
Approach	4202c(2)(a)	4-15
Boobytraps	4202c(2)(b)	4-17
Entry	4202c(2)(a)	4-15
Search	4202c(2)(a)	4-15
Military working dog teams	4202e	4-17
Personnel	4202b	4-13
Detailed body search	4202b(2)	4-15
Frisk	4202b(1)	4-13
Quick body search	4202b(1)	4-13
Search operation orders	4202d, Fig. 4-6	4-17, 4-18
Vehicle	4202a, App. M, Fig. 4-4	4-13, M-1, 4-14
Senior officer's security measures	App. G	G-1
Children	App. G	G-3
Home	App. G	G-1

	Paragraph	Page
Senior officer's security measures—Continued		
Official functions	App. G	G-2
Private functions	App. G	G-2
To and from work	App. G	G-2
Travel	App. G	G-3
Soft target procedures	App. J	J-1
Individuals	App. J	J-2
Married quarters	App. J	J-2
Householder	App. J	J-2
Military warden scheme	App. J	J-2
Security in public places	App. J	J-2
Installations/units	App. J	J-1
Installation/unit security plan	App. J	J-1
Liaison	App. J	J-2
Responsibility	App. J	J-1
Unit security	App. J	J-2
Military events open to the public	App. J	J-3
Transportation	App. J	J-3
Civil transport	App. J	J-3
Contract hire transport	App. J	J-3
Parking passenger-carrying military vehicles	App. J	J-3
T		
Tactical responses	4203	4-17
Ambushes	4203a	4-17
Ambush orders	4203a(3), Fig. 4-7	4-19
Failure, causes	4203a(2)	4-19
Urban ambushes	4203a(1)	4-17
Bomb explosion or discovery	4203d	4-21
Riot control	4203b	4-20
Advance	4203b(5)	4-20
Deploy	4203b(2)	4-20
Dominate the area	4203b(7)	4-20
Give warning	4203b(3)	4-20
Make arrests	4203b(6)	4-20
Return control to civil authorities	4203b(8)	4-21
Take pictures	4203b(4)	4-20
Talk	4203b(1)	4-20
Withdraw	4203b(8)	4-21
Urban shootings	4203c	4-21
Tactical security	4101	4-1
Telephone call procedures	App. L	L-1
Terrorism goals	Chapter 1	1-1
Terrorism today	1001	1-1
Terrorist classification sheet	Fig. 5-5	5-11

	Paragraph	Page
Terrorist group organization	1003, Figs. 1-1, 1-2	1-2
Active cadre	1003b	1-2
Active supporters	1003c	1-3
Hardcore leaders	1003a	1-2
Passive supporters	1003d	1-3
Terrorist operations	1004	1-3
Aircraft theft	1004d	1-3
Ambush	1004f	1-3
Arson	1004b	1-3
Assassination	1004m	1-4
Explosives	1004a	1-3
Extortion	1004j	1-4
Hostage-taking	1004h	1-4
International narcotics support	1004i	1-4
Kidnapping	1004g	1-3
Marjacking	1004e	1-3
NBC attack	1004l	1-4
Psychological terror	1004k	1-4
Robbery	1004j	1-4
Skyjacking	1004d	1-3
Vehicle theft	1004c	1-3
Terrorist profile	1002	1-2
Terrorist tactics and training	1005	1-4
Terrorist targets	1006	1-4
Threat estimates	3003, Fig. 3-1	3-3, 3-4
Installation/unit assessment	3003b	3-4
Criticality assessment	3003b(2)	3-5
Damage control assessment	3003b(3)	3-5
Installation vulnerability assessment	3003b(1)	3-5
Recovery procedures assessment	3003b(4)	3-5
Mission	3003a	3-4
Terrorist vs. friendly vulnerabilities and capabilities	3003d	3-6
Threat assessment	3003c	3-5
THREATCON system	App. D	D-1
Tri-level concept	2002	2-2

U

United States		
Antiterrorism policy	2002	fig 2-1
Constitutional	App. A	A-2
Emergency authority	App. A	A-2
Federal property, protection	App. A	A-2
Department of Defense	2001c, App. A	2-2, A-5
MCCC	2001c, 2004a, App. A	2-2, 2-5, A-5
NCA	2001a	2-1
NMCC	2001c	2-2

	Paragraph	Page
United States—Continued		
Department of Justice	2001a, App. A	2-1, A-4
FBI	2001a, App. A	2-1, A-5
Department of State	2001b	2-2
Jurisdictional authority	Table 2-1	2-2
Military response	App. A	A-1
Policy	2001, App. A	2-1, A-1
Responsibility	App. A	A-1
Statutory	App. A	A-2
Contingencies, specified	App. A	A-3
Domestic emergencies	App. A	A-3
Public order, restore/maintain	App. A	A-2
Public safety	App. A	A-3

☆U.S. GOVERNMENT PRINTING OFFICE:2000-517-712/94634