



UNITED STATES MARINE CORPS

HEADQUARTERS MARINE CORPS AIR STATION MIRAMAR
PO BOX 452000
SAN DIEGO CA 92145-2000

StaO P3302.1

G-3

11 FEB 2002

STATION ORDER P3302.1

From: Commanding General
To: Distribution List

Subj: ANTI-TERRORISM/FORCE PROTECTION (AT/FP) PLAN

Ref: (a) OPNAVINST 5530.13B
(b) DOD Inst. 2000.16
(c) MCO 5740.2F
(d) MCO P5530.14
(e) MCO 5500.14A
(f) MCO 5500.13A
(g) MCO 3400.3E
(h) MCO 3302.1C
(i) FMFM 7-14 (NOTAL)
(j) StaO P5510.2B

Encl: (1) LOCATOR SHEET

1. Purpose. To establish policy, procedures, responsibilities, and standards for the Anti-terrorism/Force Protection (AT/FP) Plan aboard Marine Corps Air Station (MCAS), Miramar.

2. Cancellation. StaO 3301.1.

3. Policy. It is Marine Corps policy to protect military personnel and civilian employees, their families, government facilities, and material resources from acts of terrorism and other criminal and destructive acts. Commanding Officers must develop an operational capability that provides defense in depth against all threats. Commanding Officers are guided by the provisions of this Order and the references in attaining the measures needed to be both proactive and reactive toward acts of terrorism and other criminal and hostile acts.

4. Background

a. Terrorism as defined in Chapter 19 is the calculated use of violence or threat of violence to inculcate fear. Its intended purpose is to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

11 FEB 2002

b. Acts of terrorism are crimes, and those who perpetrate them are criminals. As criminals, terrorists are not entitled to the protection of the 1949 Geneva Convention on Prisoners of War.

c. With advances in technology and increased availability of resources, terrorist acts have become more deadly and destructive. Consequently, all Marine Corps personnel must be prepared to defend themselves in order to carry out their assigned mission in any environment.

d. The potential for terrorists to strike against our military personnel is a well documented fact and one that is embedded in the history of our Corps. All Marine Corps personnel, military and civilian, must be aware of the terrorist threat. Furthermore, all Marine Corps personnel must possess the knowledge to detect and to defend against acts of terrorism.

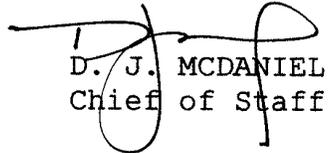
e. The standard Department of Defense (DOD) definition of "Force Protection," which can be found in reference (e) and Chapter 19 of this Order, describes force protection as a security program designed to protect military personnel, civilian employees, family members, facilities, and equipment in all locations and situations. This is accomplished through a planned and integrated application of anti-terrorism, physical security, operational security (OPSEC), personal protective services, and is supported by intelligence, counterintelligence, and other security programs. Anti-terrorism can be defined as defensive measures taken which reduce our vulnerability to terrorist acts and therefore is an integral part of the overall force protection concept.

f. The Marine Corps views force protection as an overarching concept. It includes those procedural, training, equipment and leadership principles necessary to ensure the safety and well being of Marines, family members, and civilian employees.

5. Action. Commanding Officers, Officers in Charge, and Department Heads will comply with this Order and ensure personnel under their cognizance are familiar with the contents of this Order.

11 FEB 2002

6. Concurrence. The Commanding General, 3d Marine Aircraft Wing, and the Commanding Officer, Marine Aircraft Group 46, concur with the provisions of this Order.


D. J. MCDANIEL
Chief of Staff

DISTRIBUTION: A

11 FEB 2002

LOCATOR SHEET

Subj: ANTI-TERRORISM/FORCE PROTECTION PLAN

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

RECORD OF CHANGES

Completed changes as indicated.

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

ANTI-TERRORISM/FORCE PROTECTION PLAN

CONTENTS

CHAPTER

- 1 OPERATIONAL RESPONSIBILITIES/TASKS
- 2 TERRORIST FORCE PROTECTION CONDITIONS
- 3 PROCESS TO RAISE/LOWER FORCE PROTECTION CONDITIONS
- 4 ACTIONS FOR EACH FORCE PROTECTION CONDITION
- 5 CRISIS MANAGEMENT TEAM
- 6 CRISIS MANAGEMENT TEAM MEMBER RESPONSIBILITIES
- 7 PROCEDURES TO COLLECT/ANALYZE THREAT INFORMATION
- 8 VULNERABILITY ASSESSMENTS
- 9 PHYSICAL SECURITY PROCEDURES
- 10 RANDOM ANTI-TERRORISM MEASURES
- 11 SECURITY AUGMENTATION FORCE
- 12 BARRIER PLAN
- 13 WEAPONS OF MASS DESTRUCTION
- 14 MASS CASUALTY RESPONSE
- 15 BOMB THREAT RESPONSE
- 16 HAZMAT PROCEDURES
- 17 PHYSICAL SECURITY/ANTI-TERRORISM/FORCE PROTECTION WORKING GROUP (PS/AT/FP/WG)
- 18 TRAINING
- 19 DEFINITIONS

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 1

OPERATIONAL RESPONSIBILITIES/TASKS

	<u>PARAGRAPH</u>	<u>PAGE</u>
NORMAL CONDITIONS	1000	1-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 1

OPERATIONAL RESPONSIBILITIES/TASKS

1000. NORMAL CONDITIONS

1. No indications of terrorist activities targeting U.S. military personnel or facilities in the geographic area. Actions to be taken are as follows:

a. Commanding Officers (CO), Officers in Charge (OIC) (Squadron Level or higher). Develop comprehensive AT/FP programs based on current threat assessments and vulnerabilities. Programs shall incorporate the standards outlined in reference (b).

b. AT/FP program specific requirements

(1) Continually evaluate installation and unit AT/FP programs/plans in order to avoid complacency. At a minimum, annually review and exercise programs/plans.

(2) Appoint an AT/FP Officer in writing. This may be an additional duty. See Chapter 18 for training requirements.

(3) Units deploying OCONUS must have assigned an AT/FP Officer that is Level II trained and certified. Commanders may qualify individuals who are subject matter experts and have received formal training in AT/FP as AT/FP Officers. This individual shall serve as an advisor to assist the commander in meeting their AT/FP requirements. This individual shall, prior to deployment, ensure each person within the unit has received Level I training, is aware of the terrorism threat, and is trained to employ methods to reduce risk or mitigate the effects should an attack occur.

(4) Establish command AT/FP information and awareness programs to ensure all assigned personnel to include Marines, Sailors, family members and civilian employees are aware of the general terrorist threat and the personal protection measures that could reduce individual vulnerability to acts of terrorism. Additionally, command information programs shall be capable of ensuring that all personnel are informed of increased Force Protection Condition (FPCON) levels and the measures to be implemented.

(5) Develop a mass notification system via recognizable alarms for unit and installation personnel.

c. Assistant Chief of Staff, G-3

(1) Task the Training Division with the following requirements:

(a) Monitor availability of anti-terrorism schooling.

(b) Disseminate information concerning available anti-terrorism schools.

(c) Conduct/coordinate on-site anti-terrorism schools as requested.

(d) Schedule annual training in conjunction with Safety Standdowns.

(2) Plan, develop, and conduct AT/FP exercises and evaluations in accordance with paragraph 1000.1(b)(1).

(3) Attend the AT/FP and Physical Security Council (PSC) meetings.

(4) In conjunction with the Provost Marshal's Office (PMO) and Navy Criminal Investigative Service (NCIS), maintain liaison with civilian counterparts.

(5) Submit funding requests for AT/FP equipment and projects.

(6) Notify higher headquarters in the event of FPCON changes.

(7) Retain primary staff cognizance for the preparation, implementation, and revision of this plan and supporting MCAS plans. Ensure the plan is updated in accordance with paragraph 1000.1(b)(1).

(8) Develop and maintain the capability to staff and operate a primary/alternate Command Operations Center (COC).

(9) Coordinate the use of internal/external base resources as required by the on-scene commander.

(10) Appoint an installation AT/FP Officer.

(11) Ensure the installation's threat assessment is current.

(12) Ensure the Commanding General (CG) MCAS Miramar, Tenant Commanders, and staff officers are periodically briefed on current force protection conditions.

(13) Serve as the deputy chairman of the PS/AT/FP Working Group and member of the Crisis Management Team (CMT).

(14) Ensure PS/AT/FP Working Group meetings are held quarterly.

(15) Upon activating the CMT, brief all members on the current situation.

(16) Schedule Levels II and IV training requirements.

(17) Maintain a 24-hour Explosive Ordnance Disposal (EOD) capability to include:

(a) Procedures to render safe and disposal of explosive material/devices.

(b) Procedures for handling Weapons of Mass Destruction (WMD).

(c) Assist the G3 Training Division with training station personnel to recognize Improvised Explosive Devices (IED), use immediate action measures, and bomb search techniques.

(18) Initiate the base notification process in response to changes in force protection conditions.

(19) Assist with vulnerability assessment, if needed.

(20) Conduct other tasks as directed in this plan.

(21) Be prepared to initiate the Random Anti-terrorism Measures Program (RAMS) in conjunction with PMO.

d. Installation AT/FP Officer

(1) Attend the Level II AT/FP certification course.

(2) Review and become familiar with the references listed.

- (3) Develop an installation AT/FP program.
- (4) Update and maintain installation AT/FP plan.
- (5) Ensure the AT/FP Plan complies with reference (h).
- (6) Coordinate, compile, and submit after-action/lessons-learned to the Commandant of the Marine Corps (CMC) code POS and WDID, Marine Corps Combat Development Command (MCCDC) in Marine Corps Lessons Learned (MCCLS) format per reference (h).
- (7) Ensure this plan is coordinated with local, county, state, and federal agencies as appropriate.
- (8) Compile a prioritized list of Mission Essential Vulnerable Areas (MEVAs) approved by the CG.
- (9) Compile and submit a prioritized list of AT/FP projects and equipment requirements to the CG for funding.
- (10) Exercise the AT/FP plan, including the plan for dealing with Weapons of Mass Destruction, annually.
- (11) Review the AT/FP plan annually.
- (12) Provide for individual/unit formal training requirements.
- (13) Prepare installation threat and vulnerability assessments annually and have them reviewed by the PSC.
- (14) Conduct vulnerability assessments annually at a minimum. See Chapter 8.
- (15) Conduct other tasks as directed in this plan.

e. Assistant Chief of Staff, G-1

- (1) Coordinate with the Postal Officer to ensure adequate training for postal and MCAS Miramar headquarters personnel concerning letter bombs, mail screening procedures, and emergency actions in response to suspicious packages received via the U.S. Mail.
- (2) Prepare and update civilian and military personnel rosters quarterly.

- (3) Provide administrative support as required.
- (4) Serve as a member of the PSC.
- (5) Provide an officer/SNCO representative to the COC upon activation.
- (6) Assist with vulnerability assessment, if needed.
- (7) Conduct other tasks as directed in this plan.

f. Assistant Chief of Staff, G-4

- (1) Coordinate external sources for emergency logistical support.
- (2) Establish a feeding plan for mission essential personnel and those performing AT/FP duties.
- (3) Be prepared to coordinate the requisition, receipt, movement, and issue of munitions, as required.
- (4) Be prepared to provide 24-hour refueling capabilities for aircraft, vehicles, generators, and light sets, as required.
- (5) Identify facilities for emergency shelters/temporary housing.
- (6) Identify logistics needed for shelters.
- (7) Identify all MEVA sites that may need emergency power and/or barriers in conjunction with PMO.
- (8) Coordinate logistical support with South West Regional Fleet Transportation (SWRFT).
- (9) Be prepared to coordinate and provide transportation for evacuation and movement of personnel, goods, and equipment.
- (10) Be prepared to pre-position emergency back-up generators at designated facilities, ensuring they remain on site. Plan to hard-wire generators to mission essential facilities to prevent power losses from occurring.
- (11) Capture costs of items purchased and work performed directly supporting AT/FP projects and coordinate with the AC/S, G-8 for funding through MARFORPAC/HQMC specific AT/FP funds.

(12) Be prepared to provide organic material handling equipment (MHE) when required.

(13) Coordinate with 3d MAW G-4 to identify additional motor transportation and/or material handling equipment support.

(14) Be prepared to provide estimates of damaged buildings, equipment, and utilities.

(15) Be prepared to assist PMO with executing the barrier plan. See Chapter 9, Physical Security Procedures.

(16) Be prepared to provide 24-hour emergency maintenance capabilities.

(17) Be prepared to conduct emergency maintenance, by the priority of work.

(a) Debris, refuse, and obstacle removal.

(b) Repair/restore roads systems, drainage systems, sewage treatment and collection facilities, and water distribution systems.

(c) Emergency cutoff and restoration of electrical power and natural gas as required.

(18) Serve as a member of the PSC and the CMT.

(19) Provide an officer/SNCO representative to the COC upon activation.

(20) Consider AT/FP issues during major renovation and new construction projects.

(21) Assist with vulnerability assessment, if needed.

(22) Conduct other tasks as directed in this plan.

g. Assistant Chief of Staff, G-6

(1) Be prepared to provide communication services required to establish and operate the COC.

(2) Prioritize the restoration of base communications during a base power outage.

(3) Be prepared to provide emergency operations crews to restore telephone, radio, local area network, and data communications.

(4) Serve as the liaison with local telecommunications companies to direct/prioritize efforts.

(5) Serve as a member of the PSC and the CMT.

(6) Establish a basewide email or telephonic notification system used for transmission/dissemination of emergency & threat information. Be prepared to supplement PMO's Mass Notification System if it becomes degraded.

(7) Develop a program to protect information system infrastructure.

(8) Provide communication personnel for the COC upon activation.

(9) Provide an officer/SNCO representative to the COC upon activation.

(10) Assist with vulnerability assessment, if needed.

(11) Conduct other tasks as directed in this plan.

h. OIC, Branch Medical Clinic

(1) Develop and maintain medical memorandums of agreement/understanding with local civilian and military hospitals to provide for medical support beyond base medical clinic capabilities.

(2) Be prepared to execute emergency medical services (EMS) and basic lifesaving measures.

(3) Establish procedures for treatment and evacuation of mass casualty incidents.

(4) Be prepared to provide medical support at designated on-base emergency shelter locations.

(5) Be prepared to alert essential personnel and local external medical facilities should they be needed to augment medical support.

- (6) Establish procedures for treating chemically, biologically, or radiologically contaminated victims.
- (7) Be prepared to establish emergency morgue services.
- (8) Conduct environmental inspections of on-base emergency shelters for habitability, food stores, and potable water supplies.
- (9) Identify quarantine capabilities. Coordinate with G-4 to designate a specific location.
- (10) Provide inoculations to prevention spread of disease.
- (11) Serve as a member of the PSC and the CMT.
- (12) Provide an officer/CPO representative to the COC upon activation.
- (13) Assist with vulnerability assessment, if needed.
- (14) Conduct other tasks as directed in this plan.

i. NCIS

- (1) NCIS is the primary Base agency for analyzing, processing, blending all available criminal/intelligence sources, and disseminating criminal/foreign intelligence.
- (2) Establish and maintain MOA with state and federal criminal and foreign intelligence agencies.
- (3) Ensure liaison with federal, state, and local agencies is established to receive international, domestic, and criminal threat information.
- (4) Coordinate MCAS Miramar anti-terrorism/counter-terrorism plans with civilian law enforcement agencies to ensure the timely receipt of information concerning terrorist activities, as well as mutual support plans.
- (5) Conduct annual threat assessments of MCAS Miramar in conjunction with the Installation AT/FP Officer. Develop and update an annual installation specific threat assessment.
- (6) Assist departments/units conducting Operations Security (OPSEC) training, as required.

(7) Provide periodic briefings/intelligence assessments to the CG's of 3d MAW and COMCABWEST.

(8) Conduct country specific Level I briefings or provide the Level II instructor the information for the brief as required.

(9) Assume investigative jurisdiction on all incidents within your purview.

(10) Perform high-risk personnel security details.

(11) Serve as a member of the PSC and the CMT.

(12) Assist with vulnerability assessment, if needed.

(13) Conduct other tasks as directed in this plan.

j. Provost Marshal

(1) Provide recommendations to the CG, MCAS Miramar for setting the appropriate FPCONS.

(2) Conduct routine security patrols of MCAS Miramar.

(3) Conduct routine security operations on the flight line area.

(4) Conduct mission-oriented training on a regular basis to ensure adequate readiness of security elements.

(5) Conduct periodic response planning for bomb threats, hostage negotiations, anti-terrorism, and counter-terrorism operations.

(6) Provide Terrorism Awareness training to departments/units as required.

(7) Organize and convene the Installation Physical Security Council.

(8) Assist the AT/FP Officer with identifying installation Mission Essential Vulnerable Areas (MEVAS). PMO Physical Security will maintain a copy of the finalized list.

(a) The MEVA list will be designated in writing and approved by the CG, MCAS Miramar.

(b) Maintain a list of approved MEVAs classified "For Official Use Only."

(9) Be prepared to execute the barrier plan according to the designated FPCON.

(10) Obtain and maintain any specialized equipment required to combat the terrorist threat such as Special Reaction Team (SRT) equipment; lights/mirrors for vehicle under carriage inspections; portable metal detectors; and other similar devices.

(11) In conjunction with NCIS, maintain liaison with local, state, and federal authorities on matters pertaining to a coordinated response to security threats and other mutual physical security/terrorism issues.

(12) Be prepared to institute station-wide counter-surveillance measures to detect attempts by subversives conducting surveillance of station and 3d MAW operations.

(13) In conjunction with EOD, provide safe haven/refuge for in-transit DOD shipments when contacted by the Military Traffic Management Office (MTMO).

(14) Ensure that anti-terrorism protective features and other physical security measures are included in the planning and design of military construction and special projects.

(15) Flightline Security under normal force protection conditions will be optional for Automated Entry Control System (AECS), Identification (ID) level, Vehicle control, and Entry Control Points (ECPs).

(16) Provide an officer/SNCO representative to the COC upon activation.

(17) Assist with vulnerability assessments, if needed.

k. CG, 3d Marine Aircraft Wing (MAW)

(1) Be prepared to augment MCAS Miramar's Security Augmentation Force per the MOA between MCAS Miramar and 3d MAW. Personnel report to the Provost Marshal for assignment and use in anti/counter-terrorism operations as required.

(2) Assistant Chief of Staff, G-3. Develop plans for arming Group and Squadron Duty Officers.

(3) Assistant Chief of Staff, G-2. Coordinate alert center intelligence support as necessary. Ensure Anti-terrorism Alert Center Summaries (ATACSUM) are disseminated in a timely manner, coordinated with NCIS personnel.

(4) Assist with vulnerability assessment, if needed.

l. Headquarters and Headquarters Squadron (HQHQRON)

(1) In accordance with reference (f), establish a Security Augmentation Force (SAF) for use in anti/counter-terrorism operations and coordinate their training and assignment with the Provost Marshal.

(2) Assist with vulnerability assessment, if needed.

m. Station Explosive Ordnance Disposal (EOD)

(1) Provide Explosive Awareness training and support as required.

(2) Ensure X-RAY/SIED (Suspected Improvised Explosive Device) unit can be employed immediately when needed.

(3) Assist with vulnerability assessment, if needed.

n. Staff Judge Advocate (SJA)

(1) Advise the CG, MCAS Miramar; staff; and the CMT on legal issues pertaining to AT/FP.

(2) Provide legal advice to the CG, MCAS Miramar; CMT; and PMO on matters such as use of deadly force, jurisdiction, and other criminal non-criminal.

(3) Review this plan, Memoranda of Agreement, and supporting Orders to ensure legal aspects are adequately addressed.

(4) Serve as a member of the PSC.

(5) Provide claim services for property damages suffered by disaster victims.

(6) Assist with vulnerability assessment, if needed.

o. Public Affairs Officer (PAO)

(1) Operate as the sole public spokesperson for the CG, MCAS Miramar.

(2) Compile and prepare authoritative news release(s) on all phases of AT/FP operations for release to the media and general public.

(3) Initiate liaison with local media as appropriate.

(4) Ensure public affairs operating procedures and media programs support this plan.

(5) Determine, given existing conditions, the best means and priority to disseminate information.

(6) Coordinate the release of disaster information with agencies federal, state, county, and local public relief organizations.

(7) Arrange for the escort of civilian news media representatives.

(8) Serve as a member of the PSC and the CMT.

(9) Provide one officer to the COC upon activation.

(10) Assist with vulnerability assessment, if needed.

(11) Conduct other tasks as directed in this plan.

p. MCAS, Miramar Fire Department

(1) Maintain liaison with local, state, and federal authorities on matters pertaining to a coordinated response to major incidents or disasters aboard MCAS, Miramar.

(2) Coordinate MCAS, Miramar mutual aid needs with San Diego County area emergency service providers.

(3) Coordinate use of the San Diego Hazardous Material Incident Response Team (HIRT) to clean up incidents aboard MCAS, Miramar that exceed the capabilities of station resources. See Chapter 16, HAZMAT Procedures.

(4) Coordinate use of the Metropolitan Medical Strike Team for incidents aboard MCAS, Miramar.

(5) Coordinate with G-3 to conduct local Weapons of Mass Destruction (WMD) training exercises.

(6) Identify potential staging areas, decontamination sites and available resources on base.

(7) Identify requirements for any additional equipment, monitors, or personnel protective equipment.

(8) Provide a representative to the COC upon activation.

(9) Assist with vulnerability assessment, if needed.

q. Miramar Commissary

(1) Check all patrons ID's to ensure that only authorized patrons are permitted.

(2) All vendors, contractors, vendor stockers, and visitors will be required to sign-in in the appropriate log to identify their presence.

(3) All managers and supervisors will make use of anti-terrorism training videos and other training tools to ensure readiness.

(4) Assist with vulnerability assessment, if needed.

r. Office of Counsel

(1) Serve as a member of the PSC.

(2) Provide one officer to the COC upon activation.

(3) Advise on legal matters of a civil nature.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 2

THREAT LEVELS/FORCE PROTECTION CONDITIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	2000	2-3
THREAT LEVELS	2001	2-3
FPCONS	2002	2-4
FPCON MEASURES	2003	2-5

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 2

THREAT LEVELS/FORCE PROTECTION CONDITIONS

2000. GENERAL. This section clarifies the difference between threat LEVELS and FPCONS. Terrorist threat LEVELS are intelligence estimates. Threat LEVELS are often confused with force protection conditions (FPCONS). FPCONS (Alpha through Delta) are protective measures enacted by commanders in response to the assessed threat. Respective CINC J-3 branches are the staff proponents for FPCON information, but field commanders may set any FPCON they deem appropriate to protect their personnel and resources.

2001. THREAT LEVELS

1. The Department of Defense (DOD) has developed a methodology to assess terrorist threat to DOD personnel, facilities, material, and interests. This methodology is established by reference (b), and is used by the DOD only. Other U.S. Government Departments and Agencies may apply their own analytical methodology to form their own terrorist threat analyses. As a result, there may be differences between the DOD and other Departments or Agencies on gross or simple descriptions of terrorist threat to U.S. Government interests.

2. The DOD has identified four factors to be used in shaping the collection and analysis of information from all sources bearing on terrorist threat. These factors are used in making terrorist threat analyses on a country-by-country basis. The terrorist threat level for a given country is based on an assessment of the following factors established by reference (b):

a. Operational Capability. The acquired, assessed, or demonstrated level of operational capability to conduct terrorist attacks.

b. Intentions. Stated desire and/or actual history of attacking US interests. Influencing elements include recent attacks, anti-US or host nation ideology, attacks in other countries, and response to current international events.

c. Activity. A terrorist group's activity in a country may not always be related to operational planning or present a threat

to US/host nation interests. Many groups use countries as support bases and may not want to jeopardize their status by conducting a terrorist act.

d. Operating Environment. How does the overall environment, to include political and security considerations, influence a terrorist group's ability and motivation to conduct an attack?

3. One of the following threat levels is assigned on the basis of analysis of the above factors:

a. High. Anti-US terrorists are operationally active. Their Modus Operandi (MO) includes the use of mass casualty attacks. The operating environment favors the terrorist.

b. Significant. Anti-US terrorists are present but have limited operational activity. Their preferred MO is attacks against individual personnel, but they are capable of mass casualty attacks. The operating environment is neutral.

c. Moderate. Terrorists are present but there are no indications of anti-US activity. The operating environment favors the Host Nation/US.

d. Low. No group is present or the group activity is non-threatening.

4. Commander-in-Chiefs (CINCs) (through J2s) set threat levels in respective U.S. Command Areas of Responsibility (AOR).

2002. FPCONS. The FPCON system describes the progressive level of protective measures implemented by all DOD components in response to terrorist threats. The FPCON system is the principal means the commander has to apply an operational decision on how to guard against the threat. The appropriate FPCON is determined by assessing the terrorist threat, the capability to penetrate existing physical security systems at an installation, the risk of terrorist attacks of which DOD personnel and facilities expose themselves, the ability to carry on with missions even if attacked, and the criticality to DOD missions of assets to be protected. Assessed threat LEVELS do not dictate the specific FPCON posture that the installation assumes. The installation commanders should declare a FPCON level that is appropriate for their particular location. The FPCON set by higher headquarters represents the minimum baseline standard. The installation commander may implement more stringent security measures as needed.

2003. FPCON MEASURES

1. **Normal**. Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.
2. **Alpha**. Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable.
3. **Bravo**. Applies when an increased and more predictable threat of terrorist activity exists.
4. **Charlie**. Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel or installations is imminent.
5. **Delta**. Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, FPCON DELTA is declared as a localized condition.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 3

PROCESS TO RAISE/LOWER FORCE PROTECTION CONDITIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	3000	3-3
FACTORS	3001	3-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 3

PROCESS TO RAISE/LOWER FPCONS

3000. GENERAL

1. FPCONS are graduated categories of measures or actions taken to protect personnel or assets from attack. Revised FPCONS may be implemented following the receipt of intelligence through official or unofficial sources.
2. The CG, MCAS, Miramar sets the FPCON level for MCAS' Miramar. Tenant units aboard the installation shall mirror the station FPCON.
3. Subordinate commanders may raise, but not lower, a higher-level commander's FPCON.
4. The AC/S, G-3 and Provost Marshal provide recommendations for establishing an appropriate FPCON level.

3001. FACTORS. The decision to arrive at a particular FPCON and associated security measures should be based on multiple factors including, but are not limited to:

1. The threat.
2. Target vulnerability.
3. Criticality of assets.
4. Security resources availability.
5. Operational and morale impact of security measures.
6. Damage control and recovery procedures.
7. International relations.
8. Planned U.S. Government actions, which could trigger a terrorist response.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 4

FPCON SPECIFIC ACTIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
FPCON ALPHA	4000	4-3
FPCON BRAVO	4001	4-7
FPCON CHARLIE	4002	4-15
FPCON DELTA	4003	4-19
ADDITIONAL FPCON MEASURES FOR AVIATION FACILITIES	4004	4-21

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 4

FPCON SPECIFIC ACTIONS

4000. FPCON ALPHA

1. FPCON Alpha applies when there is a general threat of possible terrorist activity against MCAS Miramar and/or its personnel, the nature and extent of which are unpredictable, and when the circumstances do not justify full implementation of the measures of FPCON Bravo. However, it may be necessary to implement certain selected measures from FPCON Bravo, as a result of intelligence received, or as a deterrent. The measures in this FPCON must be capable of being maintained indefinitely.

a. All Departments/Units

(1) Ensure all measures during normal conditions are in effect.

(2) Reemphasize bomb threat procedures.

(3) Reemphasize Operations Security (OPSEC) for awareness.

(4) Conduct random identification checks of personnel entering key facilities.

(5) Coordinate with AC/S, G-4 to identify alternate parking locations away from key facilities where 25 meters of stand off distance cannot be provided.

(6) Review reference (h) for any further action deemed appropriate.

(7) Comply with all applicable FPCON Alpha measures.

b. AC/S, G-3

(1) Notify all elements of MCAS, Miramar and appropriate headquarters units that FPCON Alpha has been set and receive acknowledgments.

(2) Provide staging areas for all personnel/equipment deploying from or returning to MCAS, Miramar. Coordinate security requirements with the Provost Marshal.

c. Classified Material Control Center (CMCC) Officer.
Maintain a current read folder of all classified terrorist threat messages for review by appropriate personnel.

d. AC/S, G-4

(1) Identify one or more centralized, alternate, parking locations to accommodate vehicles that normally park near key facilities. Coordinate with PMO.

(2) Provide support to MCAS Miramar elements in meeting any special needs for barriers to regulate access and/or provide safety buffer zones from facilities determined to be at risk.

(3) Coordinate with the AC/S, G-4, 3d MAW for use of heavy equipment, lights, etc. as necessary.

e. NCIS

(1) Keep the local law enforcement agencies advised of all developments.

(2) Coordinate and provide support to the FBI in the event that agency assumes jurisdiction over a terrorist incident.

f. PAO. Publish an educational series of articles concerning terrorism in the station newspaper, informing the public in a general sense that increased security measures are being implemented.

g. SJA

(1) Provide continuing advice regarding compliance with existing laws and regulations.

(2) Provide other legal services as required.

h. Provost Marshal. Flightline security under FPCON Alpha.

(1) The AECS (Automated Entry Control System) is required to be active.

(2) The ID level will require personnel to swipe a card. The use of a Personal Identification Number (PIN) and photo are optional.

(3) Flightline vehicle access is limited to essential use only.

(4) If the AECS is inoperable, the Entry Control Points (ECPs) are required to be manned continuously.

(5) Coordinate with AC/S, G-4 to prepare plans for alternate, centralized parking sites for key facilities where 25 meters of stand off distance cannot be provided.

i. Miramar Commissary

(1) Ensure all measures from Condition NORMAL are in effect.

(2) Reemphasize bomb threat procedures.

(3) Ensure evacuation plan is current and posted in all appropriate locations.

(4) Duty Manager will ensure that "evacuation meeting sites" are rotated for every instance the commissary is evacuated.

j. FPCON Measures

(1) Measure 1. The AC/S, G-3 and PMO will:

(a) Brief all personnel on the current force protection condition and those measures enacted to increase security. Remind all duty personnel, including family members, to be especially alert for suspicious or unusual activities and strangers, particularly those carrying suitcases or other containers, and packages.

(b) Conduct unit-level training on terrorism awareness.

(c) Be alert for unidentified vehicles on, or in the vicinity of, U.S. installations, units or facilities.

(2) Measure 2

(a) Keep key personnel (Squadron Duty Officers or appointed personnel) who may be needed to implement security plans on call. Personnel having access to security plans for evacuating or sealing off buildings and/or areas in use must be available at all times if an explosion or attack occurs.

(b) Ensure duty personnel have knowledge of, and access to, emergency plans for immediate evacuation of buildings and grounds, as well as plans for cordoning and sealing off areas.

(c) Establish on-call duty roster of heavy equipment operators. All off-duty heavy equipment operators will report their destination and expected time of return to the military police desk sergeant prior to leaving their listed recall address.

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

(4) Measure 4. Provost Marshals Office will:

(a) Increase security spot checks of vehicles and persons entering the installation and unclassified areas.

(b) Conduct random identification spot checks of passenger and commercial vehicle occupants gaining access to the installation using predetermined criteria for vehicle selection. If possible, delays in traffic beyond eight(8) to ten(10) minutes should be avoided.

(c) Conditions permitting, consider visually checking identification card, drivers license, and/or vehicle registration card of all passenger vehicles and commercial truck drivers, and the identification card of vehicle occupants and pedestrians, to include joggers and bicyclists.

(d) Physically inspect license plates affixed to vehicles entering the installation.

(e) With or without Military Working Dog (MWD) assistance, daily Commanding General's administrative vehicle inspections will be conducted at random times and locations, using predetermined criteria for vehicle selection.

(5) Measure 5. The Provost Marshals Office will limit installation access points for vehicles and personnel corresponding with a reasonable traffic flow.

(6) Measure 6. Apply one of the following measures from FPCON BRAVO individually and randomly as a deterrent:

(a) At the beginning and end of each workday, and at regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages or activity.

(b) Check all deliveries to dining facilities, clubs, etc., and advise family members to check all home deliveries.

(c) Increase surveillance of domestic accommodations, Child Development Center, dining facilities, clubs, and other "soft targets" to improve deterrence and defense.

(d) Secure and regularly inspect buildings and storage areas not in regular use.

(7) Measure 7. Review all plans, orders, personnel details, and logistics requirements related to the introduction of a higher FPCON. Convene the Installation Physical Security Council/Anti-terrorism/Force Protection Working Group to review incident response plans.

(8) Measure 8. Review and implement security measures for high-risk personnel; e.g., direct the use of inconspicuous body armor.

(9) Measure 9

(a) Provost Marshals Office will notify and consult with local authorities on the force protection conditions in effect at the installation and continue to exchange intelligence. Jurisdiction and command and control issues should be agreed upon and exercised between NCIS, the FBI, and local agencies.

(b) The Commanding General and key staff will review the installation contingency plans.

(10) Measure 10. Establish counter-surveillance in areas likely to be targeted by hostile elements. Place barriers in a ready position near gates and sensitive buildings, i.e., MEVAs or critical infrastructure, where they may be required to block, delay or channel hostile actions.

4001. FPCON BRAVO

1. FPCON Bravo applies when an increased and more predictable threat of terrorist activity exist. The measures of the FPCON must be capable of being maintained for weeks without causing undue hardship, without affecting operational capabilities, and without aggravating relations with local authorities.

a. Department/Units

- (1) Implement all measures for FPCON Alpha.
- (2) Formulate plans for posting armed guards at key facilities. Coordinate these security plans with the Provost Marshal and advise when requirements exceed personnel assigned.
- (3) Identify those personnel to be issued small arms and ammunition in the event a higher threat condition is required.
- (4) Review reference (a) for any further action deemed appropriate.
- (5) Ensure compliance with all applicable FPCON Bravo measures.

b. CG, 3d MAW (AC/S, G-3). Finalize plans for providing Marines to augment the PMO security force, and plans for the arming of Group and Squadron duty officers. Coordinate security plans with the Provost Marshal via the 3d MAW Force Protection Officer.

c. AC/S, G-3

- (1) Notify all elements of MCAS Miramar that FPCON Bravo has been set and receive acknowledgments.
- (2) Restrict Remain-Over-Night (RON) landings of military aircraft to U.S. military airfields.
- (3) Ensure Station EOD can respond on a 24-hour basis to bomb threats or discoveries of suspected devices.

d. AC/S, G-6

- (1) Establish plans for the rapid restoration/repair or use of alternate services in the event essential communications are disrupted.
- (2) Arm the communications watch officer in the Joint Communications Center. Ensure the Duty Communications Clerk is issued an M-9 pistol and thirty (30) rounds from the Station Armory.

e. PMO

(1) Increase random checks of vehicles entering the air station or parking in or adjacent to the flightline restricted area.

(2) Increase Military Police vehicle patrols of parking areas near the flightline restricted area, adjacent to hangars, and key facilities.

(3) Increase physical security checks of key facilities after normal working hours.

(4) MWD Explosive Detector teams check the exterior of vehicles in the parking lots immediately adjacent to headquarters and other sensitive buildings, i.e., MEVAs and other critical infrastructure.

(5) Flightline Security under FPCON Bravo

(a) The Automated Entry Control System (AECS) is required to be active.

(b) The ID Level requires personnel to swipe an identification card (i.e., military ID) and use a PIN for entry. The photo is optional.

(c) Flightline vehicle access is limited to essential use only.

(d) If the AECS is inoperable the ECPs are required to be manned continuously by trained augmenters.

f. Postal Officer. Increase surveillance procedures by U.S. Postal Service personnel. Coordinate emergency action plans with Station EOD in the event suspicious articles are found.

g. AC/S, G-4

(1) Stock and maintain sufficient meals and water to provide food services in the event of damage to the dining facility, prolonged power outages, or water service interruption.

(2) Be prepared to feed personnel whose duties preclude attendance at the dining facility.

(3) Coordinate Station Ordnance security measures with the Provost Marshal.

(4) Be prepared to issue small arms ammunition to the HQHQRON Armory.

(5) Create plans for rapid restoration/repair of services in the event damage (i.e. water, electric, etc.) is incurred.

(6) Assist PMO with implementing the barrier plan and alternate centralizing parking plan.

h. HQHQRON. Transfer operational control of the SAF to the Provost Marshal for use in anti-terrorism/counter-terrorism operations.

i. OIC, Branch Medical Clinic

(1) Review plans for handling mass casualties and transportation support requirements. Coordinate with outside health care providers in the event assistance is needed.

(2) Formulate plans for posting armed guards at key entrances of the clinic. Coordinate personnel requirements with the Provost Marshal.

j. PAO

(1) Publish information concerning anti-terrorism precautions for personal safety, residential security, and facility protection.

(2) Provide news releases to the local media as appropriate.

k. AC/S, Marine Corps Community Services (MCCS)

(1) Consider closing snack bars in key facilities as appropriate.

(2) Check all deliveries to all MCCS activities and provide driver access lists to PMO.

1. Miramar Commissary

- (1) Ensure all measures from Condition Normal and FPCON Alpha are in effect.
- (2) Increase awareness of persons entering facility:
 - (a) Manually verify all sign-ins.
 - (b) Ensure all delivery personnel have proper credentials.
 - (c) Assign two ID Checkers whenever possible.
- (3) Conduct general search of facility for any suspicious packages, suspicious activity and to ensure facility is locked down.
- (4) Duty Manager will perform 4 searches daily:
 - (a) One prior to store opening.
 - (b) One within 1 hour after store opening.
 - (c) One at midday.
 - (d) One at store closing time.
- (5) Duty Manager will perform general searches of the facility's outer boundaries. (0600, 1200, 1800).
- (6) Ensure personnel are aware to be cognizant of suspicious activity and or packages. All personnel will take extra care when in-checking all deliveries, looking for anything out of the ordinary.
- (7) Inform all patrons that no packages will be brought into the Commissary unless they are first inspected by ID Checker. (Asking patrons to leave packages in their cars is preferable).
- (8) Contact base officials for further information and or any other specific guidelines to be followed.
- (9) Brief personnel on changes in FPCON status and what it means to them.

m. FPCON Measures

(1) Measure 11. Repeat Measure 1 and warn personnel of any other form of attack to be used by terrorists. Unit security managers continue the threat briefing/information/orientation process for all personnel, with particular emphasis toward reporting suspicious incidents and persons.

(2) Measure 12. Key staff members will continue preparing anti-terrorism contingency plans and will remain on call.

(a) All Crisis Management Team (CMT) members, off-duty Military Police, Security Augmentation Force, primary reaction platoon personnel, and other members of the Crisis Management Force (CMF) will report their destination and expected time of return to the COC Watch Officer, or in their absence, another designated official prior to leaving their listed recall address.

(b) If resources allow, assign a driver and/or military police trained in protective service operations to the Station CG, General Officers, or other designated personnel with greater terrorist target value.

(c) The Provost Marshal will periodically recall the Special Reaction Team (SRT).

(3) Measure 13. Check plans for implementing the measures of the next higher FPCON.

(4) Measure 14. Move cars and objects such as crates, trash containers, etc., at least 25 meters from buildings of a sensitive or prestigious nature, i.e., MEVAs or critical infrastructure, if possible. Consider the use of centralized parking for those areas where stand-off cannot be provided.

(5) Measure 15. Regularly inspect and secure all buildings, rooms, and storage areas not in use.

(6) Measure 16. Inspect the interior and exterior of buildings, in normal use for the presence of suspicious objects and packages at regular and frequent intervals at the beginning and end of each workday.

(a) Security and law enforcement personnel increase physical security checks of facilities after normal working hours.

(b) Explosive Detector MWD teams check the exterior of vehicles in the parking lots immediately adjacent to headquarters and other sensitive buildings, i.e., MEVAs and other critical infrastructure.

(7) Measure 17. Examine all incoming mail for letter or parcel bomb devices.

(8) Measure 18. Inspect all deliveries to dining facilities, clubs, etc.

(a) Conduct random checks of package deliveries brought into service areas by designated personnel and employees.

(b) Advise military family members to check all home deliveries and report all suspicious letters/packages.

(c) Military Police search all commercial vehicles entering the installation, and compare vehicle contents with bills of lading or other manifest documents.

(9) Measure 19. Increase surveillance of domestic accommodations, dining facilities, clubs, LBQ's, and other "soft targets".

(a) Military Police MWD teams shall conduct a walking patrol of the installation housing area perimeter fence line, and establish regular patrols in the flightline restricted area.

(b) Implement regulations prohibiting the carrying of parcels into exchanges, clubs, and other designated buildings, except for specific circumstances and through designated buildings and doors.

(c) Signs indicating the new regulations should be conspicuously posted at the selected sites, buildings, and doors.

(10) Measure 20. To prevent rumors and unnecessary alarm, brief the general situation to the organizational staff and family members.

(11) Measure 21. Inform members of local security committees of any actions being taken and reason.

(12) Measure 22. Physically and visually inspect all visitors to the unit, to include suitcases, parcels, and other containers. Ensure proper dignity is maintained, and if possible, ensure that female visitors are inspected by a female qualified to conduct physical inspections.

(a) Commanding Officers will reduce authorized access points of all buildings under their cognizance, implement random ID checks at all building entrances, and physically inspect handbags, briefcases, and parcels of all visitors.

(b) Commanding Officers will implement 100 percent identification card checks at buildings that are, or contain, high value targets, i.e., MEVAs or other critical infrastructure.

(c) All visitors will be physically inspected by security personnel and escorted; "official visitors" may be exempted. While issuing visitor passes MPs will physically inspect visitors entering the base, to include their suitcases, parcels, and other containers

(13) Measure 23. Randomly check vehicles, personnel, and buildings. MP patrols will check roads adjacent to the installation's perimeter fence line, and report suspicious off-base circumstances to the law enforcement agency with jurisdiction in that area. Installation perimeter fence lines not accessible by vehicles should be checked on foot or by MWD teams.

(14) Measure 24. In accordance with prepared plans, protect off-base military personnel and military transport. Remind drivers to lock their parked vehicles and use caution before entering and driving.

(15) Measure 25

(a) Implement additional security measures for high-risk personnel.

(b) Utilize frost calls and station cable television to disseminate information/directions such as civilian attire, off-limits areas, alternate reporting times, etc.

(c) Train and brief unit high risk personnel in incident response and emergency aid procedures.

(16) Measure 26. Brief personnel, who may augment the guard force, on the use of deadly force and rules of engagement.

(17) Measure 27. Consult with local authorities on the threat and combined anti-terrorism measures, as appropriate.

(a) Implement the Installation Barrier Plan maintained by PMO and place barriers at gates, near designated MEVAs, and other critical infrastructure as appropriate.

(b) Support placed barriers placed around MEVAs with good observation.

(18) Measure 28. Provide increased security surveillance of critical communications facilities/assets, etc.

4002. FPCON CHARLIE

1. FPCON Charlie applies when an incident occurs or when intelligence is received indicating that some form of terrorist action against MCAS Miramar and personnel is likely. Implementing this measure for more than a short period will probably create hardship and will affect the peacetime activities of the installation, all units, and its personnel.

a. Department/Units

(1) Implement all measures for FPCON Alpha-Bravo.

(2) Ensure compliance with all applicable FPCON Charlie Measures.

(3) Establish duress code words. Units/security personnel can use these words to indicate a possible hostage situation or other problem.

(4) Request additional counter intelligence (CI) support to further augment existing CI capabilities.

(5) Execute the alternate centralized parking plan when directed.

b. AC/S, G-3

(1) Activate the CMT.

(2) Activate the COC.

(3) Airfield Operations. Post armed personnel in key airfield operation areas and coordinate their employment with the Provost Marshal.

(4) Station EOD. Conduct a recall of personnel and remain on an alert status for the duration of FPCON Charlie.

c. PMO

(1) Recommend establishing FPCON Delta when appropriate to the CG.

(2) Flightline security under FPCON Charlie.

(a) The AECS is required to be active.

(b) The ID Level requires personnel to swipe an identification card (i.e., military ID) and use a PIN for entry.

(c) Flightline vehicle access is limited to essential use only.

(d) If the AECS is inoperable, the ECPs are required to be manned continuously.

(3) Execute the barrier plan.

d. CG, 3d MAW (AC/S, G-3)

(1) Provide Marines to augment PMO, in order to provide adequate Station Security. These Marines will report to the PMO Operations Chief with T/O weapon, and 782 Gear.

(2) Provide additional ground support (MHE, motor transportation, generators, lighting) if possible.

(3) Provide Armory custodians to augment HQHQRON to assist with the maintenance, issuing and recovery of Guard Force Weapons.

e. AC/S, G-4

(1) Issue food and equipment in support of anti-terrorism plans as requested by MCAS Miramar elements.

(2) Coordinate with the Defense Commissary Agency (DECA) Officer for possible resupply of the messhall due to the potential inability of local vendors to gain access for on-base deliveries.

(3) Coordinate with the Provost Marshal regarding the relocation of dumpsters away from key facilities.

(4) Install lighting units with backup power generators at key facilities. Designate someone to fuel the backup power generators, and to refuel the generators when needed at the site. The generators will be employed if electric power is interrupted.

(5) Establish designated parking area(s) away from key facilities and institute shuttle bus service.

(6) Coordinate with PMO to allow mission essential civilian employees and contractors on base.

(7) Provide billeting at the CBQ for designated COC watch standers, as needed.

(8) Coordinate with HQHQRON and the AC/S G-4, 3d MAW for the consolidation of all Guard Force Weapons within one armory.

f. OIC, Branch Medical Clinic. Be prepared to conduct a recall of medical personnel necessary to initiate the reception, transportation, and treatment of large numbers of casualties.

g. PAO. Prepare informational news releases for the news "media." Provide copies of information prior to release to the station Security Manager for review and/or recommendations. Release the information to the news media only after approval of the CG, MCAS Miramar, and HQMC PAO. Notify local media of increased traffic congestion (due to gate restrictions) near base gates for "sig-alert" broadcast.

h. AC/S, MCCS

(1) Be prepared to secure operations at MCCS activities when directed by the CG.

(2) Be prepared to secure all alcoholic beverage sales at MCCS retail and club activities when directed by the CG.

(3) Be prepared to secure all mobile snack bar truck operations when directed by the CG.

i. Miramar Commissary

(1) Ensure all measures from Condition Normal and FPCONS Alpha and Bravo are in effect.

(2) Establish duress code word to be used in cases of Bomb Threats and Hostage situations. CODE WORD is **CODE BLUE**.

(3) Contact base officials for any information and or specific guidelines to be followed. (*This may include temporary closure of the commissary*).

(4) Coordinate with the AC/S, G-4 to provide food supplies to the Messhall, as required, due to restricted vendor deliveries.

j. FPCON Measures

(1) Measure 30. Continue FPCON BRAVO measures, or introduce those measures still remaining.

(2) Measure 31. Keep all personnel that are responsible for implementing anti-terrorist plans at their place of duty.

(3) Measure 32. Access points will be limited to an absolute minimum.

(4) Measure 33. Entry control will be strictly enforced and a percentage of vehicles will be searched.

(5) Measure 34. Enforce centralized parking of vehicles away from sensitive buildings, i.e., MEVAs and other critical infrastructure where 25-meters standoff cannot be maintained.

(6) Measure 35. Weapons will be issued to guards, as Marine Corps regulations prescribes the issuance of loaded weapons to all personnel engaged in law enforcement or security duties.

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

(8) Measure 37. Protect all designated Mission Essential Vulnerable Areas (MEVA'S) and Vulnerable Points (VP'S). Give special attention to MEVA'S and VP'S outside of the installation.

(9) Measure 38. Erect barriers and obstacles to control traffic flow. (Refer to Chapter 12)

(10) Measure 39. Consult with local authorities prior to closing public and military roads that will make sites increasingly vulnerable to terrorist attacks.

(11) Measure 40. Complete employing all barriers listed in the installation barrier plan (Refer to Chapter 12), and have MWD teams conduct walking patrols of selected installation barriers.

4003. FPCON DELTA

1. FPCON Delta applies in the immediate area where a terrorist attack has occurred, or when intelligence has been received that terrorist action against a specific location is imminent. Normally, this FPCON is declared as a localized warning.

a. Departments/Units

(1) Implement all measures directed for FPCON Alpha through Charlie.

(2) Review reference (h) for any further action deemed appropriate.

(3) Ensure compliance with all applicable FPCON Delta measures.

b. Provost Marshal

(1) Increase frequency of random perimeter patrols.

(2) Flightline Security under FPCON Delta.

(a) The AECS is required to be active.

(b) The ID level will require personnel to swipe a card, use a PIN, and Photo ID.

ANTI-TERRORISM/FORCE PROTECTION PLAN

(c) Flightline vehicle access is limited to essential use only.

(d) The ECPs are required to be manned continuously regardless if the AECS is operable or inoperable.

(e) Only mission essential contractors shall have access within the flightline, and will be escorted by a unit representative.

c. CG, 3d MAW (AC/S, G-3). Provide additional Marines to augment PMO, in order to provide adequate Station Security. These Marines will report to the PMO Operations Chief with their T/O weapon, and 782 Gear.

d. Miramar Commissary

(1) Ensure all measures from Condition Normal and FPCONS Alpha, Bravo, and Charlie are in effect.

(2) Contact base officials for any information and or specific guidelines to be followed.

(3) At the CG's direction, the Duty Manager will shut down/lock down facility if not already done so, under FPCON Charlie.

e. FPCON Measures

(1) Measure 41. Continue or introduce those measures listed for FPCON Bravo and Charlie.

(2) Measure 42. Augment guards, as needed.

(3) Measure 43. All vehicles need to be identified on the installation within operations or mission support areas.

(4) Measure 44. All vehicles will be searched upon entering the complex or installation, as well as their contents.

(5) Measure 45. Conduct positive identification of all personnel, and control all access.

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

(7) Measure 47. Control access to all areas under the jurisdiction of the U.S. command or agency concerned.

(8) Measure 48. Conduct frequent checks of building exteriors and parking areas.

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

(10) Measure 50. Consult with local authorities concerning closing public and/or military roads and facilities which will make sites increasingly vulnerable to terrorist attacks.

(11) Measure 51. Man posts as necessary to prevent attack against vulnerable facilities outside the base boundaries.

4004. ADDITIONAL FPCON MEASURES FOR AVIATION FACILITIES

1. The following Aviation Facilities FPCON measures will be completed in addition to the standard FPCON measures, in accordance with reference (b).

a. Aviation Facility FPCON Alpha and Bravo Measures

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

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

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

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

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

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

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

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

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

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

(11) Miramar Fire Department and Airfield Rescue Fire Fighting (ARFF) need to conduct practice drills.

(12) Hold practice alerts within the perimeter.

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

(14) 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.

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

b. Aviation Facility FPCON Charlie Measures

(1) Brief all personnel on the increased threat.

(2) Inform local police of the increased threat.

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

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

(5) Inspect all vehicles and buildings on a regular measure.

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

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

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

(9) Escort all visitors.

(10) Close relief landing grounds where appropriate.

(11) Check airfield diversion state.

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

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

c. Aviation Facility FPCON Delta Measures

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

(2) Inform local police of the increased threat.

(3) Cease all flying except for specifically authorized operational sorties.

(4) Implement, if necessary, appropriate flying counter-measures.

(5) Be prepared to accept aircraft diverted from other stations.

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

(7) Close military roads allowing access to the airbase.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 5

CRISIS MANAGEMENT TEAM

	<u>PARAGRAPH</u>	<u>PAGE</u>
SPECIAL THREAT SITUATIONS	5000	5-3
DEFINITIONS	5001	5-3
AUTHORITY AND JURISDICTION	5002	5-3
ACTION	5003	5-4
CMT CHECKLISTS	5004	5-11
TMF MEMBER CHECKLIST	5005	5-15

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 5

CRISIS MANAGEMENT TEAM

5000. SPECIAL THREAT SITUATIONS. The purpose of the following section is to provide guidance for the management of special threat situations involving snipers, barricaded criminals, terrorist activity, or hostages, which require special reaction/response, manpower, and training. Special threat situations have occurred on U.S. military installations throughout the world. When these situations are of sufficient magnitude to require resources beyond the control of the Provost Marshal, it is essential that the installation be prepared to effectively marshal and coordinate all required internal and external resources.

5001. DEFINITIONS

1. Crisis Management Team (CMT). A team formed at the major command or installation level concerned with plans, procedures, techniques, policies, and controls for dealing with terrorism, special threats, or other major disruptions occurring on government installations and facilities. This team controls and coordinates the installation's handling of a special threat situation.
2. Command Operation Center (COC). The command center is a facility used by the Crisis Management Team. The term Emergency Operations Center (EOC) is interchangeable with COC for the purposes of this Order.
3. Crisis Management Force (CMF). The actual force which responds to contain, control, and resolve the special threat situation. It will be tasked organized, commanded by the Provost Marshal Office, and will normally contain such assets as the Military Police, Security Forces, reinforcing forces, negotiating teams, Special Reaction Teams, firefighters, Explosive Ordnance Disposal personnel, and any other emergency personnel required. It is subordinate to the CMT.
4. On-Scene Incident Command Post. Command post used by the CMF.

5002. AUTHORITY AND JURISDICTION

1. Responsibility for responding to a special threat incident rests with the CG, MCAS, Miramar.

2. The Federal Bureau of Investigation (FBI) has primary jurisdiction for domestic terrorism and will assume jurisdiction if the special threat incident is of significant federal interest. Air Station personnel will continue to operate under military control even after the FBI assumes jurisdiction. The CMT and CMF will support the FBI to the extent necessary to resolve the incident.

3. The Naval Criminal Investigative Service (NCIS) will provide support and assistance to the CMF, but will not assume investigative jurisdiction until after the special threat situation has been resolved. At that point, the command will refer the matter to NCIS.

5003. ACTION

1. Crisis Management Team (CMT)

a. The Miramar CMT will activate when FPCON Charlie (Refer to Chapter 4) is declared, or in response to an actual threat incident of sufficient magnitude. The AC/S, G-3 is the senior CMT member and is responsible for its training, activation, and supervision.

b. The CMT will operate in the MCABWA COC, Building 9211 Room 211. This facility provides emergency power, adequate communications, and workspace, as well as easy access to the CG, principle staff officers, and 3d MAW representatives. The AC/S, G-3 will designate an alternate COC when deemed appropriate.

c. The following departments/sections will maintain a representative at the COC, once the CMT is activated:

- (1) AC/S, G-3.
- (2) AC/S, G-4.
- (3) AC/S, G-6.
- (4) 3d MAW Representative.
- (5) Branch Medical Clinic.
- (6) MCAS, Miramar Fire Department.
- (7) NCIS.

- (8) PAO.
- (9) Provost Marshal.
- (10) SJA.
- (11) Other representatives as required.

d. The CMT Center's location subsequent to initial incident notification will be in the CG's conference room, building 8630. The task of the CMT is to serve as a specialized staff element in support of the command center during counter-terrorism or other high-risk (i.e. barricaded subjects) operations. Activation of the CMT should complement rather than conflict with normal operating procedures.

e. CMT Member Checklists. Once a specified threat occurs, the COC needs to be activated and CMT members should start taking immediate action steps. Staff members' checklists will be kept in separate notebooks within the COC. The Threat Management Force commander maintains each respective checklist for overall management.

f. Reporting Procedures. Immediate and subsequent reporting to higher headquarters is necessary in any terrorist or high-risk special threat situation. These reports are Serious Incident Reports (SIR's) in accordance with reference (e). Local reporting requirements will include immediately advising the Command Center of a terrorist or high risk special threat incident providing "who, what, where, when, how, why (if known)" information upon which the decision to sound alert can be based. Individual stations should also be established as listed below to support the CMC:

(1) Emergency First Aid Station. The Emergency First Aid Station should be addressed in the local medical center's SOP. Details should identify if the aid stations are mobile, ambulance parking areas, triage, hospital, and ambulance augmentation, as well as other standard equipment and personnel requirements.

(2) Temporary Morgue Facility. If necessary, the senior medical officer will plan for the establishment of a temporary morgue facility. Items to be included in these considerations are location, body bags and shroud requirements, tags, forms, a log, and support required to assist in identification of remains.

(3) Press Center. The JPAO is responsible for establishing a press center to provide a focal point as well as a control

measure for dealing with the press. Press considerations include size of facility, sufficient outside telephone communication, and speedy gathering and transmitting of information. Command considerations are to balance these press considerations with safety issues, expeditious rescue operations, and other security and emergency requirements.

(4) Information Center. The Information Center differs from the Press Center because as it handles the inquiries concerning missing persons and property damage. The Information Center will have the capability to obtain the lists of the dead, injured, evacuees, and property damage. Here again, the commander or a designated representative is the approving authority for releasing this type of information.

(5) Recovered Property Site. The collection, safeguarding, itemizing, and disposal of recovered property will be processed in accordance with current directives. Terrorists/criminals are known to booby-trap items of equipment (e.g., flashlights, fire extinguishers, radios, etc.). Troops must be instructed to leave recovered/found property alone until trained personnel have screened them for bombs. Trained Bomb Detection Dogs will be of great value in this screening process.

(6) Logistical Support Center. A terrorist or high risk/special threat incident may last for days, weeks, even months. NEVER ASSUME THAT AN INCIDENT WILL BE RESOLVED QUICKLY, especially if it involves a hostage/barricade situation. Logistics support will be planned for by the TMF, CMT, Command Center, and other centers including media personnel. Preparations must be made to deliver food, medical supplies, and other logistical support to the hostages and their captors, in addition to the force responding to the threat. Special consideration must also be given to continuation of normal operations of other activities on the installation during a prolonged incident.

2. Threat Management Force (TMF). The Military Police Operations Officer is the commander of the TMF. The TMF is organized into several teams:

a. The Initial Response Force is responsible to the TMF commander. The Initial Response force immediately identifies the nature of the situation and reports it. They will isolate the incident and contain the situation until relieved or augmented with additional personnel.

b. The Special Reaction Team (SRT) is the military equivalent of a civilian police department's SWAT team. The SRT is organized, trained, and equipped to provide one or more entry teams and designated marksman/observer teams tailored to the specific threat. The mission of the SRT is to respond to special threat situations where human life is in jeopardy and brings about a peaceful resolution without serious bodily injury or death to anyone (hostages, suspects, terrorists, suicidals, bystanders, or law enforcement personnel). In conjunction with available support and resources, the SRT training program should ensure mission capability in the following areas.

- (1) Perimeter containment and evacuation.
- (2) Building entry and clearing.
- (3) Assault on barricaded positions.
- (4) Occupancy control.
- (5) Hostage rescue.
- (6) Terrorist/Suspect apprehension.
- (7) Selected marksman employment.
- (8) Scaling/Rappelling buildings or obstacles.
- (9) Helicopter insertion/extraction.

c. Hostage Negotiation Team. The Hostage Negotiation Team, which interacts with the terrorists on order of the TMF Commander, should be established. A typical negotiation team would be made up of the following personnel:

- (1) An OIC (NCIS Agent).
- (2) A primary hostage negotiator (NCIS, MPI, or other trained hostage negotiator).
- (3) A backup hostage negotiator (same qualifications).
- (4) A military police investigator.
- (5) A NCIS agent who is knowledgeable in international terrorism.

(6) A linguist, in the event a different language is being used.

d. Negotiator Equipment. Equipment for use by the negotiation team will be readily available. Equipment will be set aside in portable containers, field desks, etc. If it is pre-packed, items will be frequently inspected and checked to ensure they remain operational. Equipment useful to the negotiation team includes, but is not limited to:

(1) A USMC MPI command hostage incident workbook or similar references.

(2) Individual body armor.

(3) Regular cassette tape recorders and 10 hours of tape.

(4) Micro cassette tape recorders and 10 hours of tape.

(5) Electronic monitoring equipment.

(6) Ear microphones for telephones and/or recording and listening.

(7) Portable typewriter/laptop computer.

(8) Field tables and chairs.

(9) Public address systems or bullhorns.

(10) Reliable communications between the TMF and the hostage-takers.

(11) Radios.

(12) Paper and pencils/pens (Admin supplies).

e. Decision Making/Negotiations. Decision makers (CG, or C/S) will never be negotiators. Negotiators will likewise not be used as decision makers. By removing the negotiator from the decision making process helps establish the negotiator as a neutral who appears able to project equally the interest of the terrorist and the interest of society. The negotiator must be able to establish a rapport with the terrorists, which will permit the negotiator to defer decisions and still maintain rapport when demands are delayed

or refused. The psychological concept of transference between hostage taker and negotiator is extremely important. The negotiator should strive to:

- (1) Be a mediator, not an arbitrator.
- (2) Allow terrorists to set the pace, mood, and topic of conversation.
- (3) Accept the terrorist's views neutrally, expressing neither approval nor disapproval.
- (4) Keep the terrorists talking.

f. Negotiators Dress. The negotiators should dress in civilian clothes. This enhances the neutral image of the negotiator, and it blocks out the authoritarian image evoked by a uniform. (The negotiation team, if they are qualified and normally carry firearms, should be armed except during face-to-face negotiations. Face-to-face negotiations are recommended only as a last resort.) A terrorist will not see a person with a weapon as neutral. They may even see them as a direct threat to the terrorists security.

g. Military Police are split into Inner and Outer Perimeter Forces. Depending on the size of the incident site, the fourth team may be augmented or even replaced by the members of the Special Enforcement Branch or members of a Security Augmentation Force (SAF). The inner perimeter security force will operate under direct control of the TMF Commander. The photographic capability of the inner perimeter element could be an experienced Military Police Investigator or NCIS agent. They should be trained in criminal investigation photography. Photographs can identify terrorists or hostages. They can place particular items within the scene surrounding area, and they provide evidence for follow-up legal action. Consider cameras that use self-developing or 35mm film, or videotape (best situation is all three). The EOD support, if available to the inner perimeter element, should have two EOD technicians who can dispose of the explosive devices. The inner perimeter elements consist of:

- (1) One Officer-in-Charge (Military Police Officer).
- (2) One Noncommissioned OIC (Watch Commander).
- (3) Explosive Ordnance Disposal (EOD) support.

(4) Photographic capability.

(5) Personnel as assigned.

h. The outer perimeter security element has either a Military Police Officer or a Military Police Staff Non-Commissioned Officer in charge that is directly responsible to the TMF Commander. The on-site commander sets the site of the outer perimeter security team to fit the needs of the station. Remember, this is a tactical perimeter and any passage of lines must be coordinated. A single entry point is encouraged to eliminate discretion on the part of the members of this element. The outer perimeter may be made up of military police, augmented by other troops on a 4 or 5 to 1 ratio for this mission. Once a special threat incident occurs it is imperative that the Threat Management Force Team is activated and certain actions be taken immediately. It is recommended that each member have a checklist of the actions that should be performed immediately. The TMF Commander maintains copies of these, and each team should have a copy in hand upon arrival at the established command post.

i. After Action Report

(1) An after action report checklist is shown below. It should be expanded to include all important actions and decisions, which took place during the incident. This checklist should be applied immediately following an actual terrorist incident.

(a) Did intelligence sources provide adequate warnings regarding the possibility of an incident occurring?

(b) What level target did the terrorists attack: Primary, secondary, or random?

(c) Were the terrorists able to gather operational intelligence prior to the incident? How?

(d) Which crime prevention areas could have been improved to decrease the probability of the event?

1 Operations security?

2 Personnel security?

3 Physical security?

(e) Consider the Crisis Management Plan. Could it be modified to prevent another attack of this nature? How?

(f) Could the Crisis Management Plan be modified to improve the initial response capability?

(g) Could the Crisis Management Plan be modified to improve response capability during the incident?

(h) What assets could have countered this attack?

(i) What other steps were taken to:

1 Improve your anti-terrorism capability?

2 Improve your counter-terrorism capability?

5004. CRISIS MANAGEMENT TEAM MEMBER CHECKLISTS

1. Chief of Staff (C/S)

a. Be present at the COC.

b. Coordinate the initial notification and periodic updates to the next higher headquarters in accordance with reporting requirements.

c. Verify and approve for electronic message release, the Serious Incident Reports (SIRs) prepared by the G-3.

d. Meet with FBI representatives to determine jurisdiction and available FBI assets for possible scenarios.

e. Provide guidance to subordinates and make operational decisions as required.

2. Provost Marshal

a. Establish immediate contact with the Threat Management Force, and maintain constant monitoring of their activities.

b. Advise and inform the commander on all developments.

c. Contact FBI and local law enforcement agencies.

d. Ensure ingress and egress on installation is controlled.

e. Ensure that all Provost Marshal assets are available as needed.

f. Request permission from NCIS to conduct wire and oral communication interceptions (coordinate with NCIS/SJA), when appropriate.

g. Implement SOP's for bomb, arson, and other threats when appropriate.

3. SJA

a. Be accessible to all elements of the CMT.

b. Provide applicable legal guidance (jurisdiction, use of deadly force, delegation of authority, etc.).

4. PAO

a. Check with Provost Marshal upon entering the COC.

b. Establish a press center.

c. Control media personnel with press passes, escorts, etc.

d. Obtain approval for news releases, media approval, photograph release, and direct communications with press personnel, and suspect.

5. AC/S, G-3

a. Activate the CMT/COC. Alert/notify CMT personnel and ensure their presence in the COC.

b. Ensure COC equipment is present and operational.

c. Ensure other functions of the COC continue normally.

d. Ensure that events occurring at the COC concerning the special threat are recorded.

e. Alert Combat Visual Information Center to provide pictorial and or videotape account of the COC, TMF, and Special Enforcement Branch operations.

6. AC/S, G-1

- a. Check with Provost Marshal upon entering the COC.
- b. Assure access to personnel files on suspects and victims.
- c. Provide other G-1 and personnel assets as required.

7. AC/S, G-4

- a. Check with the Provost Marshal upon entering the COC.
- b. Alert subordinate supply and transportation activities.
- c. Ensure messing is available for CMT, TMF, and Press Center.
- d. Provide other supply/maintenance, and transportation assets as needed.

e. Alert procurement for possible necessary local purchases (e.g., items by TMF or to meet hostage demand; food, drinks, personal item, etc.).

f. Obtain blueprints for facilities involved in the incident.

g. Alert personnel capable of controlling electricity, water, air conditioning, etc., and have them on station stand by for possible use.

8. NCIS

- a. Check with Provost Marshal upon entering the COC.
- b. Ensure a NCIS agent is located with or at the TMF.
- c. Ensure intelligence files are obtained on suspect or suspect's group.
- d. Provide other intelligence assets as required.

9. AC/S, G-6

- a. Check with Provost Marshal upon entering the COC.
- b. Ensure telephone repairmen are available for connecting/disconnecting lines.

- c. Set up backup communication to TMF (field phone, radio).
 - d. Test and set up recording equipment and public address system, as required.
 - e. Provide other communications equipment as required.
10. G-3, Air Operations Officer
- a. Check with Provost Marshal upon entering the COC.
 - b. Brief the status of airfield operations.
11. Medical Officer
- a. Check with Provost Marshal upon entering COC.
 - b. Ensure medical personnel are on site at TMF with ambulance.
 - c. Alert emergency room for possible gunshot and/or trauma victims.
 - d. Alert psychiatric personnel.
12. 3d MAW Representative
- a. Report status/availability of aircraft.
 - b. Provide helicopter assets for use in surveillance, medical evacuation, and/or insertion flights (preferencelight complete and on standby).
 - c. Determine Landing Zone (LZ) nearest to TMF and plan its organization and control.
 - d. Provide other aviation assets as required.
13. MAG-46 Representative
- a. Report status/availability of personnel.
 - b. Report status/availability of aircraft.
 - c. Provide helicopter assets for use in surveillance, medical evacuation, and/or insertion flights (preferencelight complete and on standby).

d. Determine Landing Zone nearest to TMF and plan its organization and control if assigned.

e. Provide other aviation assets as required.

5005. TMF MEMBER CHECKLIST

1. Threat Management Force Commander

a. Ensure on site command post is established out of range and sight of the suspect.

b. Ensure the desk sergeant has made TMF notifications.

c. Ensure communications are established and maintained with the CMT.

d. Send an initial situation report to the CMC.

e. Ensure events are being recorded on an operational log as they occur.

f. Ensure inner and outer perimeters have been established.

g. Ensure innocent personnel are being evacuated.

h. Ensure negotiators have, or are attempting to open communications with the suspect.

i. Check with military police desk sergeant to ensure the team leader's patrol area of responsibility has been assumed by someone else if appropriate.

j. Ensure NCIS, local law enforcement agencies, and the FBI are notified and are prepared to render assistance as needed.

2. Initial Response Force OIC/NCOIC Duties (Isolation of the Scene of Terrorist Action)

a. Ensure the area is properly cordoned so that unauthorized personnel cannot enter unnoticed.

b. Ensure that those personnel attempting to exit the incident area are identified and sent to the assigned area to be interviewed in reference to their knowledge of the incident.

- c. Establish an inner perimeter.
- d. Deploy Marines so that:
 - (1) All exits from suspect's location are observable.
 - (2) Marines are covered and concealed from small arms fire.
 - (3) Marines relay any information observed from their positions.
- e. Prior to arrival of counterintelligence personnel, interview individuals leaving the inner perimeter, or individuals in initial vicinity of the scene, to determine the number of suspects, hostages, and number and type of weapons involved, description of suspects and/or hostages.
- f. The initial response force should immediately record witnesses and witnesses are directed to a safe location for further debriefing.
- g. Brief TMF personnel on the situation upon their arrival.
- h. If possible, the perimeter should only have one point of exit/entrance.
- i. Ensure that personnel not specifically authorized inside the outer perimeter are not permitted entry. The TMF commander must approve all personnel not normally authorized entry.
- j. Check the TMF commander immediately for situation update and orders.
- k. Ensure the evacuation of innocent personnel is completed, or is progressing in a safe/secure manner.
- l. Relay all intelligence gathered to the TMF Commander and data collection personnel (NCIS, CID).

3. Special Reaction Team Commander Duties

- a. Assess the situation.
- b. Check with the TMF Commander immediately.
- c. Ensure all SRT personnel and equipment is present.

- d. Request blueprints of affected building.
- e. Assume inner perimeter.
- f. Coordinate with the TMF Commander for specialized resources, personnel, etc.

(1) SRT Leader. Armed with a side arm and an additional weapon as required. The team leader may also carry a team radio, binoculars, and other essential equipment. The SRT leader is responsible for locating and directing counter fire against targets, creating a plan of attack, and supervising its execution.

(2) SRT Scout. Armed with a sidearm and a semiautomatic weapon or shotgun. This member will carry any equipment necessary to lead the team to its objective, such as a pry bar, manhole hook, or bolt cutter. This team member leads the SRT to the objective by conducting a reconnaissance of the approach and withdrawal routes, building entrances and rooftops, and by removing obstacles such as padlocked doors. After completing the scouting mission, the scout may be assigned a defensive or security role for the team or be designated to participate in the assault.

(3) SRI Marksman. Armed with an M-16A heavy barrel, with a telescopic sight. This team member also carries any specialized equipment designated by the SRT Team Leader. The SRT marksman should be trained and deployed in order to take appropriate action based on the situation.

4. Negotiation OIC Tasks

- a. Check with TMF Commander immediately.
- b. Ensure negotiators and equipment are present.
- c. Ensure all conversation are being recorded and that successive tapes overlap by 30-60 seconds.
- d. Ensure the negotiations team is set up in a separate room or areas, and access is limited to essential personnel only.
- e. Coordinate all information with TMF Commander.

5. Outer Perimeter Security Force OIC tasks

- a. Establish and maintain the area outside the perimeter of the incident scene.

- b. Evacuate and seal off housing and troop billeting areas.
- c. Control access to the incident area and installation.
- d. Guard all critical and restricted areas outside the incident area.
- e. Augment the installation law enforcement mission.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 6

CRISIS MANAGEMENT TEAM MEMBER RESPONSIBILITIES

	<u>PARAGRAPH</u>	<u>PAGE</u>
MEASURES AND RESPONSIBILITIES	6000	6-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 6

CRISIS MANAGEMENT TEAM MEMBER RESPONSIBILITIES

6000. MEASURES AND RESPONSIBILITIES

1. AC/S, G-3

- a. Activate the CMT and COC when directed.
- b. Supervise the CMT and COC.
- c. Prepare Serious Incident Report(s) (SIR) and others as required.
- d. Brief the CG.
- e. Coordinate with 3d MAW to arrange aviation support for the CMF if required.
- f. Exercise the CMT annually.
- g. Maintain a chronological log of all events.

2. Provost Marshal

- a. Supervise the CMF.
- b. Provide a senior representative at the COC.
- c. Ensure communications between the On Site Command Post and the COC.
- d. Develop plans for employment of the CMF.
- e. Conduct the necessary CMF training to include an annual exercise of inner and outer perimeter elements, negotiating teams, and special reaction teams.
- f. Provide security access control for the COC.
- g. Keep the AC/S, G-3 informed of all developments.
- h. Keep the local FBI/NCIS office informed of all developments; coordinate and provide support for the FBI in the event that agency assumes jurisdiction over a terrorist incident.

3. AC/S, G-4

- a. Provide control of utilities as required.
- b. Provide the CMT and CMF with blueprints of facilities as required.
- c. Provide special engineering and maintenance/ repair equipment support as required.
- d. Construct special equipment such as barricades or battering rams as required.
- e. Provide other engineer support as required.
- f. Ensure adequate motor transport and MHE support for the CMF.

4. SJA

- a. Ensure CMT decisions are in compliance with laws and regulations.
- b. Provide legal advice to the CMT.
- c. Provide other legal services as required.

5. AC/S, G-6

- a. Provide expeditious telephone installation, as required, to support the command and negotiator functions of the CMF.
- b. Provide additional portable radios for the CMF.
- c. Establish a secure voice link between the CMF and COC.
- d. Provide personnel to expeditiously turn telephone line off/on.
- e. Provide public address equipment as required.
- f. Provide communication support as required.

6. CG, 3d MAW (AC/S, G-3). Provide assistance as required.

7. CO, MAG-46 (S-3). Provide assistance as required.

8. PAO

a. Serve as sole point of contact for releasing information to the news media.

b. Clear all information releases with the CMT.

c. Coordinate with the media to prevent damaging or counter-productive broadcasts. Inadvertently releasing sensitive information such as CMF plans could alert suspects and undermine the operation.

d. Control movement of all media representatives aboard station. Establish a press center for releasing all authorized information.

9. OIC, Branch Medical Clinic

a. Provide medical support for the CMF with ambulance(s) and trained Emergency Medical Technicians at a staging area prescribed by the CMF commander.

b. Provide victim/suspect medical records for reviews by investigators, psychologists, and negotiators.

c. Provide medical support as required.

10. Miramar Fire Department. Provide EMS support as required.

11. NCIS

a. Provide periodic threat assessments.

b. Provide the CMF and Provost Marshal with negotiators and investigative support.

c. Assume investigative jurisdiction upon resolution of the special threat incident, unless the FBI has assumed jurisdiction in the case of a terrorist incident.

d. Assist in interrogating suspects when required.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 7

PROCEDURES TO COLLECT/ANALYZE INFORMATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	7000	7-3
NAVATAC SUMMARY	7001	7-3
NAVATAC FORCE PROTECTION SUMMARY	7002	7-4
NAVATAC WARNING REPORT	7003	7-4
NAVATAC SPOT REPORT	7004	7-4
NAVATAC THREAT ASSESSMENT	7005	7-4
NAVATAC THREAT BRIEFING	7006	7-4

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 7

PROCEDURES TO COLLECT/ANALYZE INFORMATION

7000. GENERAL

1. The Naval Criminal Investigative Service (NCIS) will be the primary agency to collect/analyze threat information.
2. Terrorist threat assessments, conducted annually or as required, shall be the basis and justification for recommendations on AT/FP enhancements, program/budget requests, and establishing specific unit/installation FPCON measures. The installation AT/FP officer, Physical Security Officer, or another officer designated by the Commander shall conduct these assessments.
3. Vulnerability assessments, conducted at least annually, shall be utilized as a threat based analysis and self-assessment tool to assess the vulnerability of a unit or installation. Vulnerability assessments will be conducted by a task organized, experienced based and functionally oriented team drawn from installation/unit resources. See Chapter 8 for vulnerability assessment procedures.
4. While the assessment of the terrorist threat is a command function, the NCIS maintains a world-wide structure that provides criminal investigative and counterintelligence/AT support to Marine Corps commands, except those combat-related counterintelligence matters within the functional responsibility of the Marine Corps. To fulfill this responsibility, NCIS has established the Navy Anti-terrorism Alert Center (NAVATAC), which processes real time information and operates on a 24-hour basis. The NAVATAC provides the following support to Marine Corps commands:

7001. NAVATAC SUMMARY (ATACSUM)

1. The ATACSUM is sent to all Marine Corps installations and major commands 6 days a week (excluding Saturdays).
2. It provides current operational intelligence on terrorist and related unconventional warfare threats to Department of the Navy (DON) personnel and assets, to include establishing the threat levels for specific geographic areas.

7002. NAVATAC FORCE PROTECTION SUMMARY. The Force Protection Summary is published weekly and lists countries designated by DOD as Medium to Critical terrorist threat levels. Additionally, when changes to country threat levels occur they are published in the Summary.

7003. NAVATAC WARNING REPORT. This report is sent to affected commands. It provides threat specific information on impending or likely terrorist activity, to include establishing, the threat levels for specific geographic areas.

7004. NAVATAC SPOT REPORT. This report is sent to affected commands. It provides indications and warnings of imminent terrorist activity, and advises of activities, conditions, or events that could lead to near-term terrorist operations directed against DON assets or personnel.

7005. NAVATPC THREAT ASSESSMENT

1. This assessment is sent to the following activities upon request:

a. Marine Corps installations.

b. Major Marine Corps tenant commands aboard Marine Corps installations (Marine Divisions, Marine Aircraft Wings, Force Service Support Groups, etc.).

c. Marine Corps units deploying outside of the continental United States. (Deployed units embarked aboard Navy ships in the Mediterranean Sea will automatically receive a threat assessment at least 7 to 10 days prior to commencement of each port call).

2. This threat assessment provides current operational intelligence on terrorist and related unconventional warfare threats, for the geographic area specified, to include the establishment of a threat level for that specific area.

7006. NAVATAC THREAT BRIEFING. This briefing is provided to requesting commands preparing for deployment outside CONUS.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 8

VULNERABILITY ASSESSMENTS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	8000	8-3
REPRESENTATIVES	8001	8-3
ASSESSMENTS	8002	8-4
GOALS	8003	8-4
VULNERABILITY ASSESSMENT CHECKLIST . .	8004	8-4

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 8

VULNERABILITY ASSESSMENTS

8000. GENERAL. Vulnerability assessments shall be conducted at least annually. They should focus on those elements directly related to combating terrorism, and should identify vulnerabilities that may be exploited by threat groups and recommend options to eliminate or reduce those vulnerabilities.

8001. REPRESENTATIVES. The AT/FP Officer will coordinate the completion of the assessments. A task organized, experienced based and functionally oriented team will be drawn from MCAS Miramar. The following departments/divisions will provide a representative, if needed:

1. AC/S, G-3.
2. AC/S G-4.
3. AC/S, G-6.
4. PAO.
5. Provost Marshal.
6. SJA.
7. Branch Medical Clinic.
8. HQHQRON.
9. 3d MAW, AC/S, G-3.
10. Miramar Fire Department.
11. Miramar Commissary.
12. NCIS.
13. Station Explosive Ordnance Disposal.

8002. ASSESSMENTS

1. Assessments shall identify key assets and infrastructures, and address the impact of the loss of key assets and infrastructure to the installations ability to perform its mission. Particular attention should be paid to MEVAs.
2. Assessments should address the functional areas of intelligence/counterintelligence, law enforcement and operations, physical security, civil, electrical or structural engineering, infrastructure, weapons effect mitigation, force protection plans and programs, and local community support.
3. Assessments must evaluate procedures to provide enhanced anti-terrorism protection for areas of high population density (BEQs, dining facilities, housing areas).

8003. GOALS

1. Assessments should assist in identifying:
 - a. Weaknesses in the physical security plans, programs, and structures.
 - b. Inefficiencies and diminution of effectiveness in personnel practices and procedures relating to security, incident control, incident response, and incident resolution.
 - c. Enhancements in operational procedures.

8004. VULNERABILITY ASSESSMENT CHECKLIST. This checklist will assist in the completion of a vulnerability assessment. Not all parts of the checklist may be applicable, nor should assessments be limited to the checklist questions. The checklist is a tool to assist in the assessment, and can be modified to address unique mission or specialized areas of interest as follows:

1. Reason for assessment (annual, command directed).
2. Purpose of the facility/installation.
3. Current threat level assigned by DOD, CINC, State Department.
4. Are there any indigenous terrorist groups in the area?

5. Is there a transitional terrorist threat?
6. What are the land/air routes to the facility?
7. Do the basic topographic features near the facility have an affect?
8. What type of perimeter security exists (barriers, control systems, locks, detection devices, lighting)?
9. Who mans and controls perimeter security?
10. Describe normal facility operations in terms of work hours, personnel identification, access control.
11. Analyze vehicle parking.
12. How are mail and small packages processed at the facility?
13. How does the facility warn personnel of emergencies?
14. How are contractors, vendors, and visitors identified, granted access, and controlled once they enter the installation/facility?
15. Are rations stored in a secure location?
16. Are there emergency rations?
17. Is security provided for the main and emergency power sources?
18. Are there alternate communications?
19. Is there emergency services support?
20. What assets would a terrorist target?
21. What capabilities do they have?
22. Which would be effective against targets assessed as likely?
23. What might be early signs of an attack?
24. What avenues of approach would be used to reach a target?
25. How well protected are those targets?

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 9

PHYSICAL SECURITY PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
INFORMATION	9000	9-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 9

PHYSICAL SECURITY PROCEDURES

9000. INFORMATION. The AT physical security measures shall integrate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum AT protection to personnel and assets. The measures include detection, assessment, delay, denial, and notification.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 10

RANDOM ANTI-TERRORIST MEASURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
PURPOSE	10000	10-3
INFORMATION	10001	10-3
SAMPLE MEASURES	10002	10-3
MATRIX	10003	10-6

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 10

RANDOM ANTI-TERRORIST MEASURES

10000. PURPOSE. Random Anti-terrorism Measures (RAMs) assist in setting variations in security routines, to make it harder for terrorists to identify important assets, building detailed descriptions of significant routines, or predictable movements within a targeted facility or installation. These measures will increase Anti-terrorism/Force Protection awareness for Marines, DOD personnel, their families, and all visitors. This will also increase alertness among law enforcement and security personnel. The measures can also reduce adverse operational impacts and unplanned economic costs when enhanced AT/FP measures are maintained for extended periods.

10001. INFORMATION

1. The approach to implementing the RAMs is to identify, at any Threat Condition, a set of measures extracted from higher FPCON measures already in place. A RAM program can help identify those measures that security personnel and the installation infrastructure are more capable of sustaining and those that will be duly stressful on human and material resources. RAM programs change the security atmosphere surrounding the installation. Such programs when implemented in a random fashion alter the external appearance or security "signature" of the installation.
2. Each unit on the installation may develop additional RAMs for their facilities. They must institute the directed installation RAMs. The installation AT/FP officer and security forces must have a copy of the RAMs and be notified of the implementation.
3. The impact of RAM programs on terrorist are difficult to measure, but such programs introduce uncertainty for planners and organizers for terrorist attacks just as terrorists have introduced uncertainty in planning, organizing, training and movement of DOD resources throughout the world.

10002. SAMPLE MEASURES. The RAM program should include the entire installation. The following are sample measures that can be implemented.

1. During duty hours, have personnel conduct interior/exterior inspections of their facilities for suspicious objects.
2. Have all vehicle trunks and cargo areas opened for inspection.
3. Institute parking restrictions around selected facilities.
4. Have all incoming mail trucks searched by Military Working Dogs (Drug or bomb).
5. Verify all commercial deliveries by telephone to the company and receiving agency.
6. Establish random posting of security personnel at soft targets (should be during peak hours).
7. Establish bag and parcel inspection points at facility entrances.
8. Institute bag restrictions at clubs, dining halls, and recreation centers.
9. Change routes of buses.
10. Vary reporting hours of units.
11. Man facilities twenty-four hours that are normally closed.
12. Post the security augmentation force on all Threat Condition posting.
13. Provide personal security detail to high-risk personnel.
14. Switch vehicles of high-risk personnel or executives.
15. Institute the barrier plan at gates or selected facilities.
16. Require all visitors to facilities to be escorted.
17. Deploy tactical sensors around avenues of approach
18. Have local law enforcement patrol the perimeter frequently.
19. Relocate essential functions from their primary location to their alternate.

20. Post additional personnel at sentry gates during hours of darkness or randomly throughout the day.
21. Require two types of identification to enter the installation.
22. Establish checkpoints throughout the installation.
23. Have installation personnel man parking lots to check identification of personnel.
24. Perform counter-surveillance around the installation.
25. Initiate neighborhood watch patrols in base housing.
26. Conduct courtesy patrols through local clubs.
27. Strategically place mockup cameras around the installation.
28. Use portable lighting on portions of the perimeter.
29. Dispersal of equipment throughout the installation (relocate motor pool assets).
30. Alternate pick-up locations for school children.
31. Institute security ride-along on school and city buses.
32. Have utility personnel initiate checks of installation infrastructure.
33. Place portable sensors around vulnerable points of facilities and infrastructure.
34. Institute call back procedures for all visitors.
35. Conduct inspections of food deliveries using medical personnel.
36. Have family members and all other vehicle operators conduct vehicle bomb inspections prior to entering vehicles.
37. Have high-risk personnel park in spots other than their reserved spots.

10003. MATRIX. A matrix system could be used to implement RAMs throughout the installation. Personnel responsible for instituting RAMs should be tasked with maintaining the matrix. The principle of randomness should be maintained when implementing the program and the frequency can vary from weekly to monthly. Table 4.1 gives an example of a matrix system:

Table 4.1. RAM MATRIX

RAM Number *	Location	Frequency	Minimum Time	Remarks
2	All gates	Daily	1 ½ hour	CO directs number of vehicles
5	All facilities	Weekly	All day	
12	Billeting	Monthly	Night Shift	
7	3d MAW units	Quarterly	2 hours	
1	All facilities	Monthly	1 hour	
4	Commissary & Exchange	Monthly	During operating hours	

* Numbers correspond to the RAMs the installation has developed.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 11

SECURITY AUGMENTATION FORCE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BACKGROUND	11000	11-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 11

SECURITY AUGMENTATION FORCE

11000. BACKGROUND. Reference (h) establishes policy and procedures for combating terrorism at the installation and unit level, and mandates the establishment of an augmentation force as part of a CMF to counter terrorist activity. The installation AT/FP Plan establishes security measures for the protection of MCAS, Miramar, and also requires that a security force, to assist Military Police and Flightline Security Forces, be constituted. Additionally, there may be other requirements inherent to the station mission, or contingencies that may arise (natural disasters, etc.) which necessitate the immediate response of a force to augment permanently assigned personnel.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 12

BARRIER PLANS

	<u>PARAGRAPH</u>	<u>PAGE</u>
INFORMATION	12001	12-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 12

BARRIER PLANS

12000. INFORMATION. The barrier plan is designed to harden gate entrances and protect Mission Essential Vulnerable Areas (MEVAs), and critical infrastructure located on MCAS, Miramar. The barrier plan is executed when the installation assumes FPCON Charlie or when directed by the CG in response to an emergency or special situation. The Provost Marshal maintains diagrams showing the barrier placement at each gate entrance as well as around MEVAs and other critical infrastructure. These diagrams also show where barriers are stored when not in use. Since buses cannot navigate the barriers around the gates, an alternate commercial bus route may be implemented.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 13

WEAPONS OF MASS DESTRUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
INFORMATION	13000	13-3
ASSUMPTIONS	13001	13-3
TASKS	13002	13-5

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 13

WEAPONS OF MASS DESTRUCTION

13000. INFORMATION

1. The threat of Weapons of Mass Destruction (WMD) terrorism is different than the threat of NBC use on a battlefield. As events in Tokyo (1995 Sarin attack), New York City (1993/2001, World Trade Center), and Oregon (1984 Salmonella Bacterium attack) indicate, the use of chemical and biological agents in a terrorist attack are not only possible, but have been well planned and executed. These attacks have been successful and terrorized millions. This Chapter outlines the actions MCAS Miramar will take to mitigate or prevent the use of WMD aimed at the Air Station.

2. While the fielded U.S. Military is educated, trained, and equipped to operate in a "NBC" environment, the rear areas and non-deployed forces are less so. To a terrorist looking to terrorize the U.S., an installation makes an inviting target. Many areas on the installation naturally tend to congregate large masses of unprotected people i.e., the exchange, family housing and military schools, the movie theater, and troop formations. Positive, proactive measures should be in place to help lessen the effects of a WMD attack.

13001. ASSUMPTIONS

1. There is an increased possibility of a WMD attack due to the relative ease of access to chemicals, explosives, and plan designs for devices.

2. A WMD scenario will exceed the crisis response/consequence management capabilities of base resources.

3. Extensive DOD, state and federal support will be required to cope with a WMD scenario.

4. Incidents involving WMDs are often a combination of three types of incidents. Potentially, it could be a hazardous materials incident, a mass casualty incident, and a crime scene.

5. Chemical/biological WMD incidents pose significant problem for first responders.

6. The Air Station should maintain the capability to contain WMD incidents until the arrival of DOD, state, and federal response forces.
7. Mass casualty planning should supplement this Chapter. See Chapter 14 (Mass Casualty Response).
8. The Base should maintain Mission Oriented Protective Posture (MOPP) Zero for the air station in accordance with reference (g). This includes the ability to detect and monitor the presence of chemical, biological, and radiological agents.
9. Protective equipment and training is best suited for first responders i.e., emergency medical services, firefighters, and military policemen. This can include MOPP 4 protective gear (excluding Firefighters), OSHA level A equivalent, detection equipment, and a heightened awareness for the presence of NBC agents.
 - a. Equipment for first responders:
 - (1) CBR Protective Masks.
 - (2) CBR Protective Suits (Saratoga's, Jlists, Level A and B Self-contained).
 - (3) CBR Detection Equipment.
 - b. Provide initial and sustainment training for all possible first responders. Possible first responders include PMO, Fire Department, EMS and Hospital personnel, Commissary Exchange personnel and EOD. The following is a list of the basic training:
 - (1) WMD Basic Awareness course.
 - (2) WMD First Responders Awareness course.
 - (3) WMD First Responders Operations course.
 - (4) WMD Incident Command course.
10. Decontamination measures consist of rinsing with gross amounts of water/bleach mixture.

13002. TASKS. On a continuing basis, and in conjunction with State and Federal Agencies, MCAS Miramar will be prepared to respond to a WMD incident by conducting pre-incident planning and mitigation measures and performing crisis response/ consequence management operations aimed at lessening the effects of a WMD incident.

1. COC

a. Obtain initial report from first responders and determine location of incident.

b. Conduct downwind hazard predictions based on information from the on-site Commander.

c. Maintain communications with the incident on-site Commander.

d. Activate appropriate elements of the MOA/MOUs: monitor augmentation from both civilian and military forces

e. Notify the installation population via the Mass Notification System.

f. Organize the COC's incident information boards to include the following information: event situation/status; event casualty damage summary; weather status; evacuation status; area closing status; shelter facility status; resources/equipment status; hospital bed availability; contracts/agreements/services; maintain an incident log.

g. Collect, process, and disseminate information about the WMD emergency to facilitate the overall response activities.

h. Establish automated NBC Warning and Reporting Systems/ Networks (integrate with Global Command and Control System, if available).

i. Establish preformatted/preaddressed messages for release of information into NBCWRS.

j. Initiate reporting to higher headquarters.

k. Issue NBCWRS reports upon notification of suspected incident or actual incident.

2. CG, MCAS Miramar

- a. Retain jurisdiction for WMD incidents and be prepared to establish a unified command relationship with responding federal, state, and county forces.
- b. Exercise command and control through the CMT.
- c. Employ the CMF to deal with the threat.
- d. Consult with 3d MAW to consider the movement of all aircraft aboard MCAS Miramar to an alternate location to reduce the chance or level of contamination.

3. AC/S, G-3

- a. When directed by the CG, convene the CMT.
- b. Activate the COC.
- c. Consider implementing increased FPCONS.
- d. Prepare and submit installation After Action Report.

4. AT/FP Officer

- a. In conjunction with NBC, retain primary staff planning for WMD.
- b. Conduct regular training events to validate and update MWD procedures. Ensure training exercises involve WMD scenarios.
- c. Ensure WMD plans integrate available DOD, state, and federal response force and resources.

5. Special Agent in Charge, NCIS. Ensure all sources of intelligence are used to develop a WMD threat assessment. Consider the following:

- a. Terrorist group who have used or have the capability to use WMD.
- b. What type of agents have been used?
- c. What are the means of delivery?

6. Incident Commander

a. Observe. Evaluate the situation and report to dispatch:

- (1) Unit designation. Who is on-scene?
- (2) A brief description of the situation (e.g., building size, occupancy, multi-vehicle accident, etc.).
- (3) Obvious conditions (e.g., HAZMAT spill, multiple victims, traffic conditions, weather conditions, key terrain, etc.)
- (4) Description of initial action(s) taken (e.g. establish perimeter, shut down traffic).
- (5) Obvious safety concerns (e.g. we are being shot at approach from the East).
- (6) Assumption, identification, and location of the Command Post.
- (7) Request or release resources, as required.
- (8) Crowds, witnesses, and suspects.

b. Identify contingencies. Think about what can happen. Murphy's Law applies during emergency events because they are unplanned and involve danger, risk, and confusion.

- (1) Nothing is as easy as it looks.
- (2) Everything takes longer than you think it will.
- (3) If anything can go wrong, it will.

c. Determine Objectives. Decide what you want to do. Objectives are:

- (1) Measurable.
- (2) Used to monitor incident progress and establish priorities.
- (3) Based on situation and contingencies - Define the problem and courses of action.

d. Identify Resource Requirements

- (1) What resources?
- (2) Do you have them?
- (3) Where will you get them?
- (4) How long to get them?
- (5) Other agencies needed?
- (6) Special requirements?

e. Build an Incident Action Plan and Management Structure

- (1) Responsibilities - Who will do what?
- (2) On-scene Command Structure - Who will report to whom?
- (3) Coordination - How will different groups work together, and how will they communicate?

f. Take Action: Possible actions for incident stabilization

- (1) Establish Command.
- (2) Mobilize resources.
- (3) Set up a staging area.
- (4) Isolate the area. Establish inner and outer perimeter (as the situation dictates) and traffic control points.
- (5) Treat/assist injured.
- (6) Establish primary and alternate routes for egress, ingress, and evacuations.
- (7) Establish a resource staging area.
- (8) Issue warnings. The situation may require that safety warnings be issued to responding forces in order to prevent injury, and or damage to surrounding people and property.
- (9) Initiate an evacuation.

- (10) Establishing liaisons.
- (11) Pass the word (make notifications).
- (12) Establish safe contact with suspect.
- (13) Notify key personnel.
- (14) Deploy special units (tactically).
- (15) Debrief witnesses/suspects/key personnel.

7. OIC, Branch Medical Clinic

- a. Ensure Emergency Medical Service (EMS) personnel are equipped and trained to handle NBC contaminated victims.
- b. Liaison with Station NBC for use of a reasonable number of Nerve Agent Antidote Kit NAAK MK 1 kit's (Atropine and 2 PAM Chloride) when needed.
- c. Provide an on-scene medical officer to coordinate/supervise triage and evacuation actions.
- d. Advise local hospitals to prepare for the receipt of NBC contaminated victims.
- e. Be prepared to execute the Mass Casualty Plan.
- f. Establish a procedure for patient tracking and accountability.

8. Provost Marshal

- a. Ensure military police personnel are equipped and trained to respond to NBC contaminated incident scenes.
- b. Ensure military police personnel maintain an on-scene capability to identify NBC agents.
- c. Establish procedures for dispatchers to query/identify incoming calls for potential WMD incidents.
- d. Establish cordon based on weather conditions.
- e. Recommend the activation of the CMF as required.

9. Miramar Fire Department

a. Ensure fire-fighting personnel are trained to respond to and isolate NBC contaminated incident scenes. Utilize the Hazardous Incident Response Team (HIRT) for initial cleanup, and San Diego Navy PWC HAZMAT team for clean-up.

b. Establish procedures for dispatchers to query/identify incoming calls for potential WMD incidents.

c. Be prepared to perform normal fire-fighting duties in addition to WMD first responder responsibilities.

d. Recommend the activation of the CMF as required.

10. AC/S, G-4. Consider WMD protection in the design of all new construction projects.

11. OIC, EOD

a. Be prepared to operate in an NBC environment.

b. Be prepared to render safe IEDs in an NBC environment.

12. Station NBC. Determine available resources and assist in the acquisition of a reasonable number of Nerve Agent Antidote Kit NAAK MK 1 kit's (Atropine and 2 PAM Chloride) when needed. Coordinate with Branch Medical Clinic.

13. Coordinating Instructions

a. Priority of consequence management actions for incident responders:

(1) Control/containment of incident site and surrounding areas.

(2) Perform rescue operations for survivors.

(3) Decontamination of injured.

(4) Triage and evacuation of injured.

(5) Collection and preservation of evidence.

(6) Collection and identification of the deceased.

(7) Site clean up and HAZMAT disposal.

(8) Return incident site to normal operations.

b. The installation's primary responsibility is containment of the agent and the rescue those individuals believed to be alive.

c. All victims of a chemical or biological agent attack will be hastily decontaminated before evacuation to a medical facility. Patient decontamination is achieved by:

(1) Remove victim from Hot Zone.

(2) Remove contaminated clothing.

(3) Rinse with gross quantities of water and/or using various decontamination solutions.

d. Identification/classification of chemical, biological, and nuclear materials is obtained by using various detection devices.

(1) Biological Smart Tickets can be used to identify biological warfare agents Bacillus Anthracis (Anthrax), Yersinia Pestis (Plague), Botulism (Bot Pox), and Staphylococcus Enterotoxin B (SEB).

(2) Chemical warfare agents are detected using M256A1 kits, Drager Colormetric tubes, M8 and M9 paper, Photoionization detectors, and an APD 2000 chemical warfare agent detector. The APD 2000 is the modern version of the Improved Chemical Agent Monitor (ICAM).

(3) Nuclear materials are detected by using an AN/PRD-77 Radiac Set. The PDR-77 detects and measures alpha, beta, gamma and x-ray radiation.

e. Per reference (g), maintain MOPP level Zero for ten percent of the station military population.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 14

MASS CASUALTY RESPONSE

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	14000	14-3
MASS CASUALTY RESPONSE OBJECTIVES . .	14001	14-4
MASS CASUALTY PLAN ACTIVATION	14002	14-4
TASKS	14003	14-4

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 14

MASS CASUALTY RESPONSE

14000. GENERAL

1. Mass casualties can occur from any number of incidents including, but not limited to, building fires, aircraft mishaps, terrorist attacks, or natural disasters. For the purpose of this order, the assumption is that casualties have been caused by a terrorist incident.
2. In the event of a terrorist incident, law enforcement takes the lead and determines when casualties can be treated. If a bomb was used, they need to locate and ensure that the area is safe and free from other explosive devices. If one or more terrorists caused the casualties, they must be dealt with before sending Fire Department and Branch Medical Clinic EMS personnel onto the scene. PMO must safeguard the scene and make it safe for rescue personnel to do their jobs.
3. In the event of a mass casualty incident, the Miramar Fire Department is likely to be the initial emergency care provider. The Fire Department will establish a joint command center to deal with the incident. The Fire Department is the incident commander and will assume joint control with PMO if a law enforcement issue arises. The Fire Department will also assume joint control with the ARFF if the incident is located on the airfield involving an aircraft.
4. The Fire Department has connectivity with various agencies within San Diego County and can request assistance from San Diego County emergency response assets. The Fire Department Dispatch is responsible for activating Annex D. Annex D is the Unified San Diego County Emergency Service Organization, Operational Area Emergency Plan for providing multiple casualties with emergency medical care.
5. The Miramar Fire Department has established mutual aid agreements with San Diego County Fire/Emergency Medical Service agencies and the San Diego City Fire Department. San Diego County has an established emergency medical system. This system involves an organized emergency response system with fire and EMS agencies. Local hospitals within the county are designated trauma hospitals.

6. All San Diego County agencies implement the Standardized Emergency Management System-Incident Command System (SEMS-ICS). The Fire Department will implement the SEMS-ICS for any mass casualty incident. The Fire Department assumes the role of Incident Commander under SEMS criteria and manages medical operations within the statewide fire management system.

14001. MASS CASUALTY RESPONSE OBJECTIVES

1. Ensure timely coordinated medical assistance, to include evacuation of severely ill and injured patients.
2. Coordinate utilization of medical facilities and the procurement, allocation, and distribution of medical personnel, supplies, communications, and other resources.

14002. MASS CASUALTY PLAN ACTIVATION

1. Activation occurs upon confirmed notification of multiple casualties exceeding local medical capabilities.
2. Activation may occur for an imminent event of such magnitude that extensive casualties are inevitable.

14003. TASKS

1. Provost Marshal
 - a. Isolate the crime scene and ensure that it is clear before allowing EMS assets to enter.
 - b. Provide crowd and traffic control.
 - c. Establish staging areas for EMS vehicles.
 - d. Establish and maintain ingress and egress routes for emergency vehicles.
 - e. Provide perimeter control.
 - f. Provide evacuation coordination.

- g. Provide tactical communications.
- h. Provide a representative to the Incident Command Post.

2. Miramar Fire Department

- a. Establish a Joint Incident Command Post with PMO/ARFF.
- b. Notify the nearest hospital (i.e., Sharps Memorial) of the disaster, via activation of the San Diego Emergency Disaster Plan named "Annex D."
- c. The following agencies should be notified of pertinent information (such as the nature of the emergency, location, number injured).

(1) All hospitals in the affected area will coordinate with EMS regarding the Base Hospital designation.

- (2) Private ambulance coordinator.
- (3) Mercy Air aeromedical ambulance.
- (4) Emergency Medical Services.
- (5) California Highway Patrol.
- (6) Sheriff ASTREA.
- (7) Medical Examiner.
- (8) Office of Disaster Preparedness.
- (9) Red Cross.

- d. Establish the ICS Multi-Casualty Branch.
- e. Provide fire fighting.
- f. Provide extrication.
- g. Provide rescue.
- h. Provide initial triage and medical support.

- i. Maintain communication with the County EOC.
- j. Determine need for treatment teams on scene.
- k. Identify the hazardous material along with personnel for decontamination, if needed.

3. OIC, Branch Medical Clinic

- a. Provide medical support with ambulances and trained Emergency Medical Technicians.
- b. Prepare the clinic to receive casualties.
- c. Upon arriving on scene, assume responsibility for triage and prioritizing patient evacuation.
- d. Provide medical support as required.
- e. Provide a Medical Boss to the Incident Command Post and a representative to the COC upon activation.

4. OIC, ARFF

- a. Assist fire-fighting effort.
- b. Provide initial triage and medical support.
- c. Provide representative for the Incident Command Post and the COC upon activation.

5. AC/S, G-4

- a. Provide a representative to the COC upon activation.
- b. Coordinate and provide transportation for evacuation and movement of personnel, goods, and equipment.
- c. Assist registering personnel evacuated to on-base evacuation shelters.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 15

BOMB THREAT RESPONSE

	<u>PARAGRAPH</u>	<u>PAGE</u>
BOMB THREAT PHASES	15000	15-3
LETTER AND PACKAGE BOMBS	15001	15-3
PREVENTIVE MEASURES	15002	15-3
ACTION	15003	15-4
EVACUATION GUIDELINES	15004	15-6

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 15

BOMB THREAT RESPONSE

15000. BOMB THREAT PHASES. A bomb threat incident for planning purposes may be divided into various phases. Such phases may not always follow the predictable sequence and some will not necessarily occur.

1. Receipt of Bomb Threat Phase. A bomb threat may be received as a suspicious package, a written message, or most commonly, a telephone call.

2. Evacuation Phase. The decision to evacuate rests with the commanding officer/department head in charge of the building or facility threatened. When competent authority cannot be contacted, Military Police may also order an evacuation.

3. Search Phase. The Military Police will supervise all search activities and that search teams will include command personnel who are familiar with the building/facility. A search may be conducted before, after, or without an evacuation.

4. Identification/Disposal Phase. EOD personnel will identify and dispose of suspected explosive devices. If not already accomplished, evacuate personnel from the affected area.

5. Re-entry Phase. The decision to re-enter a building or facility rests with the commanding officer/department head in charge of the building or facility after the search and/or disposal phases are complete.

15001. LETTER AND PACKAGE BOMBS. Letter and package bombs vary in size, shape, and components. They may have electric, non-electric, or other sophisticated detonating systems.

15002. PREVENTIVE MEASURES. Particular attention must be given to reducing the opportunity to place a bomb or explosive device aboard the installation.

15003. ACTION

1. Unit Commanders/Department Heads. Formulate bomb threat procedures to include:

a. Instructions for duty officers and watch officers concerning the procedures to be implemented upon receipt of a bomb threat.

b. Designate personnel to make decisions to evacuate (involves the movement of aircraft, patients, minor children, the mode of movement, final destination).

c. The recall of key personnel familiar with the threatened facility to assist designated search personnel.

d. A diagram of the facility to assist search personnel.

e. Prompt notification of the Military Police.

f. Order evacuation if required.

g. Provide personnel for search teams.

2. Provost Marshal

a. Assume on-scene operational control of the bomb threat scene.

b. Notify all departments needed to assist with bomb threat.

c. Establish safe staging area for support personnel and equipment.

d. Establish security perimeters and control the access of personnel to and from the threatened site.

e. Provide crowd and traffic control at the scene.

f. Provide personnel to augment search teams.

g. Keep emergency vehicles to a minimum. Code lights or sirens should not be used.

h. If competent authority cannot be contacted and an evacuation of the building/facility is required, order an evacuation.

i. Conduct a search with teams of Military Police and organizational/departmental personnel.

j. Ensure radio transmissions are ceased within 300 meters of the bomb threat area to prevent a possible Electromagnetic Radiation (EMR) detonation.

k. If no device is found, make appropriate notifications canceling the threat.

3. Miramar Fire Department

a. Dispatch fire-fighting equipment as directed by the Provost Marshal or senior representative on scene.

b. Assist in rescue operations as directed.

c. Ensure radio transmissions are ceased within 300 meters of the bomb threat area to prevent a possible EMR detonation.

4. AC/S, G-4

a. Dispatch emergency maintenance personnel and equipment as required by PMO. (Personnel familiar with gas and electrical turn off procedures).

b. Make keys available to maintenance areas of the concerned location.

c. Assist in rescue operations as directed by the Provost Marshal or the senior representative on scene.

d. Provide drawings/sketches of the location, as needed.

e. Keep emergency vehicles to a minimum.

f. Ensure radio transmissions are ceased within 300 meters of the bomb threat area to prevent a possible EMR detonation.

5. OIC, Branch Medical Clinic

a. Dispatch ambulance(s) to the scene as directed.

b. Prepare to administer first aid.

c. Keep emergency vehicles to a minimum. Code lights or sirens should not be used.

d. Ensure radio transmissions are ceased within 300 meters of the bomb threat area to prevent a possible EMR detonation.

6. OIC, EOD

a. Provide ordnance/bomb identification training for Military Police and unit personnel, as required.

b. Upon notification of a bomb threat, duty EOD personnel will stand by at building 21020 until the threat is over or a possible device is located.

c. If a possible device is located, respond to the scene, check in with the incident commander and handle as appropriate.

15004. EVACUATION GUIDELINES

1. The decision to evacuate a building/facility as a result of a bomb threat rests with the person responsible for the personnel and government assets contained therein.

2. Orders to evacuate a building/facility should be given a calm and quiet manner so as to not create panic.

3. Personnel should be instructed to conduct a brief search their individual area, room, or office for suspicious items.

4. Drawers, doors, closets, cabinets, and other containers should be left open and unlocked to facilitate search operations.

5. Windows and doors should be opened to reduce the shock effect of a bomb explosion.

6. Evacuated personnel should be kept together in a safe area at least 300 meters from the threatened area. Due to their familiarity with the threatened area, these personnel will be needed for information and to participate in search operations.

7. A muster or roll call should be taken at the collection/gathering site. This will facilitate verification that all personnel have been evacuated should an actual explosion occur.

8. Consideration should be given to using alternate safe areas. This will reduce the opportunity for terrorists to target the safe areas if no pattern is established.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 16

HAZMAT PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL	16000	16-3
HAZARDOUS MATERIALS RESPONSE LEVELS . .	16001	16-3
RESPONDER ACTIONS TO A HAZMAT/WMD INCIDENT	16002	16-4

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 16

HAZMAT PROCEDURES

16000. GENERAL. The MCAS Miramar Fire Department is the primary responder for hazardous material emergencies on board MCAS Miramar. In an emergency involving a hazardous material (HAZMAT) incident the Miramar Fire Department will take appropriate actions to identify, control and contain the spill. The Miramar Fire Department has the responsibility to declare a working HAZMAT incident and to determine the level of response needed.

16001. HAZARDOUS MATERIAL (HAZMAT) RESPONSE LEVELS

1. Level 1, First Responder. HAZMAT spill/leak that can be safely controlled and contained at the first responder level.
2. Level 2, HAZMAT Team, Safety Officer. Mitigation steps or the spill situation requires the assistance and equipment of a single HAZMAT Team with a qualified Safety Officer.
3. Level 3, Two HAZMAT Teams, HAZMAT Coordinator, Safety Officer. Large scale incident or a spill situation that requires the efforts of two or more HAZMAT Teams with a HAZMAT Coordinator. A high risk situation involving a hazardous substance that threatens the health of people and/or the environment.
4. The Miramar Fire Department personnel will not perform spill cleanup activities.
5. The Miramar Fire Department will determine when a HAZMAT scene is controlled and contained.
6. The Miramar Fire Department shall contact the San Diego Fire Department (SDFD) HAZMAT Incident Response Team (HIRT) when mitigation is beyond the level of the first responders.
7. The SDFD HIRT is a regional HAZMAT emergency response program of the San Diego County Unified Disaster Council. The program calls for HAZMAT emergency response to be provided County-wide through the joint efforts of the SDFD HIRT and the San Diego

County Department of Health Services' HAZMAT Management Division (HMMD). MCAS Miramar has contracted with HIRT to provide HAZMAT response services.

8. Under this program, a combined response is provided. The SDFD HIRT is responsible for isolating and containing the incident, stopping the release, effecting rescues and other related tasks. The HMMD is responsible for assessing the risk to public health and safety and the environment, taking steps to mitigate these hazards, and insuring adequate clean-up of the area.

9. The SDFD HIRT will respond at the request of the Miramar Fire Department. The SDFD HIRT does not assume responsibility for scene management. MCAS Miramar maintains full control and authority over the incident and retains responsibility for any release of public information concerning the incident.

10. The Miramar Fire Department will coordinate with PMO to isolate the incident area.

11. The Miramar Fire Department will coordinate with SDFD HIRT, and 3d MAW for the location of decontamination sites.

16002. RESPONDER ACTIONS TO A HAZMAT/WMD INCIDENT

1. Protect yourself.
2. Isolate the area.
3. Position equipment.
4. Avoid contamination.
5. Control the scene.
6. Corral casualties.
7. Use defensive contamination control.
8. Gather and report critical information.
9. Perform emergency decontamination.
10. Set up decontamination stations.

11. Assist with first aid.
12. Assist with technical decontamination.
13. Preserve evidence.
14. Watch for secondary devices.
15. Document actions taken on scene.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 17

PHYSICAL SECURITY/ANTI-TERRORISM/FORCE PROTECTION
WORKING GROUP

	<u>PARAGRAPH</u>	<u>PAGE</u>
PURPOSE	17000	17-3
ACTIONS	17001	17-3
QUARTERLY MEETINGS	17002	17-4

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 17

PHYSICAL SECURITY/ANTI-TERRORISM/FORCE PROTECTION WORKING GROUP

17000. PURPOSE

1. The purpose of this group is to identify the members and establish quarterly meetings as required per the references. The purpose of the working group is to provide a means by which the Commanding General can gain full staff involvement in program design and implementation of security/anti-terrorism/force protection issues aboard MCAS Miramar.

2. All aspects of the Anti-terrorism posture of the Station will be discussed during Physical Security/Anti-terrorism/Force Protection Working Group meetings. During these meetings various topics will be addressed and their philosophy, purpose, and operational procedures discussed.

17001. ACTION. The AC/S, G-3 will coordinate the quarterly Physical Security/Anti-terrorism/Force Protection Working Group meetings, normally held in Building #9211, COC, and announce the exact time/date of the meeting. Members of the group will include the below listed members or their designated representative:

1. Chief of Staff, MCAS, (Chairman).
2. AC/S, G-1.
3. AC/S, G-3.
4. AC/S, G-4.
5. AC/S, G-6.
6. AC/S, G-8.
7. AC/S, MCCA.
8. CO, HQHQRON.
9. A 3d MAW representative

10. Counsel.

11. PAO.

12. SJA.

17002. QUARTERLY MEETINGS. The Physical Security/Anti-terrorism/Force Protection Working Group will facilitate the following items:

1. Meet quarterly or when directed by the CG, MCAS Miramar.
2. Develop and distribute the installation threat assessment and recommend those areas to be designated as vital to national security or inherently dangerous to others aboard MCAS Miramar.
3. Evaluate the AT plan.
4. Evaluate the effectiveness of the current AT program.
5. Recommend priorities for the commitment of AT resources.
6. Evaluate the results of AT related inspections, surveys, exercises and recommend corrective action.
7. Review existing regulations, directives, and plans to ensure that the installation can support an anti-terrorism/force protection program.
8. Proposed agenda items will be forwarded to the AT Officer for discussion/review at the next scheduled Physical Security/Anti-terrorism/Force Protection Working Group meeting.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 18

TRAINING

	<u>PARAGRAPH</u>	<u>PAGE</u>
FORMAL ANTI-TERRORISM TRAINING	18000	18-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 18

TRAINING

18000. FORMAL ANTI-TERRORISM TRAINING

1. General. The cornerstone of the Marine Corps AT program and the best deterrent against terrorism is an alert, educated, combat-ready Marine. To achieve the required level of training and education, a thorough and dynamic program has been designed to ensure all Marines, their dependents, and all other assigned military and civilian personnel are capable of protecting themselves and performing their duties while countering the terrorist threat.

2. Level 1, Pre-deployment Training

a. Individual awareness training conducted for all deploying Marines, Sailors, DOD civilians, and deploying family members scheduled for OCONUS deployments. Training focuses on the following categories.

b. Negligible/Low Threat Areas and Medium/Higher Threat Areas.
Note: Personnel falling under the cognizance of MARFORPAC will receive all Level I training at least annually, regardless of deployment status. Personnel will get Level 1 training which includes: Receive the Marine Corps approved program of instruction (POI) by a certified Level II instructor (instruction in terrorist operations, individual protective measures, terrorist surveillance techniques, improvised explosive device, attacks-kidnapping & hostage survival, explanation of terrorism threat levels and FPCON), and two documents: the Joint Staff Guide 5260, "Service Member's Personal Protective Guide: A Self-help to Combating Terrorism," and the "Anti-terrorism Individual Protective Measures" (AIPM) wallet card; view the Service-selected personal awareness video; receive an Area of Responsibility (AOR) specific threat brief.

3. Level II. Training focuses on the training of the unit level AT/FP Officer in order for them to conduct Level 1 training programs. Completion of Level II training is requisite for assignment as a unit AT/FP Officer.

4. Marine Corps training programs for combating terrorism are designed to heighten terrorism awareness among individual Marines. These programs consist of:

a. Threat awareness instruction in all entry level training programs, as well as annual follow-on awareness training at the unit level.

b. Supporting Marine Corps Institute (MCI) correspondence courses.

c. Mobile training teams (MTT) from a variety of Marine Corps and external sources.

d. Terrorism instruction in formal Marine Corps schools.

e. Innovative use of news and production media by PAO, and the Combat Visual Information Center.

5. The following specialized training courses are available for Marines involved in physical or personnel security programs. Quotas and funding will be allocated by CMC (POS) or CG MCCDC (T&E).

a. Course Title: Anti-terrorism Instructor Qualification Course.

Location: U.S. Army, John F. Kennedy Special Warfare Center, Ft. Bragg, North Carolina (2 weeks).

Purpose/Scope: Designed to train already well-qualified instructors in anti-terrorism measures. Students are required to prepare and deliver several blocks of instruction on such topics as terrorist history and organizations, awareness and avoidance, and hostage survival methods.

b. Course Title: Terrorism Counteraction on Military Installations.

Location: U.S. Army, Military Police School, Fort McClellan, Alabama (1 week).

Purpose/Scope: Designed for personnel serving in, or assigned to security staff positions supporting combating terrorism efforts. It teaches Marines proactive and reactive methods for developing a systematic approach to effectively counter the terrorist threat aboard bases and stations.

c. Course Title: Individual Terrorism Awareness Course.

Location: U.S. Army, John F. Kennedy Special Warfare Center, Ft. Bragg, North Carolina (1 week).

Purpose/Scope: Designed for Marines who are scheduled for overseas assignments to a moderate or higher threat area, to include deployments. It provides Marines with information on victim avoidance, and those countermeasures designed to reduce the risk of terrorist attack in a high threat environment. Course also teaches individual survival methods for Marines taken hostage.

d. Course Title: Dynamics of International Terrorism.

Location: U.S. Air Force, Hurlburt Field, Florida (1 week).

Purpose/Scope: Provides selected personnel with a basic understanding of the theory, psychology, organization, technique and operational capability of terrorist groups on an international and regional basis.

e. Course Title: High Risk Personnel (HRP) Course.

Location: Weapons Training Battalion, MCCDC, Quantico, Virginia (5 days).

Purpose/Scope: Designed to train personnel in special shooting techniques which may be required in a high risk area. This course is restricted to personnel actually designated to fill overseas high-risk billets.

f. Course Title: Anti-terrorism/Force Protection Principal Advisor Course and Anti-terrorism Training Officer Course.

Location: Expeditionary Warfare Training Group, (Atlantic), Norfolk, Virginia and Fleet Training Center, (Pacific), San Diego, California. (1 week).

Purpose/Scope: Focuses on such topics as terrorist history and organizations, awareness and avoidance, and hostage survival methods. Qualifies the students as unit AT/FP Officers to advise their commanders on AT/FP matters as well as conduct Level I training.

g. Course Title: Evasive Driving.

Location: Summit Point, West Virginia.

Purpose/Scope: Designed to train personnel in evasive driving tactics, including defensive/offensive driving, route surveillance, counter-surveillance, and psychology and awareness required to initiate protective measures. Intended for personnel driving for VIP's with the potential to be in high threat areas, or personnel who are required to drive themselves in a high threat environment.

6. The following specialized training course is available for active duty judge advocates. Quotas and funding will be allocated by CMC (JAS).

Course Title: Legal Aspects of Terrorism (5F-F43)

Location: The Judge Advocate General's School, U.S. Army, Charlottesville, VA (HQMC Course ID A0658M1).

7. Information on additional related courses of instruction is available from CMC (POS-10) at DSN 224-4177/2180, Comm: (703) 614-4177/2180.

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 19

DEFINITIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
DEFINITIONS	19000	19-3

ANTI-TERRORISM/FORCE PROTECTION PLAN

CHAPTER 19

DEFINITIONS

19000. DEFINITIONS

1. Anti-terrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to acts of terrorism, to include limited response and containment by local military forces.
2. AT Awareness. Fundamental knowledge of the terrorist threat and measure to reduce personal vulnerability to acts of terrorism.
3. AT Resident Training. Formal classroom instruction in designated DOD courses that provide specialized instruction on specific combating terrorism topics; i.e., personal protection, terrorism an analysis, regional interest, and AT planning.
4. Barrier. A coordinated series of obstacles designed or employed to canalize, direct, restrict, delay, or stop the movement of an opposing force, and to impose additional losses in enemy personnel.
 - a. Active Barrier. A barrier is considered active if it requires action by personnel or equipment to permit entry.
 - b. Fixed-Barrier. A barrier system is fixed if it is permanently installed, or if heavy equipment is required to move or dismantle the barrier.
 - c. Manmade Barrier. A roadblock, gate, fence, etc., employed to restrict the normal flow of personnel and traffic in and around designated activities.
 - d. Movable Barrier. A movable barrier system can be transferred from place to place. It may require heavy equipment or personnel to assist in the transfer.
 - e. Natural Barrier. Pre-existing terrain and topographical features such as a river, mountain, or similar feature that offers stand-off, and provides a buffer zone around areas such as flight line restricted areas.

f. Passive Barrier. A barrier is passive if its effectiveness relies on its bulk or mass, and it has no moving parts. Such a system typically relies on weight to prevent entry into a restricted area.

g. Portable Barrier. A portable barrier system is used as a temporary barrier. A movable-system can be used, but may take increased time, money, or effort.

5. Barrier Plan. Typically a part of the installation physical security plan, the barrier plan is designed to enhance the security of specific facilities and areas aboard an installation by ensuring that barriers are properly planned for and prudently installed. The plan should acknowledge types of barriers available and needed for different priority assets. Other concerns such as special skills and equipment to place barriers should be addressed.

6. Combating Terrorism (CbtTerr). Actions, including AT and CT, taken to oppose terrorism throughout the entire threat spectrum.

7. Countermeasures. Impairment of the operational effectiveness of the enemy by the employment of devices and/or techniques.

8. Counter-intelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organization or persons, or international terrorist activities, but not including personnel, physical document, or communication security programs.

9. Counter-surveillance. All measures, active or passive, taken to counteract hostile surveillance of friendly activity. Counter-surveillance should be done as unobtrusively as possible, or in a passive mode.

10. Counter-surveillance Plan. Typically a part of the installation physical security plan, the counter-surveillance plan allows for the detection of surveillance efforts by hostile intelligence agents.

11. Counter-terrorism (CT). Offensive measure taken to prevent, deter, and respond to terrorism.

12. Crisis /Consequence-Management Plan. Typically a part of the installation physical security plan, the crisis/consequence management plan includes responsive measures for various types of crisis situations. It outlines specific duties and

responsibilities of the installation's CMT and CMF. The installation operations officer normally has responsibility for the development of the crisis management plan, in coordination with key installation staff. The crisis management portion of the plan should provide for worst-case scenarios, without reinforcements. The plan should provide measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. Likewise, the consequence management portion of the plan should provide measures to protect public health and safety, restore essential installation operations and services, and provide emergency relief to affected individuals.

13. Crisis Management. Involves measures to resolve a hostile situation, and to investigate and prepare a case for prosecution.

14. Consequence Management. Addresses the consequences of an incident, and involves measures to alleviate damage, loss, hardship or suffering.

15. Family Member. That definition used for "dependent" found in Title 10, United States Code, Section 1072(2) (spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild under 21, incapable of self support or under 23 and enrolled in a full-time institution). See 10 U.S.C. 1072 (2) (1994) for the complete definition.

16. Force Protection. A security program designed to protect military personnel, employees, family members, facilities, and equipment in all locations and situations. Accomplished through a systematic approach that integrates the planning and application of combating terrorism, physical security, operations security (OPSEC), and personal protective measures supported by intelligence, counter-intelligence, and other security programs.

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

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

19. High-Risk Targets. U.S. material resources and facilities that, because of mission sensitivity, ease of access, isolation, or symbolic value, may be an especially attractive or accessible terrorist target.
20. Hostage. A person held as a pledge that certain terms or agreements will be kept. Hostage taking is prohibited by both domestic and international law. Hostage taking violates article 34 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War. The parties to the Geneva Conventions of 1949 are obliged to search for and either try or extradite persons (regardless of nationality) alleged to have committed, or to have ordered to be committed, grave breaches. The Hostage Taking Act (18 U.S.C. § 1203) prohibits the seizure or detention and threatening of a person in order to compel a third person or a governmental organization to do or abstain. From doing any act as an explicit or implicit condition for the release of the person detained. If the person seized or detained is a U.S. national, such a seizure or detention is a crime, regardless of whether the act occurred inside or outside of the United States.
21. Indicators. In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action.
22. Inner Perimeter. The boundary marking the area closest to the crisis point. The inner perimeter element normally takes no action against hostile elements without the approval of the CMF commander. Ordinarily, only law enforcement and security forces operate within the inner perimeter.
23. Military Services. Includes the Army, Navy, Air Force, and the Marine Corps. Also includes the Coast Guard under agreement with the Department of Transportation, when it is not operating as a military service in the Navy. Also identified as DOD Components.
24. Mission Essential Vulnerable Areas (MEVA). Areas aboard a military installation designated by the commander as essential to the accomplishment of the installation mission. A MEVA list should be included in every installation physical security plan.
25. Navy Antiterrorist Alert Center (NAVATAC). An element of the Naval Criminal Investigative Service (NCIS), which provides indications weekly summaries, warnings, and current operational intelligence on potential terrorist or unconventional warfare activities that are threats to Department of the Navy (DON) personnel, property or assets worldwide.

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

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

c. Non-State Supported Terrorism. Terrorist groups who operate autonomously, receiving no significant support from any government.

d. State-Directed Terrorism. Terrorist groups that operate as agents of a government, receiving substantial intelligence, logistical, and operational support from the sponsoring government.

e. State-Supported Terrorism. Terrorist groups that generally operate independently, but receive support from one or more governments.

26. Weapons of Mass Destruction (WMD). Weapons capable of a high order of destruction and/or being used in such a manner as to destroy large numbers of people. The weapons may be nuclear, chemical, biological, or radiological, but exclude the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon.