DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

IN REPLY REFER TO:
MCO 3302.1D
PSH
18 Jul 2002

MARINE CORPS ORDER 3302.1D

From: Commandant of the Marine Corps
To: Distribution List

Subj: THE MARINE CORPS ANTITERRORISM/FORCE PROTECTION (AT/FP) PROGRAM

Ref: (a) JPUB 1-02 of 12 Apr 01
(b) SECNAVINST 3300.2A (NOTAL) of 21 Mar 01
(c) DOD Instruction 2000.16 (NOTAL) of 14 Jun 01
(d) JPUB 5-03.2 of 15 Mar 92
(e) JPUB 3-07.2 of 17 Mar 98
(f) FMFM 7-14
(g) MCO 5000.17A
(h) MCO 5500.14A
(i) MCRP 3-02E
(j) MCO P5530.14
(k) MCO 5740.2F
(l) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93
(m) MCI 02.10b
(n) CJCS Instruction 5261.01 (NOTAL) of 1 Jul 01
(o) MCO P5580.2A
(p) CJCS Instruction 3610.01A (NOTAL) of 1 Jun 01
(q) MCO 1553.1B
(r) DOD Directive 4500.54G (NOTAL) of 5 Jan 92
(s) CJCS 5260 (NOTAL) of 1 Jan 97
(t) MCO 3460.1A
(u) MCRP 5-12.1C
(v) DTRA FP Security Classification Guide (NOTAL) of Feb 01
(w) DOD Directive 2310.2 (NOTAL) of 30 Jun 97
(x) DOD Directive 1300.7 (NOTAL) of 8 Dec 00
(y) DOD Instruction 1300.21 (NOTAL) of 8 Jan 01

Encl: (1) Definitions
(2) Vulnerability Assessment
(3) Terrorist Threat Assessment
(4) Criticality Assessment
(5) Risk Assessment
(6) Terrorism Threat Level
(7) Force Protection Conditions (FPCONs)
(8) Terrorism Incident Response and Terrorism Consequence Management
(9) Subordinate Element Missions
(10) Sample Antiterrorism/Force Protection (AT/FP) Plan
(11) Antiterrorism Training Programs and Requirements
(12) Terrorism/Law Enforcement/Security Internet Websites and Telephone Helplines
(13) Security Screening and Specialized Training for Marines Selected for Assignment to Hazardous Billets
(14) References
(15) Inspector General's 480 Checklist

DISTRIBUTION STATEMENT B: Distribution authorized to U.S. Government agencies only. Other requests for this publication must be referred to the sponsor.

1. Situation. Marines, sailors, civilian employees, family members, our installations, facilities, and infrastructure are symbols of the United States of America, the Marine Corps and our way of life. As such, they are all potential targets for terrorism.

a. The Department of Defense (DOD) definition of terrorism, which can be found in reference (a), DOD Dictionary of Military and Associated Terms, and enclosure (1) of this Order 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.

b. Combatting terrorism activities can be divided into two components:

(1) Antiterrorism (AT): Defensive measures taken to reduce vulnerability to terrorist acts, to include limited response and containment by local military forces.

(2) Counterterrorism (CT): Offensive measures taken to prevent, deter, and respond to terrorism (defined above).

These actions are taken to oppose terrorism throughout the entire threat spectrum.

c. Force protection as defined in reference (a) and enclosure (1), is actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

d. The term antiterrorism/force protection (AT/FP) associates the concept of defensive measures taken to reduce vulnerabilities with the definition of who and what is being protected. AT/FP therefore, encompasses those defensive measures taken to deter, detect, delay, defend, mitigate, and recover from a terrorist attack thereby reducing the vulnerability of Marines, sailors, civilian employees, family members, Marine Corps equipment, facilities and installations, information and information systems, critical infrastructures, and other materiel resources. An AT/FP plan implements these actions.

(1) The cornerstone of the Marine Corps AT/FP program and the best deterrent against terrorism is an alert, educated, combat-ready Marine.

(2) 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, sailors, family members, and civilian employees.

(3) Marines in leadership positions, regardless of rank, have a responsibility to ensure that Marines, sailors, civilian employees, and family members are properly prepared to meet, counter, and survive the terrorist threat. To this end, commanders must focus on those areas that can best be influenced, such as: training and education, proper operational planning, and the provision of the necessary resources to provide the best possible level of protection.

(4) Local AT/FP plans should consider and incorporate the aspects of terrorism consequence management and intelligence support to be complete.

e. The threat of terrorism comes from both foreign (transnational) and domestic sources as well as Government-sponsored and nongovernmental organizations.

(1) Because terrorist organizations are not generally capable of directly opposing the military strength of the U.S. in a force-on-force scenario, they will employ asymmetric warfare to place their strengths against our weaknesses. Terrorism provides the terrorists with a force projection far beyond their conventional military means.

(2) The asymmetric warfare threat posed by terrorists includes, but is not limited to: bombings, shootings, kidnappings, arson, hostage-taking, hijacking, seizure, raids/attacks, sabotage (including environmental sabotage), the use of weapons of mass destruction, information warfare, and the use of chemical, biological, radiological, nuclear, and high yield explosives (CBRNE).

(3) Terrorist organizations have a proven capability to use innovative, unconventional techniques to accomplish their mission. It is therefore incumbent upon commanders to creatively employ an effective AT/FP program to protect the assets and personnel under their control.

f. Per reference (b), DON Antiterrorism/Force Protection (AT/FP) Program and reference (c), DOD Antiterrorism Standards, the Commandant of the Marine Corps is responsible for implementation of DOD AT/FP standards and policies for the Marine Corps. This Order establishes policy, responsibilities, procedures, and standards for the conduct of the Marine Corps AT/FP program.

(1) This Order provides guidance and establishes specific procedures for defending against terrorism at the installation and unit level. Additionally, it provides for measures to increase the security and safety of based, deploying, and traveling Marine Corps personnel, family members, and civilian employees.

(2) This Order implements reference (b), DON Antiterrorism/Force Protection (AT/FP) Program and reference (c), DOD Antiterrorism Standards. References (d) through (y) provide additional guidance on specific aspects of combatting terrorism, force protection, and physical security.

2. Cancellation. MCO 3302.1C, MCO 5500.13B, and NAVMC 2927

3. Mission. Commanders shall immediately develop, implement, and maintain effective AT/FP plans in order to deter, detect, delay and defend against attack; mitigate the effects of an attack, and preserve and reconstitute Marine Corps combat power following attack.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. It is Marine Corps policy to protect military personnel and civilian employees, their families, Government facilities, and materiel resources from acts of terrorism, criminal acts, and destructive or potentially destructive events. Commanding officers will develop an operational capability that provides defense in depth against all threats. Commanding officers will be guided by the provisions of this Order in attaining the measures needed to be both proactive and reactive toward acts of terrorism and other criminal and hostile acts. Enclosures (1) through (15) to this Order have been developed and sequenced to support this intent.

(2) Concept of Operations

(a) Commanders at all levels are required to develop prescriptive AT/FP standards based on the type of unit, installation location, potential threat and operating environment. These standards shall include the minimum force protection condition (FPCON) measures listed in enclosure (7) as well as unit/installation threat specific FPCON measures.

(b) Commanders at all levels shall clearly establish AT/FP operational responsibility for all units and individuals whether permanently or temporarily assigned. When responsibilities for AT/FP overlap and are not otherwise governed by law, a specific DOD policy, or appropriate memorandum of agreement/memorandum of understanding (MOA/MOU), the geographic Combatant Commander's force protection policies will take precedence over all force protection policies or programs within the Combatant Commander's area of responsibility. Commanders in overseas locations shall coordinate their AT/FP efforts with the Combatant Commander, host-nation authorities, and the U.S. embassy as appropriate. Reference (c), DOD Antiterrorism Standards applies.

b. Subordinate Element Missions. See enclosure (9).

c. AT/FP Plan Development

(1) The development of a sound, proactive AT/FP plan is accomplished through a logical step-by-step process that utilizes the Marine Corps Planning Process (MCPP). Each unit/installation required to develop an AT/FP plan by this Order will establish an AT/FP working group. AT/FP working group membership shall consist of the unit/installation antiterrorism officer (ATO) and other members selected for their wide range of experience and knowledge. Working with the commander, the AT/FP working group will analyze the mission. Then, using the risk analysis process described in this Order, the AT/FP working group will develop appropriate courses of action (COA), wargame the COA, and select for implementation the COA that best accomplish the AT/FP mission. Thereafter, an AT/FP plan is developed to support the COA. By following the processes outlined in this Order and the MCPP, the AT/FP working group will be able to develop a comprehensive AT/FP plan that complies with DOD and Marine Corps requirements and enhances force protection for assigned personnel and their families.

(2) The foundation upon which the risk analysis for the AT/FP plan is built is a vulnerability assessment that considers the wide range of identified and projected terrorist threats, weapons and tactics against a specific location, unit or installation's personnel, facilities, and other assets. Whenever any of these factors change, vulnerabilities must be reassessed to ensure they are properly addressed in the AT/FP plan. The vulnerability assessment, combined with information developed in the criticality and terrorist threat assessments, is analyzed and a risk assessment developed. At this point, the AT/FP working group can consider and incorporate into the plan COA that will deter, detect, delay, defend, mitigate (terrorist incident response measures) and recover (terrorism consequence management measures) from the effects of a terrorist attack or other critical incident such as a natural disaster or HAZMAT incident. These actions and plans then become the basis for requests through the budget process for AT/FP program funding. The result of this process is the identification of an AT strategy encompassing the principles of force protection, physical security, incident response, and consequence management.

(3) The enclosures contained in this Order have been included to assist the ATO and the AT/FP working group in the development of the AT/FP plan and to provide additional working resources.

(a) Enclosure (1) provides definitions the AT/FP working group will find useful when discussing AT/FP issues and developing AT/FP plans and programs.

(b) Enclosure (2) provides guidance on development of a local vulnerability assessment.

(c) Enclosure (3) provides guidance on development of a terrorist threat assessment.

(d) Enclosure (4) provides information on the conduct of a criticality assessment.

(e) Enclosure (5) provides information on the conduct of a risk assessment.

(f) Enclosure (6) provides information on DOD terrorism threat level methodology.

(g) Enclosure (7) provides information on the development of localized force FPCON and the development of site-specific AT/FP measures. An AT/FP plan with a complete listing of site-specific AT measures, linked to a FPCON, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP plan, the specific AT measures and FPCON remain unclassified but shall be handled as FOR OFFICIAL USE ONLY documents.

(h) Enclosure (8) provides guidance on the development of local terrorism incidence response and terrorism consequence management programs.

(i) Enclosure (9) provides guidance on subordinate element missions that must be addressed in an installation/unit AT/FP plan.

(j) Enclosure (10) contains a sample AT/FP plan and is available on-line. Access to this website can be obtained from the appropriate Marine forces headquarters intelligence section through the chain-of-command or from Headquarters Marine Corps, Security Division.

(k) Enclosure (11) contains an explanation of antiterrorism training programs and requirements including predeployment and career development AT/FP training standards and schools available. Additional course listings can be found in reference (l), DOD Antiterrorism Handbook.

(l) Enclosure (12) is a listing of terrorism/law enforcement/security internet websites and telephone helplines available for assistance/information regarding threat and AT/FP program development. Specific requests for assistance should be made through the chain-of-command.

(m) Enclosure (13) provides direction on the identification of high-risk billets and the identification and training of personnel assigned to those billets.

(n) Enclosure (14) contains a comprehensive listing of references used in this Order.

(o) Enclosure (15) contains a checklist of actions that are directed by this Order and its enclosures.

5. Administration and Logistics. This Order contains operational information for official U.S. Government use only, thus distribution is limited to U.S. Government agencies. Requests for release of this document outside the U.S. Government must be made to the Commandant of the Marine Corps (PS).

6. Command and Signal

a. Signal. This Order is effective on the date signed.

b. Command

(1) Applicability. This Marine Corps Order is applicable to the Marine Corps Total Force.

(2) Command Relationships

(a) The Department of Justice (DOJ) is the lead agency for combatting domestic terrorism. Within the DOJ, the Federal Bureau of Investigation is the lead agency for handling and investigating domestic terrorist acts committed in the U.S.

(b) The Department of State (DOS) is the lead agency for combatting terrorism against American personnel and facilities outside the U.S. The DOS is also responsible for the foreign relations aspect of domestic terrorism.

(c) The Federal Aviation Administration has exclusive responsibility for the direction of any law enforcement activity affecting the safety of persons aboard aircraft involved in aircraft piracy.

(d) Federal law, interagency agreements, status-of-forces agreements, international agreements, and MOA/MOUs determine the DOD combatting terrorism role. Military policies, directives, and plans support the DOJ and DOS under applicable Federal laws or MOA/MOUs. The DOD retains the command and control of military forces involved in combatting terrorist operations.

E. R. BEDARD
Deputy Commandant for
Plans, Policies, and Operations

DISTRIBUTION: PCN 10203214100

Copy to: 7000110 (55)
8145005 (2)
7000006, 007, 017, 028, 034, 060, 064, 099, 144, 260/
8145001 (1)

DEFINITIONS

This enclosure provides definitions of terms that will be useful to the commander, antiterrorism officer (ATO), Antiterrorism/Force Protection (AT/FP) working group, and others in the discussion of AT/FP issues and development of an AT/FP plan.

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

2. Asymmetric Warfare. Tactics employing unanticipated or nontraditional approaches to leverage inferior tactical or operational strength against a government's or society's vulnerabilities to achieve disproportionate destructive and psychological effect.

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

4. Antiterrorism Officer (ATO). The installation, base, regional, facility, or unit AT advisor charged with managing the AT program for the commander.

5. AT Plan. An AT plan contains the specific measures taken to establish and maintain an AT program.

6. AT Program. An AT program is a collective effort that seeks to reduce the likelihood that Department of Defense (DOD) affiliated personnel, their families, facilities and materiel will be subject to a terrorist attack, and to prepare to respond to the consequences of such attacks should they occur.

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

8. Barrier. A coordinated series of obstacles designed or employed to channel, direct, restrict, delay, or stop the movement of an opposing force, and to impose additional losses in personnel, time and equipment on the opposing force. Barriers can exist naturally, be manmade, or a combination of both.

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 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 standoff, 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 manpower effort.

9. 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 emplace barriers should be addressed.

10. Base Cluster Operations Center (BCOC). A command and control facility that serves as the base cluster commander's focal point for defense and security of the base cluster. The BCOC is the command post for emergency operations when the BCOC concept is in effect.

11. Combatting Terrorism. Actions, including AT (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (CT)(offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

12. Consequence Management. Those measures taken to protect public health and safety, restore essential government services, and provide relief to governments, business and individuals affected by the consequences of a chemical, biological, nuclear, and/or high-yield explosive situation. For domestic consequence management, the primary authority rests with the states to respond and the Federal Government to provide assistance as required.

13. Counterintelligence. 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.

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

15. Countersurveillance. All measures, active or passive, taken to counteract hostile surveillance of friendly activity. The countersurveillance should be done as unobtrusively as possible, or in a passive mode.

16. Countersurveillance Plan. Typically a part of the installation physical security plan, the countersurveillance plan allows for the detection of surveillance efforts by hostile intelligence elements.

17. Counterterrorism (CT). Offensive measure taken to prevent, deter, and respond to terrorism.

18. Crisis Intelligence Cell (CIC). A CIC may be established in response to a terrorist or other crisis incident. The CIC is designed to coordinate the intelligence, investigative and criminal information needs of the installation and on-scene operational commander. The CIC should be physically separated from the emergency operations center and the crisis management force (CMF) commander. It should be linked to both, however, by a wide variety of wire

and wireless communication means, including a direct data link. The CIC may be staffed by representatives from NCIS, counterintelligence, CID, civilian law enforcement agencies, and others depending upon the commander's requirements and the availability of assets. The design of the CIC should be flexible, to allow for the rapid integration of other Federal, state, and local agencies, as appropriate. See enclosure (6).

19. 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 crisis management team (CMT) and crisis management force (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.

20. Crisis Management. Measures to resolve a hostile situation and investigate and prepare a criminal case for prosecution under Federal law. Crisis management will include a response to an incident involving a weapon of mass destruction, special improvised explosive device, or a hostage crisis that is beyond the capability of the lead Federal agency.

21. Crisis Management Force (CMF). An organic response force capability for crisis situations. The CMF falls under the operational control of the installation provost marshal.

22. Crisis Management Team (CMT). The CMT coordinates the installation's response to and recovery from a variety of critical incidents, including terrorism. It identifies infrastructures and key assets critical to the installation's operation (e.g., MEVAs). The CMT and physical security council may be combined.

23. DOD-Designated High Physical Threat Countries. Geographic areas determined to be of significant terrorist threat to DOD travelers, as designated by the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict (ASD (SO/LIC)) in coordination with the Assistant Secretary of Defense, International Security Affairs (ASD (ISA)), the Assistant Secretary of Defense, International Security Policy (ASD (ISP)), and the Deputy Under Secretary of Defense, Strategy and Resources (DUSD (S&R)).

24. DOD-Designated Potential Physical Threat Countries. Geographic areas determined to be of potential terrorist threat to DOD travelers, as designated by the ASD (SO/LIC) in coordination with the ASD (ISA) and the ASD (ISP), and the DUSD (S&R).

25. DOD Terrorism Threat Analysis Methodology. In AT, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups, which could target a facility. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. The DOD methodology consists of analyzing four factors; the terrorist organization's operational capability, its intentions, activity, and the operating environment the terrorist organizations area of operations.

26. Domestic United States. For AT, the Continental United States (CONUS), also referred to as the lower 48 states, plus Alaska and Hawaii.

27. Family Member. That definition used for "dependent" found in 10 U.S.C. § 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 educational institution). See 10 U.S.C. § 1072 (2)(1994) for the complete definition.

28. Force Protection. Actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive e time an place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

29. High-Risk Billet. Authorized personnel billets (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.

30. High-Risk Personnel (HRP). 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.

31. 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.

32. 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 U.S.

33. Indicator. 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.

34. 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.

35. Intelligence Support. The collection and dissemination of terrorism related information.

36. 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.

37. Mission Essential Vulnerable Areas (MEVA). Areas aboard a military installation that contain assets designated by the commander as essential to the accomplishment of the installation mission. A prioritized MEVA list should be included in every installation physical security plan.

38. Multiple Threat Alert Center (MTAC). An element of the Naval Criminal Investigative Service (NCIS), which serves as the fusion point and production center within the Department of the Navy (DON) for all terrorist, criminal, cyber, and counterintelligence information indicative of a threat to DON assets throughout the world. The MTAC processes real time information and operates on a 24-hour basis to provide commanders with a timely and common operational picture of security threats and vulnerabilities to reduce risks to Marine Corps forces and assets.

39. Outer Perimeter. A boundary established outside the inner perimeter to a crisis point. The outer perimeter provides a broad buffer zone between innocent bystanders and the crisis point. The outer perimeter is characterized by posts, barriers, and an entry control point.

40. Overseas. For AT, all areas outside of the Continental U.S. (OCONUS) except for Alaska and Hawaii which are considered part of the Domestic U.S.

41. Physical Security. That part of security concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment, installations, material, and documents, and to safeguard them against espionage, sabotage, damage and theft.

42. Random Antiterrorism Measures (RAM). The implementation of multiple security measures in a random fashion. When activated, RAMs provide a "different look" at security procedures in effect, to deny the terrorist surveillance team the opportunity to accurately predict security actions. The plan is used throughout all force protection conditions (FPCONs) and consists of using selected security measures from higher FPCONs, as described in enclosure (7), as well as other measures not associated with FPCONs. Using a variety of additional security measures in a normal security posture prevents overuse of security forces, as would be the case if a higher FPCON were maintained for an extended period of time. RAMs are implemented in a strictly random manner, never using a set time frame or location for a given measure.

43. Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

44. Special Reaction Team (SRT). A SRT is a team of specially trained military police personnel, operating under the auspices of the installation provost marshal, armed and equipped to respond to and resolve special threat situations beyond the scope of normal law enforcement capabilities.

45. Terrorism. The calculated unlawful use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies, in the pursuit of goals that are generally political, religious, or ideological.

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 that 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.

46. Terrorism Consequence Management (TCM). TCM is DOD preparedness and response for mitigating the consequences of a terrorist incident including the terrorist use of a weapon of mass destruction. DOD consequence management activities are designed to support the lead Federal agency (domestically, Federal Emergency Management Agency; overseas, DOS) and include measures to alleviate damage, loss of life, hardship or suffering caused by the incident; protect public health and safety; and restore emergency essential Government services.

47. Terrorist Incident Response Measures. A set of procedures in place for response forces to deal with the effects of a terrorist incident.

48. Terrorism Intelligence Cell. See Crisis Intelligence Cell (CIC).

49. Terrorism Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity that identifies the specific weapons and/or tactics that a terrorist organization is capable of using against the installation. This assessment is the planning tool that identifies the full range of threats the AT/FP working group uses to conduct the annual vulnerability assessment.

50. Terrorist Force Protection Conditions (FPCON). A DOD-approved system standardizing the department's identification of and recommended preventative actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principle means for a commander to apply an operational response to protect against terrorism and facilities. The FPCON system allows the military services to more easily coordinate responses to terrorist threats.

51. Vulnerability

a. In AT, a situation or circumstance, if left unchanged, that may result in the loss of life or damaged to mission-essential resources.

b. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or will to fight diminished.

c. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

52. Vulnerability Assessment. The process the commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining antiterrorism measures that, can protect personnel and assets from terrorist attacks.

53. Weapons of Mass Destruction (WMD). Any weapon or device that is intended or has the capability of a high order of destruction and/or being used in such a manner as to destroy large numbers of people. Can be a chemical, biological, radiological, nuclear, or large explosive device. The definition excludes the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon.

VULNERABILITY ASSESSMENT

1. General

a. The vulnerability assessment is the foundation upon which the antiterrorism/force protection (AT/FP) plan is built. In addition, it is the first step in the risk management process. It complements the criticality assessment and threat assessment and completes the picture of how a unit or installation might be attacked. There are two types of vulnerability assessments that a unit must consider. The first is an assessment of the particular area where the unit will be operating and the second is an assessment of the unit's own vulnerabilities. Previous vulnerability assessments should be reviewed to ensure that vulnerabilities identified earlier have been adequately addressed.

b. Assessments will consider the full range of identified and projected terrorism threats against a specific location or installation, personnel, family members, facilities and other assets, as identified in the threat matrix. Vulnerability assessments should focus on those elements directly related to combating terrorism, including the prevention of terrorist acts, and if prevention fails, limiting mass casualties. Assessments should identify vulnerabilities that may be exploited by threat groups and recommend options to eliminate or reduce those vulnerabilities.

c. Commanders shall conduct vulnerability assessments at least annually. In-coming commanders should acquire and familiarize themselves with the most recent vulnerability assessment available and conduct a new vulnerability assessment upon assumption of command. Assessments will be classified in accordance with the Defense Threat Reduction Agency (DTRA) Force Protection (FP) Security Classification Guide (NOTAL) of Feb 01.

d. Commanders shall identify those unit assets likely to become terrorist targets, paying particular attention to mission essential vulnerable areas (MEVAs), as defined in enclosure (1) of this Order. Commanders shall develop procedures for enhanced antiterrorism protection of MEVAs during periods of increased threat.

2. Sources of Vulnerability Assessments

a. The Joint Staff, through the DTRA, conducts Joint Staff Integrated Vulnerability Assessments (JSIVAs), and CMC (PS) conducts Marine Corps Integrated Vulnerability Assessments (MCIVAs). All Marine Corps installations will be subject to a JSIVA, MCIVA or other joint or Marine Corps-sponsored vulnerability assessment at least once every 3 years. These assessments may occur more frequently by request or in response to emergent threats. The benchmarks used by JSIVA and MCIVA teams for the conduct of their vulnerability assessments can be valuable tools in the development of vulnerability self-assessment. These benchmark guidelines are available on-line. Access to this website can be obtained from the appropriate Marine forces headquarters intelligence section through the chain-of-command or from CMC (PS).

b. Port Integrated Vulnerability Assessments and Airfield Vulnerability Assessments are available from organic intelligence/counterintelligence assets, the Naval Criminal Investigative Service or via the chain-of-command.

c. Geographic Combatant Commander vulnerability assessments may also be available such as USEUCOMs Joint Risk Assessment Management Program.

d. Vulnerability self-assessments (local assessments) shall be conducted by all installations and units (squadron/battalion and above) at least once per year. A unit's AT/FP program should be subject to continual assessment to avoid complacency and to benefit from experience. It should also appropriately reflect the span-of-control of the commander and focus on critical items the commander may be able to influence. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts and changing local conditions make periodic assessments essential.

e. Higher headquarters vulnerability assessments will be conducted on lower-level units at least once every 3 years to ensure unity of AT/FP efforts throughout subordinate commands. Vulnerabilities identified during a higher headquarters vulnerability assessment shall be prioritized, tracked and reported to the next general/flag officer specifying the action to be taken to correct the vulnerabilities identified.

(1) At installations that are shared (i.e., where the Marine Corps is a tenant), a higher headquarters vulnerability assessment completed by the installation satisfies the 3-year assessment requirement for units located within the confines of the assessed installation. Higher headquarters vulnerability assessments satisfy the annual requirement for a local vulnerability assessment.

(2) Higher headquarters vulnerability assessments shall be conducted at housing areas, facilities, activities and installations that:

(a) consist of 300 or more personnel on a daily basis;

(b) installations whose existence has a direct bearing on the war fighting capabilities of the Marine Corps or the U.S.;

(c) any facility bearing responsibility for emergency response; and,

(d) facilities with the authority to interact with local non-military host-nation (HN) agencies or having agreements with other agencies or HN agencies to procure these services.

(3) Higher headquarters vulnerability assessments may be conducted as necessary to identify time-critical requirements or emergent needs.

3. Vulnerability Assessments at Installations. Vulnerability assessments of facilities and installations will address the broad range of physical threats to security of personnel and assets at least annually. The vulnerability-based analysis will identify vulnerabilities that may be exploited and suggest options.

a. Vulnerability assessments shall assess the following functional areas:

(1) AT/FP plans and programs. Specifically, the installation's AT/FP plan and its ability to accomplish the requirements of this Order and other prescriptive standards that have been established.

(2) Counterintelligence, law enforcement liaison, and intelligence support assessment shall focus on the ability to receive threat information and warnings from higher headquarters and local resources, collect information on the threat and process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment will examine the ability to disseminate threat information to subordinate commands, tenant organizations, in-transit units, assigned or visiting personnel and how that process supports the implementation of appropriate force protections measures. The ability to disseminate threat information should include a "flash" system to deliver high value information as rapidly as possible.

(3) AT/FP physical security measures shall be assessed to determine the unit's ability to protect personnel by detecting, deterring, delaying or defending against acts of terrorism. Physical security techniques include procedural measures such as: perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks, and armed response to warning or detection; and physical security measures such as: fences, lights, intrusion detection, access control, closed-circuit television cameras, personnel and vehicle barriers, biological, chemical and radiological agent detectors and filters, and other security systems. The assessment should consider commercial-off-the-shelf AT/FP technology where existing technology or procedural modifications do not provide satisfactory solutions.

(4) Assessment of vulnerability to a threat and terrorist incident response measures shall examine the assessed unit's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices including weapons of mass destruction (WMD). The assessment shall further examine the ability to provide structural or infrastructure protection against terrorist events. The ability to respond to a terrorist event with emphasis on a mass casualty situation shall also be examined.

(5) Assessment of terrorist use of WMD shall include the vulnerability of installations, facilities, personnel and family members to include the use of chemical, biological, nuclear or radiological agents.

(6) The assessment shall examine written plans and programs in the areas of counterintelligence, law enforcement liaison, intelligence support, security and post-incident response, especially a mass casualty event to include a disease outbreak caused by terrorist use of biological weapons.

(7) Assessments shall focus on the most likely terrorist threats. At a minimum, units shall use the minimum threats identified in the Threat Matrix, appendix (A) of this enclosure, and be assessed on their ability to implement AT/FP measures under increasing force protection conditions (FPCONs) in response to an increase in the terrorist threat level or a terrorist threat warning.

(8) The assessment shall examine the availability of resources to support the plans as written and the frequency and extent to which plans have been exercised.

(9) The assessment shall examine the degree to which plans complement and support the ability to identify changes in terrorist threat, react to changes, and provide an appropriate response to a terrorist event.

(10) The assessment shall examine the level and adequacy of host nation, local community, interservice, and tenant support to enhance force protection measures or respond to a terrorist incident.

(11) The assessment shall determine the integration and feasibility of plans with the host nation, local community and interservice and tenant organizations to provide security, law enforcement, fire, medical and emergency response capability in reaction to a terrorist event with emphasis on mass casualty situations.

(12) The assessment shall determine the adequacy of resources available to execute agreements and the extent and frequency to which plans are exercised.

(13) The assessment shall determine the status of formal and informal agreements with supporting organizations via memorandum of agreement/ memorandum of understanding, technical agreements, interservice support agreements, host-tenant support agreements, or other models.

(14) Site-specific circumstances may require additional functional areas to be examined. Thus, the assessor will task organize the team to address these additional requirements.

b. Team composition and level of expertise must support the assessment of functional areas described above. Team members shall have expertise in the following areas: physical security; civil, electrical or structural engineering; special operations; operational readiness; law enforcement; medical operations; infrastructure; intelligence/counterintelligence; and consequence management. Commanders may tailor team composition and scope of the assessment but must meet the intent of providing a comprehensive assessment.

(1) The preferred method of conducting vulnerability assessments is with a task-organized, experience-based and functionally oriented team drawn from installation/unit sources, joint, combined, or coalition sources if applicable. All team members must be functionally oriented and have experience in the assessment area to be considered for team membership.

(2) Assessment teams may be augmented by personnel with expertise in the areas of: linguistics; chemical, biological, radiological weapons effects; AT/FP technology; explosive ordnance disposal; special warfare; communications; information assurance or operations; consequence management; and other specialties as determined by the assessor.

(3) The expertise needed to perform a successful assessment will normally be located within the Marine Corps, but may be made available from other services, U.S. Government agencies HN sources, or the local community. Units should request this support through the chain-of-command. Commands

should develop and make available sufficient resources to make the skill sets required to adequately perform an assessment available.

4. Pre-Deployment AT/FP Vulnerability Assessment. Pre-deployment AT/FP vulnerability assessments shall be conducted for all units prior to deployment. These assessments should form the basis for unit AT/FP plans as well as appropriate force protection measures to reduce risk and vulnerability. Assessment of unit vulnerabilities shall be subject to continual evaluation once deployed.

a. DOD requires component commanders to provide deploying units with on-board and/or advance-site assessments prior to and during visits to areas of significant or high threat levels or where a geographically specific terrorism warning report is in effect. This includes routes that may be used by transiting forces. This requirement may be waived by the geographic Combatant Commander for deployments and/or visits to controlled locations such as existing military installations or ships afloat. Deploying units must coordinate with the appropriate Marine forces antiterrorism officer (ATO) to ensure proper planning is accomplished. Oftentimes the Marine forces ATO will have capabilities and resources that can be made available to deploying forces.

b. Deploying commanders shall utilize AT/FP measures to reduce risk and vulnerability before, during, and after deployment. If warranted, commanders faced with emergent AT/FP requirements prior to movement of forces should submit Combatting Terrorism Readiness Initiatives Fund requests in accordance with CJCS Instruction 5261.01A (NOTAL) of 1 Jul 01 to produce necessary materials or equipment for required protective measures. Assessments and implementation of standards should occur in a timely manner and should be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating area of responsibility (AOR)-specific training and in obtaining necessary physical security materials and equipment. Coordination with the applicable Marine forces ATO is required.

c. Commanders should research and identify AT/FP equipment or technology requirements through the chain of command. The use of commercial-off-the-shelf or Government-off-the-shelf products should be stressed to meet near-term requirements.

5. MSHARPP Vulnerability Assessment Methodology. MSHARPP is an acronym that stands for Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity. The MSHARPP methodology may be a useful tool in identifying lucrative targets for terrorists. Installations and units can use MSHARPP to identify and prioritize force protection concerns. Consideration is given to the local threat, likely means of attack available to the enemy, and variables affecting the disposition (e.g., “attractiveness” to enemy, potential psychological effect on community, etc.) of potential targets. After a list of potential targets is developed, MSHARPP selection factors are used to assist in further refining the assessment by associating a weapon/tactic to a potential target to determine the efficiency, effectiveness and plausibility of the method of attack and to identify vulnerabilities related to the target. After the MSHARPP values for each target or component are assigned, the sum of the values indicate the highest

value target (for a particular mode of attack) within the limits of the enemy's known capabilities.

a. Mission

(1) Mission focuses mainly on the threat to the situations, activities, capabilities, and resources on an installation that are vulnerable to a terrorist attack. The mission components consist of the equipment, information, facilities, and/or operations or activities that are necessary to accomplish the installation's mission. When assessing points in this area, determine whether or not an attack on mission components will cause degradation by assessing the component's:

(a) Importance. The value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

(b) Effect. The ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

(c) Recoverability. The time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

(2) Assess points to the target equipment, information, facilities, and/or operations or activities (scale of 1-5; 5 being worst) in this area based upon the degree of mission degradation if attacked by a terrorist.

(3) Mission Criteria Scale

(a) Installation cannot continue to carry out its mission until the attacked asset is restored.

(b) Ability to carry out a primary mission of the installation would be significantly impaired if this asset were successfully attacked.

(c) Half of the mission capability remains if the asset were successfully attacked.

(d) The installation could continue to carry out its mission if this asset were attacked, albeit with some degradation in effectiveness.

(e) Destroying or disrupting this asset would have no effect on the ability of the installation to accomplish its mission.

b. Symbolism

(1) Consider whether the target represents, or is perceived by the enemy to represent, a symbol of a targeted group (e.g., symbolic of U.S. military, Christianity, Government, authority, etc.). Assess points in this area based upon the symbolic value of the target to the enemy.

(2) Symbolism Criteria Scale

(a) High profile, direct symbol of target group or ideology, asset is perceived to be vital to the mission of the installation.

(b) Low profile, direct symbol of target group or ideology.

(c) Low profile and/or obscure symbol of target group or ideology.

c. History

(1) Do terrorist groups have a history of attacking this type of target? While you must consider terrorist trends worldwide, focus on local targeting history and capabilities.

(2) History Criteria Scale

(a) Strong history of attacking this type of target.

(b) History of attacking this type of target, but none in the immediate past.

(c) Little to no history of attacking this type of target.

d. Accessibility

(1) A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The enemy must not only be able to reach the target but must also remain there for an extended period. The four basic stages to consider, when assessing accessibility are:

(a) Infiltration from the staging base to the target area.

(b) Movement from the point of entry to the target or objective.

(c) Movement to the target's critical element.

(d) Exfiltration.

(2) Accessibility Criteria Scale

(a) Easily accessible or standoff weapons can be employed.

(b) Inside Perimeter fence, climbing or lowering required.

(c) Not accessible or inaccessible without extreme difficulty.

e. Recognizability

(1) A target's recognizability is the degree to which it can be recognized by an operational element and/or intelligence collection and reconnaissance asset under varying conditions. Weather has an obvious and significant impact on visibility for both friendly and enemy forces. Rain, snow, and ground fog may obscure observation. Road segments with sparse

vegetation and adjacent high ground provides excellent conditions for good observation. Distance, light, and season must be considered.

(2) Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the enemy.

(3) Recognizability Criteria Scale

(a) Target is clearly recognizable under all conditions and from a distance; requires little or no training for recognition.

(b) Target is easily recognizable at small-arms range and requires a small amount of training for recognition.

(c) Target is difficult to recognize at night or in bad weather, or might be confused with other targets; requires training for recognition.

(d) Target cannot be recognized under any conditions—except by experts.

f. Population

(1) Population addresses two factors, quantity of personnel and their demography.

(2) Demography asks the question "who are the targets?" Depending on the ideology of the terrorist group(s), being a member of a particular demographic group can make someone (or some group) a more likely target. Therefore, when assessing points in this area, determine whether or not the group(s) have a history of or are predicted to target:

(a) Military personnel.

(b) Family members (U.S. citizens in general).

(c) Civilian employees of the U.S. Government (include local nationals)

(d) Senior officers or other high-risk personnel.

(e) Members of an ethnicity (racial, religious, or regionally defined).

(3) Quantity addresses the number of people that would become victims if a particular target were attacked. Going on the assumption the intent of the attack is to kill or injure personnel, it follows that the more densely populated an area/facility is, the more lucrative a target it makes (all other things being equal).

(4) Population Criteria Scale

(a) Densely populated; prone to frequent crowds, facility routinely contains substantial numbers of personnel known to be targeted by

the enemy and/or the population is comprised of personnel deemed vital to the accomplishment of the installation's mission.

(b) Relatively large numbers of people, but not in close proximity (i.e., spread out and hard to reach in a single attack), contains known target group, but rarely in large concentrations, population has no special segment necessary for mission accomplishment.

(c) Sparsely populated; prone to having small groups or individuals, little target value based on demographics of occupants.

g. Proximity

(1) Is the potential target located near other personnel, facilities, or resources that, because of their intrinsic value or "protected" status and a fear of collateral damage, afford it some form of protection (e.g., near national monuments, protected/religious symbols, etc., which the enemy holds in high regard)?

NOTE: It is important to consider whether the target is in close proximity to other likely targets. Just as the risk of unwanted collateral damage may decrease the chances of attack; a "target-rich" environment may increase the chances of attack.

(2) Proximity Criteria Scale

(a) Target is isolated; no chance of unwanted collateral damage to protected symbols or personnel.

(b) Target is in close enough proximity to place protected personnel, facilities, etc., at risk of injury or damage, but not destruction.

(c) Target is in close proximity; serious injury/ damage or death/total destruction of protected personnel/facilities likely.

h. Table 2-1 of this enclosure is an example of an MSHARPP worksheet. Values from 1 to 5 are assigned to each factor based on the associated data for each target. Five represents the highest vulnerability or likelihood of attack and 1 the lowest. Accordingly, the higher the total score, the more vulnerable the target. Because this analysis is highly subjective, some analysts prefer simple "stoplight" charts with red, yellow and green markers representing descending degrees of vulnerability. The MSHARPP analysis must consider both the present force protection posture and enhanced postures proposed for escalating FPCONs.

TARGET	M	S	H	A	R	P	P	TOTAL	WEAPON
HQ BLDG	5	4	5	1	3	4	1	23	4,000 Truck IED
Barracks B	2	4	5	4	4	[illegible]	[illegible]	25	220 lb Car IED
Comm Center	5	4	2	3	[illegible]	[illegible]	1	23	4,000 Truck IED
SF Ops Center	3	[illegible]	[illegible]	[illegible]	[illegible]	4	2	22	7.62 (Sniper)
Fuel Storage	4	[illegible]	[illegible]	[illegible]	5	1	3	22	50 lb Satchel Charge
Hanger A	5	[illegible]	3	2	5	5	4	29	Mortar
Wpns Storage	5	5	1	1	5	3	1	21	RPG
Elec Transformer	5	2	3	5	5	0	4	24	Grenade

Specific target vulnerabilities must be combined with exploitable perimeter control vulnerabilities. If access routes are well protected and not deemed exploitable an otherwise vulnerable target becomes a less attractive.

Table 2-1.--Example of an MSHARPP Worksheet.

FOR OFFICIAL USE ONLY

THREAT CAPABILITIES						
Tactic	**Severity Level**	**Weapon**	**Delivery Method**	**Inside Perimeter**	**Outside Perimeter**	**Comments**
Vehicle Bomb		**50 lb**	**Car**			**Construction Design, Protected Perimeter**
		100 lb	**Car**			**Construction Design, Unprotected Perimeter**
		220 lb	**Car**			**AT Planning, FPCONs**
		220 lb	**Car**			**With contaminant (CBRN)***
Placed Bomb		**50 lb**				
		50 lb				**With contaminant (CBRN)***
Mail Bomb		**2 lb**				
Ballistics		**7.62 mm**				
		.44 Mag				
		9 mm				
Standoff Weapons		**Mortar**				
		RPG				
Executive/ Personnel Protection		**Assassination**				
		Kidnapping				
		Barricade/ Hostage				
		Civil Disturbance				
		Bomb Threat				
Airfield		**MANPAD**				
		Hijacking				
Seaport		**220 lb**	**Boat**			
		220 lb	**Boat**			**With contaminant (CBRN)***
		Surface Threat				**May include swimmer, floating explosive objects**
		Sub-surface Threat				**May include swimmer, submersibles, mines**
WMD		**Chem/Bio Letter**				
		Placed Contaminant	**Open container/ Deliberate spill**			**< 5 Gal (40 lbs) of contaminant (CBRN)***
		Sprayed Contaminant	**Backpack/ Vehicle**			**< 5 Gal (40 lbs) of contaminant (CBRN)***
		Bio Attack	**Food/ Water/ etc**			**Surreptitious Attack**

TERRORIST THREAT ASSESSMENT

1. General

a. The terrorist threat assessment is the second step in an analytical risk management process. The terrorist threat assessment is a process that is used to conduct a threat analysis and develop an evaluation of the potential terrorist threat.

b. Commanders will prepare a terrorist threat assessment at least annually and for every overseas exercise/deployment that will identify the full spectrum of known or estimated terrorist capabilities including weapons and tactics. The threat assessment will integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources. This information shall be incorporated into the unit's antiterrorism/force protection awareness program.

2. Threat Assessment. The goal of this step is to develop an understanding of the terrorist threat to the assets identified in the criticality assessment. This information will be used to estimate the susceptibility of those assets to an attack during the vulnerability assessment. Understanding threats requires an understanding of the terrorist's intentions and motives, as well as their capability to attack critical assets. Therefore the assessment should clearly distinguish between threat assessment (capability estimate that supports antiterrorism (AT) planning) and threat warning (indications and warnings). Because access to this type of information is often limited, this is generally the weakest link in the overall risk assessment process. The process outlined below provides a useful framework for data collection and analysis.

3. Threats. Threats can be defined as an indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets. Threat must be defined in terms that are meaningful to the planner; i.e., the plausible weapons and associated tactics that are used by the terrorist organization, and weapons and tactics that are within the terrorist organizations capability, even if those weapons and tactics are not currently being used. From this information the threat working group can determine the tactics the aggressors will likely employ and the threat severity levels associated with those tactics. The threat severity levels describe the specific tools, weapons, and explosives associated with each tactic. This information will be used to determine the vulnerability of an asset to a particular weapon or tactic and allow planners to produce effective countermeasures, response plans, and consequence management measures.

4. Threat-Based Assessment. Department of Defense (DOD) Instruction 2000.16 (NOTAL) of 14 Jun, 2001, DOD Antiterrorism Standards, requires that AT programs be threat-based; that threat assessments of feasible terrorist capabilities be the basis for assessing vulnerabilities, planning AT physical security measures, and justifying AT enhancements and budget proposals.

a. Installations and expeditionary sites must develop a threat assessment that identifies a range of feasible terrorist capabilities that AT program managers can use as a planning tool. This will allow vulnerabilities to be assessed in the context of specific threats; routine physical security and antiterrorism/force protection measures can be tailored to counter specific threats or mitigate specific vulnerabilities, and will allow audit trails for acquisitions.

b. A baseline threat, used for assessing vulnerabilities and planning countermeasures, facilitates the allocation of resources especially when the need to plan for multiple installations arises. It also supports decision-making when specific warning reports are received. If warning is provided regarding a specific threat, the commander immediately knows whether the planned countermeasures adequately defend the installation against that threat or if it will be necessary to regroup and plan additional measures because the imminent threat is outside the range of baseline threat used in the planning process.

c. The Threat Matrix, located at appendix (A) to enclosure (2), identifies a range of minimum terrorist threat capabilities and will be used as the baseline for planning purposes. Should the installation's threat analysis identify additional or greater threats, they will be added to the matrix.

5. Frequency of Threat-Related Incidents. A high frequency of threat-related incidents can indicate an increased likelihood that a similar incident may take place in the future, especially if capability and intent are high. The absence of previous incidents has little significance in predicting future incidents and should have no bearing on the development of a threat assessment that identifies a range of feasible terrorist capabilities.

6. Threat Data. The collection and analysis of threat information is critical to the risk assessment process. In order to make valid assessment of threats it is essential to understand as much as possible about each specific adversary. Information resources can be divided into two types: those that provide unclassified or "open-source" information, and those that provide classified information. Generally, both are used in the development of threat data.

a. The Naval Criminal Investigative Service (NCIS) is the Department of the Navy (DON) component with primary responsibility for law enforcement, counterintelligence (counter intelligence operations, and security policy matters). NCIS maintains a worldwide structure to ensure operational readiness of Marine Corps commands by preventing terrorist attacks against DON forces, protecting against compromise of DON sensitive info/systems, and reducing crime against the DON. To fulfill this responsibility, NCIS has established the Multiple Threat Alert Center (MTAC), which serves as the fusion point and production center within the DON for all terrorist, criminal, cyber, and counterintelligence information indicative of a threat to DON assets throughout the world. The MTAC processes real time information and operates on a 24-hour basis to provide commanders with a timely and

common operational picture of security threats and vulnerabilities to reduce risks to Marine Corps forces and assets. The MTAC provides the following support to Marine Corps commands:

(1) MTAC Special Analysis Reports (SARs). SARs are daily reports that cover topics such as threat advisories, threat supplements (counterterrorism, counterintelligence, criminal, and cyber) that are aimed at specific geographical areas and are published as soon as information is received. They provide current operational intelligence on terrorist and related unconventional warfare threats to DON personnel and assets.

(2) MTAC Summary Report. The MTAC Summary Report is a daily summary of all the SARs that have been produced.

(3) MTAC Force Protection Summary. The Force Protection Summary is published weekly on Sunday and lists countries designated by DOD as moderate to high terrorist threat levels. Additionally, when changes to country threat levels occur they are published in the summary.

(4) MTAC Spot Report

(a) This report is sent to affected commands.

(b) It provides threat specific information on impending or likely terrorist activity.

(5) MTAC BLUE DART Report

(a) This report is sent to affected commands.

(b) 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 personnel or assets.

b. There are many sources of unclassified information such as mass media, U.S. Government publications and internet websites. Websites of interest include: Computer Emergency Response Team (CERT), National Security Institute (NSI), Center for Security Policy, Extranet for Security Professionals (ESP), and the OPSEC Professionals Society. Additional security websites and helplines are located in enclosure (12).

c. Geographic Combatant Commander will be able to provide information relative to the threat in their specific area of responsibility.

7. Threat Assessment. The goal of this step in the risk management process is to make a factually based estimate combining information from classified and unclassified intelligence sources with locally developed information on the existing threat.

CRITICALITY ASSESSMENT

1. General. A criticality assessment is the third step in the risk management process. Not all assets and activities warrant the same level of protection; therefore, it is necessary to identify the assets that need to be safeguarded and assess their relative value. Generally, assets are valued relative to the impact of their potential loss. If an adversary places a high value on an asset, the likelihood of that asset becoming a target increases.

2. Criticality Assessment. During this step, a survey of assets and determination of the value of the assets is completed. The criticality assessment should identify the installation or deployed unit's key assets including personnel, information, equipment/materials, facilities, activities/operations and critical infrastructures. It should be emphasized that high population locations are lucrative terrorist targets, regardless of their importance to mission accomplishment. High population areas consist of places where people eat, sleep, gather, and places where command functions occur.

a. The criticality assessment begins with a survey to compile information about valued assets. This information is available from a variety of sources including site personnel (host-nation, Combatant Commanders, representatives, Officers-in-Charge, managers, operations personnel, security personnel, logistics personnel, other facility staff, construction personnel, contractors, and maintenance staff); a review of existing security plans, and security survey/audits; rosters of classified documents, and personnel located at a particular site; and, open source information. Because of joint usage the criticality assessment should be coordinated with adjacent units/services/communities.

b. The data collected in the survey is analyzed to determine the most valued assets and to determine the relative degree of impact if an asset were to be compromised in some way. It is important to recognize that the value of people, information, and activities is difficult to quantify in terms of dollars therefore, a criticality assessment determines whether or not an attack on a component will cause degradation in mission capability by assessing the asset's:

(1) Importance. The value of the area or assets located in the area, considering their function, inherent nature, and monetary value.

(2) Effect. The ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts.

(3) Recoverability. The time required for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies.

3. Mission Essential Vulnerable Areas (MEVAs). The product of this phase of the Risk Management process will be the identification of assets that could be expected to become potential terrorist targets; the impact of a terrorist attack on those assets; and, the consequences of the loss or partial loss of those assets. This information is then used to develop a prioritized list of MEVAs and other lucrative terrorist targets. MEVAs are defined in enclosure

(1) as being areas designated by the commander as containing assets essential to the accomplishment of the installation/unit mission. In addition to MEVAs, other assets that should be considered potential targets because of their value to the commander in terms of potential loss of life, psychological, economic, or sociological impacts will be identified.

RISK ASSESSMENT

1. General

a. The risk assessment is the final step in the risk management process. The risk assessment provides antiterrorism (AT) planners with the ability to improve the installation's baseline security posture and efficiently and effectively deploy resources during higher force protection conditions (FPCONs). It also provides information that is useful to the commander in making resource allocation decisions designed to protect personnel and assets from possible terrorist threats in a resource-constrained environment. The risk assessment is developed on the foundation of the threat assessment, criticality assessment, and vulnerability assessment described in enclosures (2), (3), and (4) respectively. The result will identify an AT strategy that will encompass physical security, FPCONs, terrorist incident response measures, consequence management measures, personal security, operational security (OPSEC), and AT awareness, which will produce a comprehensive AT program. Additionally, the risk assessment will help the AT officer (ATO) identify countermeasures necessary to mitigate vulnerabilities, their costs and tradeoffs and will become the basis by which protective measures are planned and their implementation prioritized.

b. The process described above is an iterative versus sequential process. That is, each step may yield new information that affects the information developed earlier. Data gathered during each step of this process shall be documented and maintained for further analysis and use as backup data for proposed recommendations and alternatives.

c. The risk assessment will become the basis and justification for recommendations by the commander on antiterrorism/force protection (AT/FP) enhancements, program/budget requests, application of random antiterrorism measures (RAM) and the establishment of FPCONs. Information developed from the risk assessment includes: what assets are vulnerable, what are the actual or estimated threats, how important the assets are, and what are the estimated costs of eliminating or mitigating the threats.

2. Risk Assessment Methodology. Risk assessments shall consider the factors of threat, asset criticality and vulnerability of facilities, programs and systems, as well as deterrence/response capabilities. Risk assessments shall analyze the following four elements:

a. The terrorist threat;

b. the criticality of the assets;

c. the vulnerability of facilities, programs and systems to terrorist threats; and

d. the ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

The risk assessment allows the commander to obtain a clear picture of the current AT/FP posture and identify those areas that need improvement. During the risk assessment, important information is also collected that can be used

when writing the AT/FP plan.

3. Assessing Risk and Determining Priorities for Asset Protection

a. The elements of the criticality assessment, threat assessment, vulnerability assessment should be reviewed, additional information obtained and revisions made to the assessments as necessary.

b. The elements of threat and vulnerability should be considered together and an estimate of the probability or likelihood of an occurrence estimated. Then, the probability of occurrence and the impact (derived from the criticality assessment) are considered together and a judgment of the level of risk is made. In this manner, both the likelihood and magnitude of the event are considered.

c. Where the vulnerabilities are great and the threat is evident, the risk of exploitation is greater. Therefore, a higher priority for protection must be considered. Where the vulnerability is slight and/or the adversary has little capability to exploit vulnerabilities, the risk is lower and the priority for new countermeasures is lower.

d. The areas of greatest risk that are identified by the risk assessment will serve as the basis for deciding where to focus countermeasures and what countermeasures to apply.

e. Once the likelihood and magnitude of an event is estimated, a judgment must be made as to the acceptable level of risk for a particular asset. The acceptable level of risk may vary with the factors of time, circumstances, and the commander’s attitude toward risk.

4. Identification of Countermeasures, Costs, and Options

a. Based on the information obtained and analyzed in the risk assessment, potential countermeasures to reduce vulnerabilities can be identified and considered. Countermeasures generally fit into one of the following five categories: intelligence, procedures, equipment, physical and manpower.

(1) Procedures. OPSEC, training, awareness programs, legal prosecution, polygraph, security investigations, disclosure statements, personnel transfer, contingency planning, two person rules, passwords, and periodic searches.

(2) Equipment. Locks, window bars, doors, fences, alarms, Hardware/software, badges, lighting, paper shredder, weapons, CCTV, safe haven, vaults.

(3) Physical. New construction, barriers, retrofitting, purchase of additional land, earthwork.

(4) Manpower. Contractor guards, local police, additional military security forces.

(5) Intelligence. Counterintelligence, countersurveillance, host nation/local law enforcement information, criminal data.

b. Each proposed countermeasure should mitigate risk by deterring, detecting, delaying, defending, and/or defeating the threat and be evaluated in terms of the level of risk reduction obtained. In order to identify the most effective countermeasures, they must be evaluated based on the effect that each will have on the existing risk level. This will be accomplished by evaluating the impact of the countermeasure on the vulnerabilities identified in the vulnerability assessment and considering if the countermeasure will have an affect on the threat or criticality of the asset. During the analysis it may become apparent that certain countermeasures will reduce risk for several vulnerabilities thereby increasing the value of that particular countermeasure.

c. Commanders should ensure that appropriate procedures, processes, training and manpower (assets that are most readily available and normally offer the most immediate and least expensive remedy available to the commander) have been utilized to the fullest extent possible.

d. Every countermeasure has a cost associated with it that can be measured in terms of dollars, effect on mission, inconvenience, time and personnel. In order to select the most appropriate countermeasure, the cost associated with each must be determined.

(1) Dollar cost of countermeasures including purchase price and life cycle maintenance costs, including installation, preventative maintenance, repair, warranty, replacement and disposal costs should be considered. The life expectancy of the countermeasure should be considered as well as the salaries of staff and contractors to implement, maintain, monitor, and train others.

(2) Effect on mission costs includes reduced manpower available for mission requirements, increased time required for deployment, etc. While mission costs are hard to estimate, they must be considered. Poor selection of a countermeasure can have a devastating effect on mission capability.

(3) Inconvenience may result in additional costs if personnel bypass the countermeasure. Countermeasures that are least inconvenient should be employed whenever possible.

(4) In terms of time, the time required to implement, oversee, and prepare for implementation as well as time require for follow-up and evaluate should be considered.

(5) Personnel costs include the number of staff needed to use the countermeasure as well as the skills, knowledge, and abilities of the personnel involved and staff training needs.

(6) Generally, the least expensive countermeasure that will reduce risk to an acceptable level will be selected. However, in a given instance, a high-cost countermeasure may protect against more than a single vulnerability and may prove to be the least costly countermeasure to employ.

5. Cost-Benefit Analysis

a. Based on the results of the risk assessment, it must be determined

which of the countermeasures options mitigate risk to an acceptable level at a reasonable cost. Factors that influence countermeasure decisions include:

(1) Value of the Asset. What is the impact if the asset is lost or damaged?

(2) Current Exposure to Harm/Loss. How vulnerable is the asset?

(3) Availability of Protective Measures. What is the state-of-the-art and effectiveness?

(4) Availability of funds. What resources are available compared to asset value?

(5) Mandatory Security Requirements. What is mandated by regulation?

b. For a particular vulnerability, a variety of countermeasures may be available. Each of the various countermeasures will reduce risk to a varying degree and have differing associated costs. The events to be protected against, countermeasures, risk reduction and costs should be laid out in a decision matrix and recommendations made to the commander. The ultimate goal of this process is to provide the least cost/maximum benefit options to the commander.

c. Once the appropriate countermeasures have been selected and are in place, they must be tested and evaluated to ensure they are as effective as anticipated in the risk assessment. A monitoring system should be established to detect any changes in criticality of assets, threats and/or vulnerabilities that might change the risk assessment.

6. Integration of the Risk Analysis Process. The risk analysis process encompasses the vulnerability assessment, threat assessment, criticality assessment, and risk assessment. Using the information generated and analyzed during the risk analysis process the commander establishes site-specific measures to mitigate the baseline threat.

a. For example, assume the risk analysis process has identified several buildings as having vulnerabilities to the baseline threat. Following the implementation of the plan, the commander determines the local threat has increased; a new terrorist group has been identified that is believed to posses the capability to deploy a 50 lb. placed bomb. The commander selects FPCON BRAVO based on his estimate of the situation. FPCON BRAVO, measure 14, calls for the standoff of cars and objects from buildings. The site-specific measures against the baseline threat may call for parking and trash containers to be relocated. After a period of time, assume that new information becomes available that shows that this terrorist group has the capability to deploy a 220 lb. car bomb. Based on the site-specific measures designed for the baseline threat, the commander may use a Jersey barrier wall assembly to prevent vehicles from violating the 25 meter exclusionary area for parking for the known threat. Note that in the example given, the FPCON did not increase because the capability rather than the intentions of the terrorist group had changed. If intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely, then the commander may increase the FPCON to CHARLIE, and/or include additional RAM to increase his level of comfort with the threat. If the

commander chooses to go to FPCON CHARLIE, the site-specific measure for the same weapon and tactic may call for the search of all vehicles parked in the vicinity of the vulnerable buildings or an increase in standoff distance.

b. From the above discussion, it can be seen how the risk analysis process works. The vulnerability of assets is identified during the vulnerability assessment. Then, the threat assessment is conducted, and at a minimum, the baseline threat contained in the Threat Matrix is analyzed. Measures are created to enhance protection from the terrorist weapons and tactics identified in the baseline (or actual threat if higher) for each FPCON level. RAM, which may come from higher FPCONs or be developed independently, are also created. As the threat changes, the site-specific measures change. The criticality assessment helps the commander identify and prioritize mission essential vulnerable areas whose protection is critical to mission accomplishment. This could include non-military assets and critical infrastructures such as the base child development center or a water purification treatment plant if deemed critical to mission accomplishment. The risk assessment assists the commander in balancing the mitigation of the threat with the assets available. In part, it helps the commander decide what to protect, when to protect it and what level of protection to provide. Thus the information generated in the risk assessment process is used to develop site-specific measures using the baseline threat contained in the Threat Matrix. See appendix (A) to enclosure (2).

TERRORISM THREAT LEVELS

1. Terrorism Threat Levels

a. The Department of Defense (DOD) terrorism threat level classification system is a set of standardized terms used to quantify the level of estimated terrorism threat on a country-by-country basis. Per DOD Handbook 2000.12-H (NOTAL)of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, the Defense Intelligence Agency (DIA) establishes country terrorism threat levels for DOD. Geographic Combatant Commanders may also establish terrorism threat levels for specific personnel, family members, units, and installations in countries within the Combatant Commander's area of responsibility (AOR). Commanders at all levels shall use their own threat analysis as the basis for developing plans and programs to protect assets for which the have AT/FP responsibility.

b. Terrorism threat levels should not be confused with force protection conditions (FPCONs). Threat levels do not address when a terrorist attack will occur and do not specify a FPCON status.

c. The issuance of a terrorism threat level is not a warning notice (notice of the possibility of imminent attack). The Navy Criminal Investigative Service (NCIS) Multiple Threat Alert Center (MTAC), DIA, and/or Combatant Commanders may issue separate warning notices regarding imminent terrorist attack.

d. Terrorism threat levels are the intelligence community's system for articulating and categorizing the terrorist threat worldwide. They represent a DOD-developed methodology for assessing the terrorist threat to personnel, material and interests based on a combination of the threat analysis factors. The terrorism threat level is determined for a particular area based on the presence or absence of these threat assessment factors:

(1) Operational Capability. The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.

(2) Intentions. Actions indicative of preparations for specific terrorist operations.

(3) Activity. Recently demonstrated anti-U.S. activity, or stated or assessed intent to conduct such activity.

(4) Operating Environment. The circumstances of the country under consideration (host nation security, legal system, terrain features, etc.).

2. Terrorism threat levels are determined from a combination of the above threat assessment factors. On 1 October 2000 the DIA changed the previous five-level system into one that has four levels:

a. High. An anti-U.S. terrorist group is operationally active and uses large casualty producing attacks as their preferred method of

operation. There is a substantial DOD presence and the operating environment favors the terrorist.

b. Significant. An anti-U.S. terrorist group is operationally active and attacks personnel as their preferred method of operation, or a group uses large casualty producing attacks as their preferred method and has limited operational activity. The operating environment is neutral.

c. Moderate. Terrorist groups are present but there is no indication of anti-U.S. activity. The operating environment favors the host-nation or U.S.

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

3. To fulfill all pre-travel briefing requirements when traveling overseas, personnel must be briefed in accordance with the highest terrorism threat level established by DOD or the AOR Combatant Commander for each individual country. Failure to understand and comply with briefing requirement in advance of travel requests may result in rejection of area/country clearance requests. Current terrorism threat level information for AOR Combatant Commanders can be obtained at the following numbers: JFCOM (800) 542-08646; CENTCOM (813) 828-6289/90/91; EUCOM 011-441-480-84-1414; PACOM (808) 477-7309; SOUTHCOM (888) 547-4025 EXT 3720.

4. State Department travel advisories that reflect a security concern (terrorist, insurgency/political instability, or criminal threat) can be obtained from the nearest State Department office, embassy and/or consulate, via the internet (http://www.state.gov), or by calling (202) 647-5225.

5. The NCIS MTAC 24-hour watch center point of contact: (STU-III capable) is DSN: 288-9490/18, COMM (202) 433-9490/18. MTAC watch can also be reached via:

a. SIPRNET homepage. www.ncis.navy.smil.mil

b. SIPRNET email. atac@ncismail.ncis.navy.smil.mil

c. SCI homepage. www.ncis.nmic.ic.gov

d. DODIIS email. atac@ncis.nmic.ic.gov

MTAC summaries, supplements, warning reports, and NCIS threat assessments are available on interlink via the NCIS homepage.

FORCE PROTECTION CONDITIONS (FPCONs)

1. Adjustment of FPCONs

a. Geographic Combatant Commanders have antiterrorism/force protection (AT/FP) responsibility within their area of responsibility. Service Chiefs have responsibility for AT/FP of their respective service installations and associated personnel/resources within the domestic U.S.

b. Commanders at all levels will develop a process to raise or lower FPCONs. FPCON transition procedures and measures will be disseminated and implemented by subordinate commanders. Local commanders will develop measures to support transition between FPCONs.

c. Commanders at all levels shall set a local FPCON. AT/FP plans shall include a process, based on terrorism threat information and/or guidance from higher headquarters, to raise or lower FPCON levels. Subordinate commanders may raise a higher-level commander's FPCON for those personnel and assets for which they have AT/FP responsibilities. Subordinate commanders shall not lower a higher-level commander's FPCON without concurrence.

d. Although terrorist threat assessments performed by the intelligence community will normally provide the commander with sufficient information to make prudent security determinations, such assessments must not be considered "stand alone" documents. The terrorism threat level is the intelligence community's assessment of the likelihood of a terrorist attack. FPCONs are the means the commander uses to apply operational decisions on how to guard against the threat. The commander must ensure terrorist threat assessments are kept up-to-date. The local Naval Criminal Investigative Service Resident Agent can provide current AT/FP information necessary to continually assess the terrorist threat. The commander must select an appropriate FPCON level by weighing current intelligence data and estimated terrorist threat against the loss of mission effectiveness that may occur if a higher FPCON is selected.

e. Subordinate commanders can establish higher FPCONs as the local situation warrants. FPCON measures are mandatory when declared, are implemented immediately and can be supplemented by additional measures and random antiterrorism measures (RAM). The declaration, reduction, and cancellation of FPCONs remain the responsibility of the commander issuing the order.

f. The decision to arrive at a particular FPCON and associated security measures should be based on multiple factors that may include, but are not limited to:

(1) The assessed 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.

FPCON measures should be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise.

g. Units and organizations located in civilian communities (recruiting stations, Marine Corps Reserve units, etc.) should modify FPCON measures at each level to meet their own unique requirements.

2. Development of Site-Specific Measures. Commanders at all levels shall develop site-specific measures that supplement those measures/actions contained in the FPCONs listed in this enclosure and DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93.

a. The FPCON measures identified in this enclosure are the minimum measures that will be implemented by an installation when an FPCON is prescribed. Therefore, the installation AT/FP plan must describe the specific action that will be taken to implement each required measure. An effective means to perform this function is the development of synchronization matrices for each measure for FPCON NORMAL through DELTA; additional measures addressing weapons of mass destruction (WMD) may also be included. To make the matrix efficient, each measure must answer the questions of who, what, where, when, and how each measure is going to be implemented. In addition to the general increased protection afforded by implementing these measures, measures should be developed to, at a minimum, allow an installation to specifically detect, deter, defend, and defeat those weapons and tactics identified in the threat matrix. The implementation guidance provided by these measures will also serve as the basis for determining required resources to implement the plan and the cornerstone of the table topping and exercise programs. Two examples of FPCON synchronization matrices are shown in tables 7-1 and 7-2 of this enclosure.

b. An AT/FP plan with a complete listing of site-specific antiterrorism (AT) measures, linked to a FPCON, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP plan, specific AT measures and FPCONs remain unclassified but shall be handled as FOR OFFICIAL USE ONLY (FOUO) documents. Site-specific AT measures should be:

c. Tailored to meet unique installation and unit AT/FP requirements.

d. Consider actions that will increase time and space in which to determine hostile intent.

3. RAM. The purpose of RAMs is to identify a set of protective measures in addition to those in effect in the current FPCON and implement those measure(s) for a period of time. The measures can be obtained from higher FPCONs or developed specifically for the RAM program. RAM programs change the security atmosphere surrounding a facility. Such programs, when implemented in a truly random fashion, alter the external appearance or security “signature” of an installation. Several purposes are served by adopting a set of RAM. Among these are:

a. Provide additional training and increase alertness of assigned security personnel through mental stimulation by changing the routine.

b. Increases awareness for DOD personnel, their dependents, visitors and neighbors.

c. RAM may be used as a tool for commanders to test which measures have higher productivity costs than others.

d. They deter attack by altering the observable security signature of a facility.

e. Provide some of the increased security of a higher FPCON without the costs of full implementation. Generally, more sustainable than the higher FPCON would be.

f. Reduce adverse operational impacts and economic costs compared to higher FPCON levels.

4. FPCON Waivers. If it is determined that certain FPCON measures are inappropriate for current operations, or for proper threat mitigation, a waiver may be requested. Overseas, the wavier procedure directed by the geographic Combatant Commander applies. In the domestic U.S., the first general officer exercising operational control in the chain-of-command has the authority to waive FPCON measures. Nothing in this waiver process is intended to diminish the authority or responsibility of commanders to exercise oversight of FPCON and RAM program execution.

a. To ensure a consistent force protection posture is maintained, tenants on installations and facilities shall coordinate waiver actions with the host installation before submitting them to the chain-of-command.

b. All waiver requests will be directed to the waiver authority. Information copies will be sent to the unified command's joint operations center, major/fleet command's operations center, or service operations center as applicable.

c. Approved waivers, to include mitigation measures or actions, must be forwarded to service, unified, major, or fleet command level recipients within 24 hours.

5. FPCONs

a. FPCON NORMAL. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

b. FPCON ALPHA. FPCON ALPHA applies when there is an increased general threat of possible activity against personnel or facilities, the nature and terrorist extent of which are unpredictable. *ALPHA measures must be capable of being maintained indefinitely*.

(1) Measure 1. Remind all personnel, including family members, at regular intervals to:

(a) Be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers.

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

(c) Be alert for abandoned parcels, suitcases or any unusual activity.

USMC recommended, Measure 1-1: Troop information program: brief all personnel on the current threat condition, and those measures enacted to increase security. Remind all duty personnel to be especially alert for suspicious or unusual activity, strangers, or unidentified vehicles.

USMC recommended, Measure 1-2: Conduct unit level terrorism awareness training.

(2) Measure 2. Keep the Duty Officer or other appointed personnel having access to plans for evaluating or sealing off buildings and/or areas in use, or where an explosion or attack has occurred, available at all times. Keep key personnel who may be needed to implement security plans on call.

USMC recommended, Measure 2-1: Ensure duty personnel have knowledge of, and access to, emergency plans. (Give special attention to the evaluation of buildings and grounds in use, as well as the plans for condoning off areas.)

USMC recommended, Measure 2-2: 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 (or the duty officer/NCO for units without a provost marshal) prior to leaving their listed recall address.

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

(4) Measure 4. Increase security spot checks of vehicles and persons entering installations and non-classified areas under the jurisdiction of the U.S. command or agency.

USMC recommended, Measure 4-1: Installation military police (MP) institute random identification spot checks of passenger and commercial vehicle occupants entering the base or station, using predetermined criteria for vehicle selection. If possible, delays in traffic beyond 8 to 10 minutes should be avoided.

USMC recommended, Measure 4-2: Installation MP, with or without the assistance of military working dog (MWD) teams, conduct daily Commanding Officer's administrative vehicle inspections at random times and locations, using predetermined criteria for vehicle selection.

USMC recommended, Measure 4-3: Installation MP physically inspect and verify license plates affixed to vehicles entering the base or station.

USMC recommended, Measure 4-4: Installation MP check the identification card, drivers license and/or vehicle registration card of all passenger vehicle and commercial truck drivers, and the identification card of vehicle occupants and pedestrians (to include joggers and bicyclists).

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

(6) Measure 6. As a deterrent, apply one of the following measures from FPCON BRAVO individually and randomly:

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

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

(c) Check all deliveries to messes, clubs, etc. (advise family members to check all home deliveries.)

(d) As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other "soft targets" to improve deterrence and defense, and to build confidence among staff and family members.

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

USMC recommended, Measure 7-1: Convene the installation security council to review incident response plans.

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

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

USMC recommended, Measure 9-1: The installation Provost Marshall will notify adjacent police jurisdictions of threat conditions in effect at the base or station, and continue to exchange intelligence.

USMC recommended, Measure 9-2: The commander and key staff review installation contingency plans.

USMC recommended, Measure 9-3: Jurisdiction and command and control issues are agreed upon and exercised between the Federal Bureau of Investigation (FBI) and local or host-nation agencies.

(10) Measure 10. Spare.

USMC recommended, Measure 10-1: Place barriers in "ready" position near gates and/or sensitive buildings, where they may be required to provide blocking, delaying or canalizing actions.

USMC recommended, Measure 10-2: Establish countersurveillance in areas likely to be targeted by hostile elements.

c. FPCON BRAVO. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. *Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.*

(1) Measure 11. Repeat measure 1 in paragraph 4b above, and warn personnel of any other terrorist form of attack.

USMC recommended, Measure 11-1: 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. Keep all personnel involved in implementing antiterrorist contingency plans on call.

USMC recommended, Measure 12-1: Key staff members continue preparation for implementing AT contingency plans.

USMC recommended, Measure 12-2: All members of the crisis management team (CMT), off-duty military police, primary reaction platoon personnel, and other members of the crisis management force (CMF) report their destination and expected time of return to the MP desk sergeant or other designated official prior to leaving their listed recall address.

USMC recommended, Measure 12-3: As far as resources allow, assign a driver and/or MP trained in protective service operations to the base commander, general officers, or other designated personnel with significant terrorist target value.

USMC recommended, Measure 12-4: The provost marshal directs a periodic recall of the special reaction team (SRT), if one is established.

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

(4) Measure 14. Where possible, move cars and objects such as crates, trash containers, etc., at least 25 meters from buildings, particularly those buildings of a sensitive or prestigious nature. Consider the application of centralized parking.

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

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

USMC recommended, Measure 16-1: Security and law enforcement personnel increase physical security checks of facilities after normal working hours.

USMC recommended, Measure 16-2: Explosive detector MWD teams check the exterior of vehicles in the parking lots immediately adjacent to headquarters and other sensitive buildings.

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

(8) Measure 18. Check all deliveries to messes, clubs, etc.

USMC recommended, Measure 18-1: Designated personnel and employees randomly check package deliveries brought into service areas.

USMC recommended, Measure 18-2: Military dependents are advised to check all home deliveries, and to report all suspicious letters and packages.

USMC recommended, Measure 18-3: Military police search all commercial vehicles entering the installation, and compare vehicle contents with bills of lading or other manifest documents.

(9) Measure 19. As far as resources allow, increase surveillance of domestic accommodations, schools, messes, clubs, and other "soft targets."

USMC recommended, Measure 19-1: Military police MWD teams conduct walking patrols of selected parts of the installation's housing area perimeter fenceline.

USMC recommended, Measure 19-2: The installation commander implements regulations prohibiting the carrying of parcels into exchanges, clubs, and other designated buildings, except for specific circumstances and through specific doors where they will be checked for contraband. Signs indicating the new regulations should be conspicuously posted at these selected sites.

USMC recommended, Measure 19-3: Security and law enforcement personnel increase patrolling of "soft targets" such as bachelor enlisted quarters (BEQ) and exchanges.

(10) Measure 20. Make organizational staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(11) Measure 21. At an early stage, inform members of local security committees of any action being taken and why.

(12) Measure 22. Physically inspect visitors to the unit, and a percentage of their suitcases, parcels, and other containers.

USMC recommended, Measure 22-1: Commanding officers reduce authorized access points of all buildings under their cognizance, direct random ID checks at all building entrances, and direct the physical inspection of handbags, briefcases and parcels of all visitors.

USMC recommended Measure 22-2: Commanding officers direct 100 percent identification card checks at buildings which are, or contain, high value targets.

USMC recommended, Measure 22-3: Security personnel physically inspect all guests ("official visitors" may be exempted), and escort all visitors.

USMC recommended, Measure 22-4: While issuing visitor passes, MP conduct a physical inspection of visitors entering the installation, to include their suitcases, parcels and other containers.

(13) Measure 23. Whenever possible, operate random patrols to check vehicles, people, and buildings.

USMC recommended, Measure 23-1: Installation MP mobile patrols check roads adjacent to the installation's perimeter fenceline, and report suspicious off-base circumstances to the servicing law enforcement agency. Installation perimeter fencelines not accessible by vehicles should be checked on foot or by MWD teams.

(14) Measure 24. Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock parked vehicles, and to institute a positive system of checks before entering and driving their vehicle.

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

USMC recommended, Measure 25-1: Use frost calls and base/station cable television to disseminate information and directions such as the use of civilian attire, off-limits lists, alternate reporting times, etc.

USMC recommended, Measure 25-2: Train unit high-risk personnel in incident response and emergency aid procedures.

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

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

USMC recommended, Measure 27-1: Emplace barriers at gates near sensitive buildings per the installation's barrier plan.

USMC recommended, Measure 27-2: Support emplaced barriers with sufficient observation.

(18) Measures 28 through 29. Spare.

d. FPCON CHARLIE. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. *Implementation CHARLIE measures will create hardship, and affect the activities of the unit and its personnel.*

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

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

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

(4) Measure 33. Strictly enforce entry control, and search a percentage of vehicles.

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

(6) Measure 35. Issue weapons to guards (local orders should include specific orders on the issue of ammunition). (Note: Marine Corps regulations already prescribe the issuance of loaded weapons to all personnel engaged in law enforcement or security duties.)

(7) Measure 36. Introduce increased patrolling of the installation.

(8) Measure 37. Protect all designated mission essential vulnerable areas (MEVAs) and vulnerable points (VPs). Give special attention to MEVAs and VPs outside of military establishments.

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

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

(11) Measure 40. Spare.

e. FPCON DELTA. 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 or person is imminent. *Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.*

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

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

(3) Measure 43. Identify all vehicles already on the installation within operations or mission support areas.

(4) Measure 44. Search all vehicles entering the installation, as well as their contents.

(5) Measure 45. Control all access, and implement positive identification of all personnel.

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

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

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

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

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

(11) Measure 51. Spare.

6. In addition to the FPCONs above, shipboard and aviation facility FPCONs are contained in DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism.

Force Protection Condition	**Measure**	**Action Set**	**Coordination**
ALPHA	Consult with local authorities on the threat and mutual antiterrorism measures	The installation senior intelligence officer will use all available means to determine the operational capability, intentions, activity, and operational environment of terrorist groups that might threaten the installation. If capabilities are listed, the threat assessment will likely be classified. The classified threat assessment will be maintained at X office by X. Dissemination will be based on a strict need to know basis, with appropriate security clearances.	Interface with local law enforcement agencies. Conduct interagency coordination to obtain terrorist capabilities and intentions. Coordinate with diplomatic missions, as applicable. Coordinate with MI and security personnel to establish the appropriate security controls and need to know.

Table 7-1.--FPCON Synchronization Matirx.

FPCON Alpha	Installation Actions
Definition: FPCON ALPHA applies when there is an increased general threat of possible activity against personnel or facilities, the nature and terrorist extent of which are unpredictable. *ALPHA measures must be capable of being maintained indefinitely*.	Convene FPWG and develop courses of actions. This planning session should consider implementation of higher FPCONs. Further, sequential implementation of FPCONs cannot be assumed. Complete all required actions for previous FPCONs. Report actions complete to the EOC. Be prepared to implement higher FPCONs.
Measure 1: Remind all personnel, including family members, at regular intervals to: (1) Be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. (2) Be alert for unidentified vehicles on, or in the vicinity of U.S. installations, units, or facilities. (3) Be alert for abandoned parcels, suitcases, potential location for explosive devices or any unusual activity. Combatant Commander, Service, or other mandated measures: Brief all personnel on the current threat, and those measures enacted to increase security. Remind all duty personnel to be especially alert for suspicious or unusual activity, strangers, or unidentified vehicles. Combatant Commander, Service, or other mandated measures: Conduct unit level terrorism awareness training.	PAO: Advertise in the installation paper that all personnel should be alert and inquisitive about strangers. Be suspicious of items that don't belong in the area and be alert for abandoned parcels. This information needs to be disseminated to all personnel who work or reside on the Installation. All Units: Regularly brief all personnel on the current terrorism threat as part of the troop information program. EOD: Conduct suspicious packages/IED training for all mail handlers. Unit AT/FP Officers: Advise FPWG that all personnel have received an antiterrorism brief.

Table 7-2.--FPCON Synchronization Installation Action Matrix.

TERRORISM INCIDENT RESPONSE AND TERRORISM CONSEQUENCE MANAGEMENT

1. General. The dividing line between incident response and consequence management is not always distinct, and the two functions may, at times, seem to overlap and become indistinguishable. Terrorism incident response measures can be thought of as immediate actions normally taken by first responders (police/fire/rescue) or task organized incident response teams that are based on established procedures to defeat an attack, minimize loss of life and protect public health. During incident response it may not be clear that the incident was the result of a terrorist act or some other event such as an accident or criminal activity. Terrorism consequence management measures are longer term and wider in scope. Consequence management seeks to alleviate damage, minimize loss of life, hardship or suffering, protect public health and safety; and restore essential emergency services. From a military perspective, consequence management includes the restoration of combat effectiveness.

2. Terrorism Incident Response

a. The purpose of terrorism incident response measures is to establish procedures to be implemented when a terrorist incident occurs at or near the installation/unit's location. Terrorism incident response is an integral element of antiterrorism/force protection planning and is designed to deter, disrupt or mitigate potential terrorist attacks. Response measures should be established for each weapon and tactic that could feasibly be employed against the installation/unit or its personnel as identified in the threat assessment. While these response measures may be very similar to response measures used for criminal activity, they must have the additional level of fidelity needed to cope with the additional demands of a terrorist incident.

b. Terrorism incident response measures shall be designed to facilitate the flow of information within and between all levels of the response infrastructure, and promote interaction and coordination among all responding organizations/units.

c. In general, terrorism incident response measures will provide guidance for:

(1) Reporting the incident.

(2) Determining the nature and scope of the incident response required.

(3) Using the incident command system or other control structure.

(4) Procedures for coordinating emergency response personnel/agencies.

(5) Dispatching emergency response personnel and equipment to the incident site.

(6) Protecting personnel and equipment at the incident site.

(7) Evacuating passengers and nonessential personnel.

(8) Providing incident briefings and situation updates as necessary.

(9) Providing medical treatment and transportation to medical facilities.

(10) Managing the emergency.

(11) Restoring normal operations and reconstituting the ability to perform antiterrorism functions.

(12) Incident debriefings and after-action reports.

d. Terrorism incident response varies depending on the nature and location of the incident. There are generally three distinct phases through which an incident may evolve although many incidents will not develop beyond the first phase. Events of undetermined origin may ultimately be found to have been the result of a terrorist attack. Therefore, care must be taken to treat the location of the incident as a crime scene in order to preserve evidence. This process will aid a follow-on criminal investigation by the Federal Bureau of Investigation (FBI) or host-nation (HN) authorities.

(1) Phase I is the commitment of locally available resources including on-duty watch sections, available military lay enforcement, security force patrols explosive ordnance disposal personnel and available backup units.

(2) Phase II begins when the emergency operations center is activated. It includes the augmentation of the initial response force by additional law enforcement and security personnel and/or special reaction team. During this phase, either the FBI or HN may assume jurisdiction over the incident. If this occurs, Marine Corps forces will assume a supporting role and provide assistance as necessary.

(3) Phase III is the commitment of the specialized FBI, Department of Defense (DOD) or HN counterterrorist forces. During this phase, steps will be taken to terminate the incident through negotiation, assault, or other actions.

e. The table below provides a matrix depicting customary implementation of authority and jurisdiction in terrorism incident responses. It is useful for the commander in determining who has authority during a particular phase of incident response.

f. Commanders shall ensure terrorism incident response measures will contain current residential location information for all assigned personnel (military and civilian) and their dependents when stationed outside the U.S. in areas where the terrorism threat level is “moderate” or greater. Such measures should provide for enhanced security and/or possible evacuation as necessary.

3. Terrorism Consequence Management

a. Terrorism consequence management is a critical portion of the response to terrorism. It should include emergency response, and disaster planning to respond to a terrorist attack for engineering, logistics, medical, mass casualty response transportation, personnel administration, and

local and/or HN support. Effective terrorism consequence management planning can reduce the impact of terrorism on the unit, installation and surrounding community.

b. In addition to chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) weapons, consequence management measures should be established for each weapon and tactic that could feasibly be employed against the installation or its personnel as identified in the threat assessment.

c. In a terrorist incident involving weapons of mass destruction, the key consequence management planning issues are medical and public health. The four major components for consequence management in response to a terrorist incident are threat assessment; emergency consultation; specialized technical assistance; and additional assets as needed from available entities, to include Federal and private sector. Terrorism consequence management plans should address these components.

d. The type of incident encountered drives health response requirements. A chemical incident results in immediate effects at a known site, on-scene determination of the causative agent, and a timely response. The effects of a biological weapon may not be apparent for days and would include response issues such as mass prophylaxis, mass patient care, and mass fatality management. Conventional explosives may potentially involve significant damage to key infrastructure, which will further exacerbate the damage caused by the attack, and would require response forces to be able to support themselves for a period of time.

e. Effective response planning should be directed toward enabling local systems to quickly and safely identify and treat victims in a mass casualty environment, protect those who are at risk, ensure that adequate augmentation to these efforts is available, and recovery operations can commence as soon as possible.

f. Consequence management planning should encompass all aspects of recovery, from initial response to completed recovery.

Incident Location	Initial Response	Containment of Incident	Incident Resolution	Incident Investigation (Lead Agency)	Prosecution (Lead Agency)
DOD Installation (CONUS or U.S. Territories & Possessions)	DOD military/civilian security forces	Initially DOD Military/civilian security forces, with transition to FBI or civilian law enforcement dependent on jurisdiction	Military EST/SRT (customary or usual) FBI or other appropriate civilian law enforcement dependent on jurisdiction	Federal Bureau of Investigations (FBI)	Department of Justice (DOJ)
DOD Personnel Off-Base (CONUS & U.S. Territories or Possessions)	Local law enforcement; FBI	Local law enforcement; FBI	Local law enforcement; FBI	Local law enforcement for state or local law violations; FBI for Federal law violations	Local state's attorney for state or local law violations; DOJ for Federal law violations
DOD Installation Overseas (On Base)	U.S. military/ civilian security forces or host government security forces in accordance with SOFA	U.S. military/ civilian security forces or host government security forces in accordance with SOFA	Host government security forces supported by U.S. military in accordance with SOFA	Host government for prosecuting violation of host nation laws; DOJ for prosecuting violations of U.S. law	Host government for prosecuting violation of host laws; DOJ for Federal law violations
DOD Personnel Overseas (Off Base)	Host government	Host government	Host government with U.S. assistance on request	Host government for investigating violation of host laws; DOJ for investigating violations of U.S. law	Host government for prosecuting violation of host laws; DOJ for prosecuting violation of U.S. laws

Table 8.1--Customary Implementation of Authority and Jurisdiction in Terrorism Incident Response.

SUBORDINATE ELEMENT MISSIONS

This enclosure describes the actions that subordinate elements are required to accomplish in order to comply with this Order and Department of Defense (DOD) Instruction 2000.16 (NOTAL) of 14 June 01.

1. Marine forces commanders/commanding generals/commanding officers (battalion/squadron level and higher) shall implement the following actions:

a. General Development of Antiterrorism (AT) Standards. Commanders shall develop and maintain a comprehensive antiterrorism/force protection (AT/FP) program for personnel and assets for which they have AT/FP responsibility. At a minimum AT/FP programs will address the following general areas:

(1) Procedures will be developed to collect and analyze current terrorist threat information, threat capabilities, and vulnerabilities to terrorist attack.

(2) Terrorism threat assessment, vulnerability assessments, terrorist incident response measures, and terrorist consequence management measures.

(3) Plans and procedures to enhance AT/FP protection.

(4) Procedures to identify AT/FP requirements and program resources.

(5) Construction considerations.

(6) Exercise/deployment considerations.

b. AT Officers (ATOs). ATOs, responsible to the commander, shall be assigned in writing and shall be trained in AT procedures in a formal Level II AT Training course. This may be an additional duty. Enclosure (11) identifies recommended training for assigned ATOs.

c. AT/FP Awareness Programs

(1) Establish command AT/FP information and awareness programs to ensure all assigned and sponsored 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 taken and implemented. FMFM 7-14, MCRP 3-02E, MCO 3460.1A, MCI 02.10b, CJCS 5260 (NOTAL) of 1 Jan 97, DOD Directive 1300.7 (NOTAL) of 8 Dec 00, and DOD Instruction 1300.21 (NOTAL) of 8 Jan 01 will be used as guidance in developing these programs.

(a) At least annually, provide level I AT awareness training to all Marine Corps personnel and civilian employees if they are deployed or eligible for deployment or if the terrorism threat level within the U.S. and its territories rises above moderate. All active duty Marines will receive level I AT awareness training at least annually. Ensure all deploying

Marines are level I qualified prior to overseas deployment. Enclosure (11) applies.

(b) During periods of elevated threat conditions, issue a copy of MCRP 3-02E, The Individual's Guide for Understanding and Surviving Terrorism, or a handout containing essential information derived from that Order, to all personnel.

(c) MCRP 3-02E contains information on vehicle bomb searches. During periods of elevated threat conditions, ensure a copy of MCRP 3-02E or a handout containing essential information derived from that order, is maintained with the government vehicle operator's record (trip ticket) for all government vehicles.

(2) Develop a means of mass notification of unit and installation personnel of actual emergency or implementation of higher FPCONs via systems, methods, or alarms for potential emergencies. The systems, methods, or alarms used should possess a capability to immediately notify personnel of the emergency, should have their own set of reactions, and should be drilled frequently to familiarize all personnel with individual responsibilities and actions.

(3) Provide area of responsibility (AOR)/country specific threat information brief for all personnel planning to travel outside the U.S. regardless of threat level.

(a) Enclosure (11) can be used to assist commands in obtaining AOR/country specific and other terrorism and security related information. Consult the applicable Marine forces ATO for additional information.

(b) Certain additional training requirements such as: code of conduct training, survival evasion resistance escape training, or other on/off-site training may be required before deployment/transfer/travel to a specific country or geographic region. Therefore, coordination with geographic Combatant Commander/Marine forces ATO and U.S. embassy must commence as soon as the requirement for deployment/transfer/travel becomes known.

(4) All Marines shall be encouraged to enroll in Marine Corps Institute (MCI) 02.10B, Terrorism Awareness for Marines, following entry-level training, upon assignment to initial duty station, or prior to deployment. This course is available from the MCI in CD ROM and internet-based versions.

d. Weapons of Mass Destruction (WMD). Commanders will assess the vulnerability of personnel and assets for which they have AT responsibility to terrorist use of WMD including the use of chemical, biological, radiological and nuclear weapons, and high yield explosives (CBRNE). Assessments will address potential use of WMD as well as measures to protect and reduce vulnerability to terrorist use of WMD.

(1) Commanders shall take appropriate measures to protect DOD personnel, families, facilities, and materiel, and reduce the vulnerability to terrorist use of WMD.

(2) Reports through the chain of command shall be processed immediately when organizations with WMD capabilities are identified.

e. AT/FP Plans and Programs. AT/FP programs shall include well-defined plans that describe and implement the program. Commanders shall maintain a comprehensive AT/FP program for those personnel and assets for which they have AT/FP responsibility. The Joint Staff Deputy Directorate for AT/FP, J-3, has developed a product titled the Installation Antiterrorism Program and Planning Tool (IPPT) that provides an AT/FP planning template and WMD appendix in an interactive CD-ROM format. The IPPT may be used as a guide for the development of AT/FP plans for installations, forward deployed and in-transit units. These planning templates are also available in a non-interactive format on-line at the J-34 unclassified website. The website also provides information on how to acquire the planning template CD-ROM. Enclosure (10) contains a sample AT/FP plan for use in the development of AT/FP plans.

(1) AT/FP plans shall clearly describe site-specific AT/FP measures.

(2) AT/FP plans shall be written for permanent operations or locations, and incorporated in operations orders for temporary operations or exercises.

(3) AT/FP programs shall include the tenets of countersurveillance, counterintelligence and other specialized skills and shall identify appropriate organizations as the focal point for the integration of local and/or host-nation (HN) intelligence, counterintelligence, and criminal intelligence information into AT operations. Commanders shall constantly strive to ensure that proactive techniques and assets are incorporated to detect and deter terrorists.

(4) Comprehensive AT/FP plans shall be developed and implemented that provide maximum protection to personnel and assets. At a minimum, plans shall be reviewed, updated, and exercised annually. AT/FP plans shall address the following key elements. If these elements consist of stand-alone documents, they should be replicated in and/or referenced in the AT/FP plan:

(a) Vulnerability in accordance with enclosure (2).

(b) Terrorism threat assessment in accordance with enclosure (3).

(c) Criticality assessment in accordance with enclosure (4).

(d) Risk assessment in accordance with enclosure (5).

(e) AT physical security measures in accordance with enclosure (9).

(f) Terrorism incident response measures and terrorism consequence management measures in accordance with enclosure (8).

(5) Ensure plans, procedures, assessments, and training address potential threats to information systems and the potential use of WMD. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

(6) During periods of elevated threat conditions, initiate random antiterrorism measures (RAMs) as defined in enclosure (1) of this Order.

(7) Contain procedures for notification of higher headquarters in the event of terrorist, criminal or other incidents or the observation of pre-operational activity (e.g., probing, surveillance, bomb threat) through appropriate channels (i.e., OPREP3/SIR, law enforcement, AT/FP working group, etc.) for follow on action.

(a) Whenever an actual terrorist incident occurs, immediately notify the following agency (as appropriate):

1. If the incident occurs within the U.S. or its possessions, notify the servicing field office of the Federal Bureau of Investigation (FBI) and the Naval Criminal Investigative Service (NCIS).

2. If the incident occurs on foreign territory, notify the Combatant Commander who will in turn notify the Department of State (DOS) and HN authorities. Installation commanders will implement applicable provisions of the Status of Forces Agreement (SOFA) or other agreements between the HN and the U.S.

(8) Because incidents of terrorism generate considerable media interest, include the Public Affairs Officer (PAO) in all planning, training, exercises, and operational activities related to terrorist events. PAOs will be guided by chapter 5 and Appendix R of FMFM 7-14 (currently under review for publication as MCRP 3-02D) and Appendix 3 of DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism.

f. Threat Information Collection and Analysis. If applicable, commanders shall task organizations under their command to gather, analyze and disseminate terrorism threat information, as appropriate. Commanders should encourage personnel to report information on individuals, events, or situations that could pose a threat to the security of DOD personnel, families, facilities, and resources.

g. Threat Information Flow. Terrorist activities are best recognized through the sharing of information. Commanders will forward up and down the chain of command all information pertaining to actual and suspected terrorist activity.

(1) Where local information indicates gaps, additional information should be requested via the appropriate intelligence collection and production channels.

(2) Transiting units will be provided with tailored terrorist threat information by their higher headquarters.

h. Physical Security Measures. In order to ensure an integrated approach to AT/FP, tenant commanders must publish a physical security plan that encompasses measures to enhance security, especially during periods of heightened FPCONs, and compliments the overall installation effort. Where there are multiple commanders at an installation, the installation commander

will be responsible for coordinating and integrating the various physical security measures into the AT/FP plan.

(1) AT/FP physical security measures shall integrate facilities, equipment, trained personnel, and procedures in order to maximize protection of personnel and assets. Well-designed measures will deter, detect, delay, deny, defend, and mitigate the effects of an attack. Provisions shall include assessment, notification, and a clear delineation of who will do what, where, when, and how.

(2) Plans shall identify and include provisions for the security of mission essential vulnerable areas (MEVAs) as identified in the criticality assessment, including use of physical security equipment, security procedures, response forces, crisis/consequence management and emergency response.

(3) Physical security measures should include provisions for the use of: physical structures; physical security equipment; chemical, biological, or radiological detection and protection equipment; security procedures; RAMs; response forces; and emergency measures.

(4) Major tenant commands shall actively participate in the installation physical security council and the installation crisis management team (CMT). FMFM 7-14 (currently under review for publication as MCRP 3-02D) applies.

i. AT/FP Program Training and Exercises

(1) Commanders shall conduct field and staff AT/FP training exercises at least annually in order to familiarize personnel with the implementation of the AT/FP plan and to identify requirements and provide justification for budget requests for resources as necessary. AT/FP training shall include: AT/FP physical security measures, terrorist incident response measures and terrorist consequence management measures.

(2) AT/FP training shall be incorporated into unit-level training plans and pre-deployment exercises. AT/FP training shall be evaluated by measurable standards that will include credible deterrence and response standards; deterrence specific tactics, techniques and procedures; terrorist scenarios and hostile intent decision-making. At a minimum these exercises should be operational in nature and should include the evaluation of:

(a) Procedures for collecting, analyzing and disseminating terrorist threat information.

(b) Procedures for analyzing threat capabilities, indications and warnings.

(c) Procedures for determining vulnerabilities to terrorist attack.

(d) Ability to deter incidents and enhance AT/FP protection through the dissemination and implementation of specific FPCON measures.

(e) Alarms and immediate action drills.

(f) Procedures for responding to, containing, mitigating, and recovering from the effects of terrorist incidents.

(g) Procedures for recognition, response, and reporting concealed improvised explosive devices (IEDs).

(h) At the conclusion of every AT/FP exercise, provide an after action report (AAR) for inclusion into the Marine Corps Lessons Learned System (MCLLS), per MCO 5000.17A.

(3) Records of AT/FP training exercises shall be maintained for 1 year.

(4) Commanders shall ensure joint operations and exercises include AT/FP training and planning requirements.

(5) AT/FP plans shall be included in operations orders for permanent and temporary operations and exercises.

j. Comprehensive AT Review

(1) To avoid complacency, commanders at all levels will routinely review effectiveness of daily AT/FP procedures and physical security measures under the prevailing FPCON.

(2) Commanders will review their own AT/FP programs and plans and that of their immediate subordinate in the chain of command at least annually and also whenever the terrorism threat level changes.

(3) AT/FP programs and plans are reviewed to facilitate AT/FP program enhancement, ensure compliance with DOD and Marine Corps AT/FP standards, and ensure the design and implementation of physical security measures coincident with the AT/FP program are consistent with the local terrorism threat level.

k. Construction Considerations

(1) Whenever possible incorporate AT/FP considerations into planning for new construction, renovation and rehabilitation to mitigate AT/FP vulnerabilities and terrorist threats. Ensure that AT/FP protective features and other physical security measures are included in the planning and design of military construction (MILCON) and special projects. The installation provost marshal or other competent authority shall review all MILCON, facility modifications, and special projects.

(2) Commanders shall develop a prioritized list of AT/FP factors for site selection teams. These criteria shall be used to determine if facilities, either currently occupied or under consideration for occupancy can adequately protect occupants from terrorist attack.

l. Deployment Considerations

(1) Effective AT/FP is a fundamental responsibility of the commander during all phases of a deployment. Early and continuous contact with the geographic Combatant Commander’s representatives is important to help

deploying commanders develop appropriate awareness of the threat environment. AT/FP considerations for deployment can be divided into four phases.

(a) Pre-Deployment Activities. Includes identification and training of key personnel, assessment of AT/FP requirements at all deployment locations, development of terrorist threat situational awareness, and close coordination with the combatant commander to ensure continuity of AT/FP functions.

(b) Deployment and Build-Up. Includes movement security, physical security, and operational security.

(c) Integration and Employment. Focus on AT/FP, rear area and line-of-control security operations, harden forces against attack, continue intelligece flow with an end-state goal of a mature AT/FP situational awareness for the threat environment, continually evaluate and update AT/FP posture and procedures through training and assessment, and ensure coordinated hand-off of AT/FP responsibilities between rotating units.

(d) Exit and Redeployment. Continue security functions as forces are withdrawn, continue to evaluate and reassess AT/FP requirements during this phase, safeguard convoys and route of movement, work to counteract complacency during this phase of the operation, exercise, or deployment.

(2) Prevention/detection, mititagtion, and response should be emphasized during all phases of the operation, exercise, or deployment.

2. Commanding generals/commanding officers of installations. In addition to the requirements of paragraph 1 above, installation commanders shall implement the following actions:

a. Physical Security Plans and Procedures. In order to develop and maintain the capability to deter, detect, delay, defend, mitigate and recover from the effects of a terrorist incident installation commanders will draft and maintain a comprehensive and integrated installation physical security plan, per MCO P5530.14. The installation physical security plan will be included as an annex or appendix in the installation AT/FP plan. The physical security plan is not intended to replace the AT/FP plan. At a minimum, this plan will:

(1) Establish and organize the installation physical security council, per MCO P5530.14. The council assists the commander in gaining full community involvement and support in the planning for terrorist and other critical incidents. Membership should include major subordinate activity representatives and key members of the installation staff (such as the comptroller, staff judge advocate, provost marshal, operations security (OPSEC) personnel, intelligence officer and/or NCIS Resident Agent (NCISRA), medical representative, PAO, logistics officer, and facilities engineer, and others). The physical security council shall be convened at least quarterly.

(2) Contain a crisis/consequence management annex, barrier annex, countersurveillance annex, RAM annex, tenant unit plans and other contingency plans or annexes required by unique local conditions.

(3) Establish an installation CMT, per FMFM 7-14 (currently under review for publication as MCRP 3-02D). The CMT coordinates the installation's response to and recovery from a variety of critical incidents, including terrorism. It identifies infrastructures and key assets critical to the installation's operation (e.g., MEVAs). The CMT and physical security council may be combined.

(a) Maintain liaison with local, state, Federal, and foreign authorities. As applicable, memorandum of agreement/memorandum of understanding (MOA/MOU) shall be established on matters pertaining to a coordinated response to security threats, emergency medical response, communications interface with cooperating agencies, intelligence sharing, "posse comitatus" restrictions, and other mutual physical security and loss prevention issues.

(b) The installation provost marshal will keep the servicing NCISRA apprised of these consultations.

(4) Establish and train an installation crisis management force (CMF), per FMFM 7-14 (currently under review for publication as MCRP 3-02D). The CMF provides an organic response capability for crisis situations and falls under the operational control of the installation provost marshal.

(5) Installation commanders may form a special reaction team (SRT) under the auspices of the provost marshal. When established, the installation SRT will be organized, equipped, and trained per MCO P5580.2A. Installations without this capability shall establish an MOA/MOU with local, state, federal or foreign authorities to ensure a capable response.

(a) Installations in the same geographic area may consolidate their resources to form a single regional SRT. Once an SRT is tactically employed, it falls under the operational control of the using installation commander.

(b) Provide for specialized equipment to combat the terrorist threat, such as SRT equipment, lights/mirrors for vehicle undercarriage inspections, portable metal detectors, and similar devices.

(c) Installation commanders will exercise caution when committing the SRT to ensure the team is employed within its operational and equipment capabilities. If a situation exceeds the capability of the local SRT, installation commanders may consider, based on existing MPU/MOAs, requesting additional support from neighboring DOD installations, local law enforcement agencies, and the supporting field office of the FBI. At installations located overseas, the SOFA prescribes options available to the installation commander.

(6) First responders (military police, fire, and medical personnel) shall be trained and equipped to respond to both conventional and WMD attack.

(7) Contain response procedures for a variety of terrorist and other crisis incidents (e.g., hostage/barricade, bomb threat, kidnapping, sabotage, environmental disasters, mass casualty response, weapons of mass destruction etc.) JPUB 3-07.2 of 17 Mar 98, FMFM 7-14 (currently under review for publication as MCRP 3-02D), and enclosure (8) apply.

(8) Contain procedures to provide enhanced AT/FP protection for areas of high population density.

b. AT Guidance for Off-Installation Housing. Commanders in moderate, significant, and high terrorism threat level areas shall provide guidance for assigned personnel who are not assigned on-installation or other Government quarters on the selection of residence to mitigate risk of terrorist attack. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

(1) Periodic physical security reviews of off-installation housing shall be conducted in significant and high threat level areas. Commanders shall provide AT/FP recommendations to residents and facility owner, facilitate additional mitigating measures, and, as appropriate, recommend to appropriate authorities the construction or lease of housing on an installation or in safer areas.

(2) Commanders in significant and high threat level areas shall ensure that an informal residential security review is completed before personnel enter negotiations for lease or purchase of off-installation housing.

(3) Commanders shall include coverage of private residential housing in AT/FP plans where private residential housing must be used in moderate, significant, or high threat level areas.

(4) Commanders at all levels shall incorporate family member and dependent vulnerabilities into all antiterrorism assessment, mitigation, and reporting tools. In moderate, significant, or high threat level areas, commanders shall include coverage of facilities and transportation service and routes used by personnel and their dependents.

(5) Ensure terrorism incident response plans contain current residential location information for all DOD personnel and their dependents assigned to moderate, significant or high terrorism threat level areas. Such plans should provide for enhanced security measures and/or possible evacuation of DOD personnel and their dependents. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

c. Executive Protection and High-Risk Personnel Security

(1) Commanders shall be familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DOD officials who are entitled to additional protection as a result of their position. Commanders shall take measures necessary to provide appropriate protective services for such individuals in high-risk billets and high-risk personnel. Review and revalidation of protective services shall occur on at least an annual basis.

(2) Commanders should ensure individuals requesting supplemental security measures are aware of constraints and understand their individual responsibilities in accepting additional security measures. Commanders should ensure individuals receiving supplemental security measures have

completed required AT training, are cleared for assignment to billets, facilities, or countries requiring such protection, and have been thoroughly briefed on the duties of protective service personnel.

(3) Reviews of supplemental security needs shall be undertaken within 30 days of a change in the terrorism threat level assigned to an AOR containing high-risk billets or to which high-risk personnel have been assigned.

(4) Commanders shall be familiar with the application of security measures for DOD officers in high-risk billets and shall take measures necessary to provide appropriate protective services for such individuals. Review and revalidation of protective services will occur on at least an annual basis. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

(5) The assignment of Marines to certain billets external to the Marine Corps may require special training to properly prepare them for the potential hazards of these assignments. Personnel assigned to designated "high-risk billets" shall be screened to ensure completion of required training. Enclosures (11) and (13) apply.

d. Exercises and Training. Conduct an AT/FP exercise at least annually to evaluate the installation's ability to counter or contain a terrorist threat.

(1) This AT/FP exercise will be operational in nature and will include activation of the installation emergency operations center, the crisis intelligence cell, the CMT, the CMF, all installation and tenant commands, and other activities as appropriate. Representatives from the servicing NCISRA and civilian law enforcement agencies should be involved to the maximum extent possible.

(2) At the request of the installation commander, and if funding is provided by the installation, the Deputy Commandant for Plans, Policies, and Operations (DC PP&O) (PS) may provide an observer or evaluator to assist the base or station in the conduct of the AT/FP exercise.

(3) At the conclusion of every AT/FP exercise, provide an AAR for inclusion into the MCLLS, per MCO 5000.17A.

e. Vulnerability Assessments. Due to the unique skill sets necessary to perform a thorough vulnerability assessment, installation commanders should develop organic resources capable of supporting requests from tenant units for assistance in the completion of these assessments. Resources may also include assistance from the other services, U.S. Government agencies, or the local community through the conditions of a MOU/MOA.

3. Commanding generals/commanding officers of Marine Corps air stations, Marine Corps air facilities and Marine Corps airfields. In addition to the requirements previously mentioned, airfield and air station commanders shall:

a. Assign flight line security (FLS) priorities based on the threat level and the nature of assets being protected. The FLS Program was established to increase the level of physical security of assets within the

flight line restricted area through systematic employment of security personnel and equipment designed to detect, delay, and/or deny access to unauthorized personnel. The level of security inherent at the installation determines the extent of the FLS effort required, and must be considered when distributing resources for the execution of the FLS program, as per MCO 5500.14A

b. Provide the Federal Aviation Administration and other authorized federal officials all information pertaining to aircraft piracy, such as onboard documents, equipment, weapons of mass destruction, or material determined to be sensitive in nature. CJCS Instruction 3610.01A (NOTAL)of 1 Jun 01 applies.

4. Deputy Commandant for Plans, Policies, and Operations (DC PP&O) shall:

a. Designate a full-time staff officer in writing to supervise, inspect, exercise, review, assess, and report on Marine Corps AT/FP programs.

b. Exercise overall staff cognizance for matters relating to AT/FP.

c. Coordinate physical security, military police, Marine Security Guard (MSG), and Marine Corps Security Force (MCSF) issues and initiatives in support of Marine Corps AT programs.

d. Represent the Marine Corps at the annual DOD worldwide AT conference, and other AT/FP fora.

e. Represent the Marine Corps at the DOD AT coordinating committee, its subcommittees, and its executive council.

f. Represent the Marine Corps at the DOD physical security review board (PSRB).

g. Perform those other specific duties pertaining to the screening and specialized training of personnel assigned to high-risk billets, as listed in enclosure (13) of this Order.

h. Coordinate with the Deputy Naval Inspector General for Marine Corps Matters/Inspector General of the Marine Corps (DNIGMC/IGMC) regarding integration of the provisions of this order into the automated inspection reporting system (AIRS) discrepancy listing.

i. Coordinate/schedule higher headquarters level assessments of installation and unit AT/FP plans at least once every three years.

j. Provide augmentation assistance to DNIGMC/IGMC in evaluations of unit and installation AT/FP plans.

k. Publish a MCBul that identifies all external high-risk billets and associated required training for those billets per enclosure (13) of this order.

5. Deputy Commandant for Manpower and Reserve Affairs (DC M&RA) (MMEA/MMOA), Headquarters, U.S. Marine Corps shall:

a. Perform, as listed in enclosure (13) of this Order, those duties pertaining to the screening and specialized training of personnel assigned to hazardous billets.

b. Modify existing leave and liberty policy and NAVMC 3 (Leave and Authorization Form) to certify accomplishment of level I training prior to foreign leave.

6. Deputy Naval Inspector General for Marine Corps Matters/Inspector General of the Marine Corps (DNIGMC/IGMC) shall:

a. Coordinate with the DC PP&O (PS) regarding integration of the provisions of this Order into the AIRS discrepancy listing.

b. Conduct evaluations of unit and installation AT/FP programs.

7. Commanding General, Marine Corps Combat Development Command (T&E), Quantico, VA shall:

a. Establish and coordinate with the DC PP&O (PS) quotas for appropriate schools, including those in enclosure (11), to ensure that sufficient training opportunities are available to support the requirements of this Order and disseminate related training information as required.

b. Perform, as listed in enclosure (13) of this Order, those duties pertaining to the screening and specialized training of personnel assigned to hazardous billets.

c. Per DOD Instruction 2000.16 (NOTAL) of 14 Jun 01 and enclosure (11), provide entry-level AT/FP instruction to all Marine recruits and all Marine officer candidates, to familiarize them with the terrorist threat and appropriate individual protective measures. Coordinate the development of program of instruction (POI) for entry-level AT/FP instruction with CG MCCDC (T&E) to ensure a common standard for all recruit and officer candidate training is achieved.

d. Develop appropriate POIs for level I, II, and III training and ensure that AT/FP instruction is incorporated into all appropriate professional military education courses.

8. Deputy Commandant for Programs and Resources (DC P&R) shall: ensure adequate funding for antiterrorism and force protection programs.

9. Director, Command, Control, Communications, Computers (C4)/Commander MARFOR-INO shall develop and implement an information systems security program that provides direction, guidance, and measures, both procedural and material, to protect Marine Corps information systems.

a. Utilize state-of-the-art technologies to counter rapidly changing threats and vulnerabilities to C4 structures.

b. Provide training to end users and system support personnel to heighten awareness and develop abilities to counter emerging threats and vulnerabilities.

c. Deploy computer network defense tools throughout the Marine Corps' C4 system.

d. Employ a defense-in-depth strategy by integrating the capabilities of people, procedures and technology to achieve strong, effective, multi-layer, and multi-dimensional protections.

10. Director, Intelligence (I) shall:

a. Support and coordinate with the DC PP&O (PS) regarding requirements for terrorism-related intelligence.

b. Develop assessments for potential terrorist use of WMD against personnel and assets. Process reports immediately when significant information is obtained identifying organizations with WMD capabilities.

11. Deputy Commandant, Installations and Logistics (DC I&L) shall:

a. Support and coordinate with the Naval Facilities Engineering Command (NAVFAC) the development of policy for installation facility master planning which factors in and documents the requirement for AT/FP.

b. Develop and maintain a tracking system to identify MILCON programming and expenditures for AT/FP.

c. Support and coordinate with NAVFAC the development of policies/ prescriptive standards that incorporate design measures into MILCON projects and modifications to existing facilities.

d. Support force readiness by anticipating, articulating and identifying installation requirements for training, programs, systems, organizations, facilities support, and services to support Force Protection Requirements such as:

(1) Intrusion detection systems, ground sensors, closed circuit television, day and night surveillance cameras, thermal imaging, perimeter lighting and advanced communication equipment, to improve security at all sites.

(2) Employ explosive detection and countermeasures devices.

(3) Physically harden structures.

(4) Develop guidance on required standoff distances and the construction of blast walls and the hardening of buildings.

(5) Relocate and consolidate units at vulnerable facilities to more secure sites.

(6) Reinforce entry control points and provide a defense in depth.

(7) Cable single rows of Jersey barriers together and use enhanced barriers to shield and protect vulnerable compounds and structures.

(8) Establish threat based standoff or exclusion areas around compounds and bases.

e. Provide guidance to in-garrison and deployed units as to readily available equipment and standards for installation AT/FP.

f. Logistics contracting processes shall be designed to incorporate considerations for AT/FP measures during contracting requirements, award, execution, and the evaluation process when the effort to be contracted for could affect the security of operating forces, particularly in-transit forces. During the evaluation process, future contract awards shall consider adequate AT/FP performance.

12. Commanding officers of Marine Corps organizations physically located outside a Marine Corps installation (i.e., Marine Corps recruiting districts and stations, Marine Corps reserve units, etc.) will comply with applicable provisions of this Order, and the reporting requirements specified in paragraph 1e(7) of this enclosure.

13. Headquarters Marine Corps Health Services. Provide information relative to CBNRE effects, decontamination, treatment, and inoculation, quarantine, triage, and mass casualty treatment techniques as applicable.

14. Marine Corps Systems Command (MCSC) shall implement the following actions:

a. Upon request, MCSC shall provide assistance to installations and commands on the procurement of their AT/FP equipment needs. This can include market research, technological availability, and upon receipt of funding, MCSC can conduct centralized acquisition of validated requirements.

b. Upon request, MCSC will inform the installations and commands of readily available equipment and technologies that may address respective AT/FP missions based upon past market analysis, on-going programs, and other known sources.

c. With identification of funding, MCSC can maintain equipment listing of items that are readily available for use with/for AT/FP missions. This activity would also include monitoring individual command and installation purchases, market research/analysis, and maintenance of a centralized database (web based) that could be accessed by any Marine command or installation.

SAMPLE ANTITERRORISM/FORCE PROTECTION (AT/FP) PLAN

UNITED STATES MARINE CORPS
[INSTALLATION/UNIT NAME]
[CITY, ST ZIP]

[DATE]

[INSTALLATION/UNIT NAME] AT/FPP - 02

COPY_____ OF _____ COPIES

UNITED STATES MARINE CORPS
[INSTALLATION/UNIT NAME]
[LOCATION]

[INSTALLATION/UNIT NAME] AT/FPP - 02

TABLE OF CONTENTS

[INSTALLATION/UNIT NAME] AT/FPP - 99

UNITED STATES MARINE CORPS
[INSTALLATION/UNIT NAME]
[CITY, ST ZIP]

[DATE]

[INSTALLATION/UNIT NAME] AT/FPP-99

SECURITY INSTRUCTIONS

1. The long title of this plan is [Installation/Unit Name] Antiterrorism/Force Protection Plan 02. The short title is [AT/FPP-02]. This plan will be revised or updated annually.

2. The contents of the AT/FPP-02 are "FOR OFFICIAL USE ONLY".

3. Authority is granted to reproduce extracts from the AT/FPP-02 for internal use only. Authority to reproduce this document for distribution outside the Command is vested with Director, Operations Division.

UNITED STATES MARINE CORPS
[INSTALLATION/UNIT NAME]
[CITY, ST]

[DATE]

AT/FPP-02
RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE OF ENTRY	SIGNATURE

MCO 3302.1D
18 Jul 2002

UNITED STATES MARINE CORPS
[INSTALLATION/UNIT NAME]
CITY, ST

[DATE]

AT/FPP-02

PLAN SUMMARY

1. Purpose. [*Commentary:* The antiterrorism/force protection plan will define the nature and scope of emergency response planning. It will set forth emergency operations procedures and provide guidance for emergency preparedness, disaster relief and antiterrorism operations.]

2. Background. [*Commentary:* Military installations are vulnerable to natural and manmade disasters such as flash flooding, hurricanes, thunderstorms, hazardous material incidents, resource shortages, terrorist activities, general civil disturbances or other disasters. Recent world events have demonstrated a willingness of terrorists to use weapons of mass destruction which have the potential to produce catastrophic loss of life and property destruction. It is therefore prudent that commanders maintain effective plans and preparations for dealing with these potential manmade or natural incidents. This plan will outline the organization, assignments, and procedures to be executed in the event of a significant crisis.]

3. Summary

a. [*Commentary:* The primary mission of the command in any emergency is to protect the lives of personnel, and minimize damage or loss to military and personnel property. The plan will be developed to provide a sound basis for emergency preparedness programs and training activities. Furthermore, the plan will establish the organizational and operational concepts and procedures necessary to minimize loss of life and property damage and expedite recovery operations.]

b. [*Commentary:* In the preparation of the plan, emergency responsibilities will be assigned, when possible, to activities having the same or similar responsibilities during normal operations. For many, this plan represents a logical expansion of existing functional responsibilities.]

MCO 3302.1D
18 Jul 2002

Copy no. ____ of ____ Copies
[Installation/Unit Name]
[Location]
[DTG]

[INSTALLATION/UNIT NAME ANTITERRORISM/FORCE PROTECTION PLAN (AT/FPP) 02 (AT/FPP-02)(U)

(U) References: See appendix 4 (Publication Reference List) to annex V (References).

(U) Time Zone: Lima (Local).

(U) Task Organization. See annex A (Task Organization).

1. (U) SITUATION

a. (U) General. [*Commentary:* The plan applies to all personnel assigned or attached to the installation/unit. The political/military environment should be described in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation antiterrorism/force protection (AT/FP) operations. Mission accomplishment, personnel safety, security, and safeguarding equipment are inherent responsibilities of the Commander. The protection of personnel and assets, from incidents ranging from natural disasters (such as severe weather) to manmade hazards (ranging from hazardous material incidents to terrorist acts), present many complex challenges. The plan establishes a baseline AT/FP posture which can be "ramped up" in response to potential or realized threats.]

b. (U) Enemy. See annex B (Intelligence). [*Commentary:* The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. Describe the general threat of terrorism including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of weapons of mass destruction (WMD). This information should remain unclassified when possible. Annex B, Intelligence, should identify specific threats.]

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships). [*Commentary:* Specify the forces available (both military and civilian) to respond to a terrorist attack. Include the next higher headquarters and adjacent installations, and any units/organizations that are not under installation command, but may be required to respond to such an incident. These units/organizations may include host-nation (HN) and U.S. military police forces, fire and emergency services, medical, and federal/state and local agencies, special operations forces, engineers, detection (chemical, biological, radiological, and nuclear), decontamination units and explosive ordnance disposal (EOD). Include effective memorandum of agreement/memorandum of understanding (MOAs/MOUs) and any other special arrangements that will improve forces available to support the plan.]

d. (U) Attachments/Detachments. See annex A (Task Organization) and annex J (Command Relationships). [*Commentary:* List any installation/civilian agencies NOT normally assigned to the installation that are needed to support

the plan. Explain interagency relationships and interoperability issues. This information can be listed in other annexes.]

e. (U) Assumptions

(1) (U) (List planning/execution assumptions) [*Commentary:* Include all critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT/FP plan. Examples of some typical assumptions are listed below:

(a) (U) Natural disasters and destructive weather such as hurricanes, tornadoes, lightning, snow, flooding, forest fires, and earthquakes are likely to occur.

(b) (U) Manmade incidents (Criminal/Non-criminal) such as: theft, sabotage, hazardous material spills, WMD, chemical, biological, radiological, nuclear, and high yield explosive (CBRNE) devices, mass casualty incidents, increasing threat conditions based on intelligence on terrorist or criminal activity, bomb threat, and hostage/barricaded suspect(s).

(c) (U) Tenant organizations available to support AT/FP operations.

(d) (U) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(e) (U) Terrorists, criminals, protesters, subversives, and natural disasters will remain a threat to U.S. installations.

(f) (U) The unpredictability and increasing sophistication of terrorism could result in incidents occurring with little to no forewarning.

(g) (U) Sound security measures, randomly implemented, are viable, visible deterrents to terrorists.

(h) (U) Routine and/or lax security measures accentuate vulnerabilities.

(i) (U) Federal, state, and local resources will be available to augment response limitations. Local, non-military response forces will arrive within [time] of notification.

(j) (U) Units specializing in WMD response will arrive on-site within [number of hours based on installation location] of notification.

(k) (U) The HN is supportive of U.S. policies, and will fulfill surge requirements needed to respond to a WMD incident in accordance with standing MOAs/MOUs.]

2. (U) MISSION. [*Commentary:* Construct a clear, concise statement of the command's mission and describe how AT/FP supports the mission. The primary purpose of the AT/FP plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat,

enhance security and AT/FP awareness, and to assign AT/FP responsibilities for installation personnel.

Example for an installation: MCB, (installation) will, in conjunction with tenant organizations, local, county, state, and federal agencies, conduct continuous AT/FP operations within the boundaries of MCB (installation) and the surrounding area, as described in appropriate MOU/MOA, in order to deter, detect, delay, and defend Marines, sailors, civilian employees, their families, and base resources from the effects of natural disasters or manmade incidents. In the event a natural disaster or manmade incident occurs, exercise incident response and consequence management measures as described in this Plan to minimize disruption to the execution of base and tenant organizational missions and restore operational capabilities as soon as possible.

Example for a deployed unit: 1st Bn, (Regiment) Marines when deployed will be operating within the jurisdiction of (country) and will be a tenant command at (installation). 1st Bn, (Regiment) Marines, will conduct continuous AT/FP operations in order to deter, detect, delay, and defend Marines, sailors, civilian employees, and their families from natural or manmade incidents. In the event of a natural disaster or manmade incident, exercise incident response and consequence management measures as described in this Plan to minimize disruption and restore operational capabilities as soon as possible. The actions undertaken will be governed by MOU/MOA established between the HN and the installation and appropriate coordination between the installation and 1st Bn, (Regiment) Marines as described in this Plan.

3. (U) EXECUTION

a. (U) AT/FP Plan Development. [*Commentary:* This section should describe AT/FP plan development. The development of the plan is an iterative versus sequential process. That is, each step may yield new information that affects the information developed earlier. Data gathered during each step should be documented and maintained for further analysis and presentation as backup data for proposed recommendations and alternatives. The process of begins with the antiterrorism officer (ATO) working with an AT/FP working group that has been appointed by the commander to assist in plan development. The plan should describe the composition, charter, and responsibilities of the AT/FP working group.]

(1) (U) Vulnerability Assessment. [*Commentary:* An installation/unit vulnerability assessment is the foundation upon which the AT/FP plan is built. It complements the criticality assessment and threat assessment and completes the picture of how a unit or installation might be attacked. The ATO with the AT/FP working group will conduct a vulnerability assessment at least annually, as required by MCO 3302.1D, that considers the full range of terrorist weapons and capabilities. The result of the vulnerability assessment will be a prioritized listing of specific target vulnerabilities.]

(2) (U) Terrorist Threat Assessment. [*Commentary:* The second step in plan development is the terrorist threat assessment. Commanders will prepare a terrorist threat assessment at least annually that will identify the full spectrum of known or estimated terrorist capabilities including weapons and tactics. The threat assessment will integrate threat information prepared by the intelligence community, technical information from security and

engineering planners, and information from other sources. Appendix 1 of enclosure 2 to MCO 3302.1D provides a range of terrorist threat capabilities that will be used as the threat baseline for planning purposes.]

(3) (U) Criticality Assessment. [*Commentary:* The third step in plan development is the criticality assessment. The conduct of the criticality assessment will result in a list of mission essential vulnerable areas (MEVAs)(located in tab A to appendix 3 to annex C of this sample order), and other assets that should be considered potential targets because of their value to the commander in terms of potential loss of life, psychological, economic, or sociological impacts.]

(4) (U) Risk Assessment. [*Commentary:* The fourth step in AT/FP plan development is the risk assessment. The risk assessment allows the commander to plan for the most effective use of the resources available and to develop requirements for additional funding requests.]

(5) (U) [*Commentary:* Once the above steps have been completed, the commander can develop force protection condition (FPCON) integrated action sets (located in enclosure (1) to tab (D) to appendix (3) to annex (C) that provide specific actions for each measure of each FPCON for each anticipated terrorist threat capability. If future terrorist threat assessments provide information of terrorist capabilities exceeding the baseline threat, the commander will need to reevaluate the integrated action sets.]

(6) (U) [*Commentary:* With the information developed thus far, combined with information from other available resources, the commander should be able to compile additional information to support additional portions of the AT/FP plan.]

b. (U) Concept of Operations. [*Commentary:* The installation's AT/FP concept of operations should be phased in relation to pre-incident, incident, and post-incident actions. AT/FP planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations.]

(1) (U) Pre-Incident Phase. [*Commentary:* This phase integrates and includes all pre-incident response and consequence management planning, equipment acquisition, training, education, construction considerations, and special and routine actions taken before an attack or incident occurs.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase includes all actions to be taken once an incident occurs. Depending on the severity of the incident, these actions may include but are not limited to: activation of the emergency operations center (EOC) and the crisis management team (CMT), deployment of first responders and crisis management force (CMF), activation of MOU/MOAs as necessary. It also includes actions taken to manage the incident and actions directed towards a return to normal operations. Actions taken during the incident phase are critically reviewed and improvements to the plan are made.]

(3) (U) [*Commentary:* The situation may dictate that the installation not only conducts the initial response but also sustained response operations. In the domestic U.S., national-level responders (Federal Emergency Management Agency (FEMA), Red Cross, and Federal Bureau of

Investigation (FBI)) may not be immediately accessible or available to respond to an installation's needs. Overseas, HN support may be available as established in standing MOU/MOAs. The commander should be familiar enough with the HN's supporting agencies; their command structure and operating environment to know how completely the support detailed in the MOU/MOAs will be delivered. In either case, the installation must plan for the worst-case scenario, by planning its response based on the organic resources available and anticipated support through MOA/MOUs.]

b. (U) Tasks. [*Commentary:* Specific tasks for each subordinate unit or element listed in the task organization paragraph. Key members of the installation have responsibilities that are AT/FP and/or WMD specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the tasks and responsibilities, what these responsibilities entail, and how these will be implemented. While the tasks and responsibilities for each AT/FP planning and response element will be delineated in the pre-incident, incident and post-incident action set matrices, it is recommended that the installation commander identify/designate the primary lead for each element and enter that information in this paragraph.]

(1) (U) [First Subordinate Unit/Element/Tenant]

(a) (U) [Task Listing.]

c. (U) Coordinating Instructions. [*Commentary:* This paragraph should include antiterrorism (AT) specific coordinating instructions and subparagraphs, as the commander deems appropriate. In addition, this section of the AT/FP plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT/FP plan. Coordinating instruction functional areas include: 1) AT planning and response elements; 2) procedural; 3) security posture; 4) threat specific responsibilities; and, 5) special installation areas. The reader will be directed to specific annexes that will provide amplifying instructions on these topics. The sections listed below are representative, and may not be all-inclusive. Any of the functional areas described below may or may not apply in a given case. The areas described below may be addressed in separate annexes or in the basic order depending on the needs of the installation/unit.]

(1) (U) AT Planning and Response. [*Commentary:* Initial and sustained response to an attack must be a coordinated effort between the many AT/FP planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the local/state/federal agencies within the U.S. or HN when located overseas.

(2) (U) Procedural

(a) (U) Alert Notification Procedures. See annex C (Operations) and annex K (Communications and Information Systems).

(b) (U) Use of Force/Rules of Engagement. See annex H (Legal).

(c) (U) Installation Training & Exercises. See annex O (Training).

(d) (U) Incident Response. See annex C (Operations).

(e) (U) Consequence Management. See annex C (Operations).

(f) (U) High-Risk Personnel Protection Procedures. See appendix 9 to annex C (Operations).

(g) (U) AT Program Review. See annex O (Training).

(h) (U) Higher Headquarters Vulnerability Assessments. See appendix 4 to annex O (Training).

(3) (U) Security Posture Responsibilities

(a) (U) Law Enforcement. See appendix 8 to annex C (Operations).

(b) (U) Physical Security. To include lighting, barriers, access control. See appendix 7 to annex C (Operations).

(c) (U) Other On-Site Security Elements. See appendix 8 to annex C (Operations).

(d) (U) Operations Security. See appendix 11 to annex C (Operations).

(e) (U) Technology. See the basic order.

(f) (U) EOC Operations. See appendix 12 to annex C (Operations)

(g) (U) Critical Infrastructure Protection. See appendix 14 to annex C (Operations).

(f) (U) Other.

(4) (U) Threat Specific Responsibilities

(a) (U) HAZMAT (Optional). See appendix 2 to annex C (Operations).

(b) (U) Antiterrorism. See appendix 3 to annex C (Operations).

(c) (U) Bomb Threats. See appendix 4 to annex C (Operations).

(d) (U) Hostage/Barricaded Suspect(s). See appendix 5 to annex C (Operations).

(e) (U) Weapons of Mass Destruction. See appendix 6 to annex C (Operations).

(f) (U) Information Operations. See appendix 10 to annex C (Operations).

(g) (U) Other.

(5) (U) Special Security Areas

(a) (U) Airfield Security. See appendix 13 to annex C (Operations).

(b) (U) Port Security. See appendix 13 to annex C (Operations).

(c) (U) Embarkation/Arrival Areas. See appendix 13 to annex C (Operations).

(d) (U) Buildings. See appendix 13 to annex C (Operations).

(e) (U) Other.]

4. (U) ADMINISTRATION AND LOGISTICS. [*Commentary:* Include the administrative and logistics requirements to support the AT/FP plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for pre-incident, incident, and post-incident measures addressing the following: locations of consolidated WMD defense equipment; expedient decontamination supplies; individual protective equipment exchange points; special contamination control requirements; retrograde contamination monitoring sites; WMD equipment/supply controlled supply rates and pre-stockage points; and procedures for acquire chemical defense equipment. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the concept of operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Finally, include fiscal instructions on how to support AT/FP operations.]

a. (U) Administration. See annex P (Personnel Services).

b. (U) Logistics. See annexes D (Logistics), E (Fiscal).

c. (U) Reports. See annex U (Reports). [*Commentary:* Reports are required by MCO 3302.1D and may be required by higher headquarters.]

5. (U) COMMAND AND SIGNAL. [*Commentary:* Include instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and emergency operations center. Enter the installation's chain-of-command. Highlight any deviation from that chain-of-command that may occur as a result of a WMD incident. The chain-of-command may change based on the deployment of a joint task force or a national command authority-directed mission. Identify the location of chemical staffs or any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Coordinate with higher headquarters to establish procedures to allow for parallel coordination with higher and the service component operations center to report a terrorist WMD incident. The installation must provide for prompt dissemination of notifications and alarm signals, and the timely/orderly transmission and receipt of messages between elements involved in and responding to the incident.]

a. (U) Command Relationships. See annex A (Task Organization) and annex J (Command Relationships).

b. (U) C3 Systems. See annex K (Communications and Information Systems).

c. (U) Command Post Locations

(1) (U) Primary: [Location]

(2) (U) Alternate: [Location]

d. (U) Succession of Command

(1) (U) First alternate: [Position/Title]

(2) (U) Second alternate: [Position/Title]

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

Annexes:

A – Task Organization
B - Intelligence
C - Operations
D - Logistics
E - Fiscal
F – Public Affairs
G - Air Operations
H - Legal
I – Area Commanders
J - Command Relationships
K – Communications and Information Systems
L - Health Services
M - Safety
N - Execution Checklist
O – Training
P – Personnel Services
U - Reports
V – References
Z - Distribution

ANNEX A (TASK ORGANIZATION) TO AT/FPP-02 (U)

(U) References: See appendix 4 (Publication Reference List) to annex V (References).

(U) Time Zone: Lima (Local).

1. (U) AT/FP WORKING GROUP (PRE-INCIDENT). [*Commentary:* The AT/FP working group is task organized to support the commanders AT/FP program. Members are selected based on their wide range of experience and capabilities. Membership should include each organization that will provide input into the AT/FP plan, including HN and representatives of organizations with which MOU/MOAs have been executed. The AT/FP working group may breakdown into smaller functional area working groups, but its main purpose is to ensure that a sufficient level of coordination between all components of the AT/FP plan has been obtained.] See annex J (Command Relationships).

2. (U) PHYSICAL SECURITY COUNCIL (PSC) TASK ORGANIZATIONS (PRE-INCIDENT). [*Commentary:* The task organized structure represented will be used to implement AT/FPP-02 and is designed to synchronize AT/FP efforts under one commander. Normal operational and administrative command structure will not be circumvented.] See annex J (Command Relationships).

Organization	Personnel Assigned

3. (U) CMT TASK ORGANIZATIONS (INCIDENT RESPONSE AND CONSEQUENCE MANAGEMENT). [*Commentary:* The CMT is activated, upon direction of the commander to perform incident response and consequence management for incidents that are beyond normal response capabilities of installation/unit activities.]

Organization	Personnel Assigned

Appendices:

1 - Table of Organization

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 1 (TABLE OF ORGANIZATION) TO ANNEX A (TASK ORGANIZATION) TO AT/FPP-02 (U)

(U) T/O Line#	(U) Billet	(U) Rank	(U) MOS	(U) Organization
Emergency Operations Center				
Crisis Humanitarian Assistance Plan				
Family Assistance Center/Emergency Shelters				
Reaction Platoon				
Checkpoints	Additional Gate Security			
Command Information Bureau				

Official:

[Name]

[Title]

ANNEX B (INTELLIGENCE) TO AT/FPP-02 (U)

(U) References: See appendix 4 (Publications Reference List) to annex V (References).

(U) Time Zone: Lima (Local)

1. (U) SITUATION

a. (U) General. [*Commentary:* This annex supports the commander's intent by coordinating the intelligence functions that provide support to AT/FP issues. Generally, the information contained in this annex will be provided by the intelligence agency supporting the installation/unit. It should include the person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence.] [National-level agencies, Combatant Commanders and intelligence systems provide theater or country threat levels and threat assessments. Obtain these assessments, as they will serve as a baseline for the installation's tailored assessment. The installation should have a process in place for developing the installation's tailored threat assessment or "local threat picture." The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation's tailored AT product. Note: Overseas commanders cannot change the threat level, which is developed at the national-level although they CAN change FPCONs. The Defense Intelligence Agency (DIA) does not issue a Threat level for installations located within the U.S. Therefore; the installation must obtain the local terrorist threat information from the Naval Criminal Investigation Service Resident Agent (NCISRA).]

b. (U) Characteristics of the Area.

c. (U) Climatology.

d. (U) Terrain.

e. (U) Enemy Forces.

(1) (U) See appendix 1 (Threat Assessment)

(2) (U) [*Commentary:* Opposing forces may include, but are not limited to the following:

(a) (U) Terrorist organizations, whose operational traditions may be either national (to include domestic organizations), transnational or international. These groups may be either non-state supported, state supported, or state directed. Such organizations can be expected to operate in a determined fashion to achieve their political goals and are prepared to kill innocent bystanders in the process.

(b) (U) Subversive, radical and other dissident groups or elements which may commit unlawful acts with a primary goal of disrupting base activities.

(c) (U) A mentally disturbed individual(s).

(d) (U) One or more common criminals forced to take hostages to effect their escape. Criminals may change (or appear to change) their objectives and become "politically motivated" when it suits their illicit purpose.

(e) (U) Catastrophic natural or man-made disasters, such as hurricanes, tornadoes, high winds, earthquakes and forest fires.

(3) (U) Opposing forces may be armed and dangerous.

(4) (U) Opposing forces' actions and reactions may be difficult to predict.]

f. (U) Friendly Forces

(1) (U) Military forces. See annex A (Task Organization) and annex J (Command Relationships).

(2) (U) Civilian forces. [*Commentary:* List or describe support from Federal, state, county and local law enforcement agencies may become involved in AT/FP incidents/operations in mutual aid situations. Additionally, the Naval Criminal Investigative Service (NCIS) has exclusive responsibility for criminal and security investigative or counterintelligence matters with Federal law enforcement agencies. NCIS is the primary agency for liaison with state and local and foreign law enforcement, security and intelligence agencies, including those of military departments. See annex A (Task Organization) and annex J (Command Relationships) for additional information on the relationship between military and civilian agencies.]

g. (U) Assumptions

(1) (U) (List intelligence assumptions) [*Commentary:* Include all critical assumptions used as a basis for this annex. Possible examples follow:

(a) (U) The installation/unit is a potential target for terrorism, criminal activity, civil disturbances, and man-made or natural disasters.

(b) (U) Resident security forces may be inadequate in some instances.

(c) (U) Terrorist attacks have the potential to adversely affect both military and civilian activities on and in the vicinity of the installation or unit. Mutual assistance between military and civilian law enforcement, first responders and emergency management agencies will be necessary and available through MOA/MOU.

(d) (U) The impact of terrorist attack or other types of incidents may be diminished through warnings and advisories disseminated by Federal, state and local authorities as well as commercial news media.]

2. (U) MISSION. [*Commentary:* The installation/unit will maintain the ability to collect, process, analyze, disseminate intelligence and blend various intelligence disciplines in order to provide a proactive, tactically sound AT/FP plan and security posture.]

3. (U) EXECUTION

a. (U) Intent: [*Commentary:* This annex is intended to supplement and support an aggressive AT/FP program by providing guidance for the collection, analysis and dissemination of intelligence in order to support AT/FP operations.]

b. (U) Concept of Operations. [*Commentary:* The primary source of criminal intelligence and foreign counterintelligence material, documentation, and information for installations and units located within the U.S. will be provided by NCIS. Secondary sources of information, both internal and external (from local civilian law enforcement authorities and installation military police) can and will be used to supplement the NCIS information gathering effort.] [Overseas, the gathering of terrorist information is principally a Central Intelligence Agency (CIA) responsibility with the Department of State (DOS), DIA and HN being active players. Units deploying to an area under the cognizance of a Geographic Combatant Commander can obtain threat analysis information from the Combatant Commander through the chain-of-command.]

(1) (U) [*Commentary:* NCIS performs the Intelligence mission, to ensure the availability of accurate and timely intelligence necessary to successfully accomplish the mission, and satisfy requests for essential elements of information (EEIs) from tenant units aboard installations within the U.S. Upon receipt of information that a terrorist (or other) attack aboard is imminent, NCIS will immediately inform installation officials per effective MOU/MOA.]

(2) (U) [*Commentary:* Identify authority/agency authorized to act as a conduit for the two-way flow of threat information, to include, but not be limited to threat analysis, threat assessment, and threat condition. This authority issues guidance on the receipt, collection, and dissemination of threat information, and provides secure handling of sensitive information and communications.]

(3) (U) [*Commentary:* This annex provides intelligence related and security guidance during the pre-incident and incident response and crisis management phases of AT/FP operations.]

(a) (U) [*Commentary:* Pre-Incident Phase. Pre-incident planning, or the establishment of a "baseline force protection posture" is an on-going process. For the purposes of intelligence, this is a perishable commodity because activities, weather, demographics, etc. change from day-to-day. Many items, such as the policy for the protection and safeguarding of classified material, do not change appreciably. Pre-incident operations may be based on both perishable and consistent intelligence, and all units must apply intelligence information in order to make preparations for the worst-case scenario.]

(b) (U) [*Commentary:* Incident Response and Consequence Management Phase. Incident reactions include those actions that are implemented upon notification that a crisis is inevitable, and continue until the threat condition posture is relaxed. Actions executed during this phase build on those actions taken during the pre-incident phase, and strengthen the baseline force protection posture. It also includes recovery and reconstitution efforts that return the installation/unit to normal operations. These actions are situation dependent. Refer to annex C (Operations) for detailed tasking pertaining to various threats.]

(4) (U) [*Commentary:* This annex outlines methods and procedures for the receipt, collection, and dissemination of sensitive or classified AT/FP information during any or all of the three main phases of operations. This annex serves as a guide for tenant units to use to execute the coordination required for the collection and dissemination of threat information, and describes the unit/personnel responsibilities involved in handling such information.]

c. (U) Coordinating Instructions

(1) (U) [Available Intelligence Products]

(a) (U) ATAC Intelligence Summaries (Source)

(2) (U) [Distribution of intelligence products]

(3) (U) [Distribution of urgent intelligence (threat) information. This is information which could require the modification of security posture or that an actual terrorist attack is imminent. List distribution as required.]

(4) (U) [Level I threat briefing]

(5) (U) [Fusion cell]

(6) (U) [Open-source information from news media, hearings, publications, reference services, and the internet.]

(7) (U) [Criminal records]

(8) (U) [Local information derived from personnel, family members, and individuals.]

4. (U) ADMINISTRATION AND LOGISTICS. See annex D (Logistics).

5. (U) COMMAND AND SIGNAL

a. (U) Command. See annex A (Task Organization) and annex J (Command Relationships)

b. (U) Signal. See annex K (Communications and Information Systems)

Appendices:

A - Threat Assessment
B - Essential Elements of Information (EEIs)
C - Mapping, Charting, Geodesy

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) References: See appendix 4 (Publication Reference List) to annex V (References).

(U) Time Zone: Lima (Local).

1. (U) GENERAL

a. (U) Purpose. [To set forth the details for the conduct of emergency management and AT/FP operations.]

b. (U) Mission. See basic plan.

c. (U) Area of Operation.

d. (U) Situation. See basic plan.

2. (U) CONCEPT OF OPERATIONS.

a. (U) Pre-Incident Phase. See basic plan and appendices to this annex.

b. (U) Incident Response and Consequence Management. [*Commentary:* The focus of this phase is restoration of normal operations to include:

(1) (U) Restoration of primary, alternate, and tertiary evacuation routes.

(2) (U) Restoration of base support services.

(3) (U) Restoration of telecommunication services.

(4) (U) Debris and/or HAZMAT cleanup and disposal.

(5) (U) Resettlement of personnel evacuated from on-base housing.

(6) (U) Reporting and follow-up investigations.

(7) (U) Stand-down of crisis management personnel.]

3. (U) CONDUCT OF OPERATIONS

a. (U) Destructive Weather. See appendix 1.

b. (U) HAZMAT. See appendix 2.

c. (U) Antiterrorism. See appendix 3.

d. (U) Bomb Threats. See appendix 4.

e. (U) Hostage/Barricaded Suspect(s). See appendix 5.

f. (U) Weapons of Mass Destruction. See appendix 6.

g. (U) Physical Security. See appendix 7.

h. (U) Law Enforcement. See appendix 8.

i. (U) High Risk Personnel. See appendix 9.

j. (U) Information Operations. See appendix 10.

k. (U) Operation Security. See appendix 11.

l. (U) Emergency Operations Center Operations. See appendix 12.

m. (U) Special Security Areas. See appendix 13.

n. (U) Critical Infrastructure Protection. See appendix 14.

4. (U) OPERATIONAL CONSTRAINTS

a. (U) Fiscal.

b. (U) Emergency medical response capabilities.

c. (U) Chemical/biological response capabilities.

d. (U) Hazardous material incident response capabilities.

e. (U) Jurisdiction. Within the U.S., the FBI as the lead Federal agency for acts of terrorism and FEMA as the lead federal agency for consequence management. Overseas, the DOS is the lead agency for response to terrorism. See annex H (Legal) for amplifying guidance.

5. (U) LIMITING FACTORS

a. (U) [*Commentary:* List factors that will limit the effectiveness of the AT/FP program. Factors include, but are not limited to:

(1) (U) Proximity of non-federal property such as highways, roads, rail-lines, and private property.

(2) (U) Bisecting waterways that could provide clandestine access to facilities.

(3) (U) Terrain that could restrict communications and observation.]

6. CRISIS MANAGEMENT

a. (U) Crisis Management Team (CMT).

(1) (U) [*Commentary:* Provide subject matter expertise for advisory and coordination purposes.

(2) (U) Influence and manage the continuous flow of information.

(3) (U) Resolve the incident by employing all available resources while minimizing adverse affects of the incident.

(4) (U) Plan for and manage multiple and/or diversionary incidents.

(5) (U) Understand and deal with political, media, and public reaction requirements.

(6) (U) Be prepared to deal with a full spectrum of man-made and natural disasters that could occur on the base.

(7) (U) Develop courses of action.]

(8) (U) See annex J (Command Relationships).

b. (U) On-scene Commander (OSC): [*Commentary:* Define who will be the on-scene commander for what types of incidents.] The on-scene commander will:

(1) (U) Observe. [*Commentary:* Size up the area and report to dispatch:

(a) (U) Unit designation of first responders on-scene.

(b) (U) A brief description of the situation (e.g., building size, occupancy, multi-vehicle accident, etc.).

(c) (U) Obvious conditions (e.g., HAZMAT spill, multiple victims, traffic conditions, weather conditions, key terrain etc.)

(d) (U) Description of initial action(s) taken (e.g. establish perimeter, shut down traffic).

(e) (U) Obvious safety concerns (e.g. First responders are receiving hostile fire from the west, recommend follow-on units approach from the East).

(f) (U) Assumption, identification, and location of the Command Post.

(g) (U) Request or release resources as required.

(h) (U) Crowds, witnesses, and suspects.]

(2) (U) Identify contingencies:

(3) (U) Determine objectives: [*Commentary:* Decide what you want to do. Objectives are:

(a) (U) Measurable;

(b) (U) Used to monitor incident progress and establish priorities; and

(c) (U) Based on situation and contingencies - Define the problem and courses of action.]

(4) (U) Identify resources requirements.

(a) (U) [*Commentary:* What resources will be needed?

(b) (U) Do you have them?

(c) (U) Where will you get them?

(d) (U) How long will it take to get them?

(e) (U) Is assistance from other military or civilian agencies needed?

(f) (U) Are there any special requirements?]

(5) (U) Build an incident action plan and management structure.

(a) (U) [*Commentary:* Responsibilities - Who will do what?

(b) (U) On-scene command structure - Who will report to whom?

(c) (U) Coordination - How will different groups work together, and how will they communicate?]

(6) (U) Take action: [*Commentary:* Possible actions for incident stabilization may include:

(a) (U) Establish command.

(b) (U) Mobilize resources.

(c) (U) Set up a staging area.

(d) (U) Isolate the area. Establish inner & outer perimeter (as the situation dictates) and traffic control points.

(e) (U) Treat/assist injured.

(f) (U) Establish primary/alternate routes for egress/ingress/ evacuations.

(g) (U) Establish a resource staging area.

(h) (U) Issue warnings. The situation may dictate the issuance of safety warnings for responding forces and to prevent injury/damage to surrounding people and property.

(i) (U) Initiate an evacuation.

(j) (U) Establishing liaisons.

(k) (U) Pass the word (make notifications).

(l) (U) Establish safe contact with suspect.

(m) (U) Notify key personnel.

(n) (U) Deploy special units (tactically).

(o) (U) Debrief witnesses/suspects/key personnel.

(p) (U) Resolve Incident.

(q) (U) See annex J (Command Relationships).]

c. (U) Crisis Management Force (CMF).

(1) (U) [*Commentary:* Task organize to resolve the incident.

(2) (U) OSC actions apply.

(3) (U) See annex J (Command Relationships).]

d. (U) Emergency Operations Center (EOC). See appendix 12 (EOC Operations).

Appendices:

1 - Destructive Weather
2 - Hazardous Material
3 - Antiterrorism
4 - Bomb Threats
5 - Hostage/Barricaded Suspect(s)
6 - Weapons of Mass Destruction
7 - Physical Security
8 - Law Enforcement
9 - High Risk Personnel
10 - Information Operations
11 - Operational Security
12 - Emergency Operations Center Operations
13 - Special Security Areas
14 - Critical Infrastructure Protection

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 1 (DESTRUCTIVE WEATHER AND NATURAL DISASTERS) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

1. (U) SITUATION

a. (U) General. [*Commentary:* Destructive weather and/or natural or man-made disasters pose a threat at any time. It is the responsibility of the commander to adopt appropriate precautionary measures to mitigate the potentially calamitous effects of such disasters. Destructive weather or other natural or man-made disasters can strike quickly with little warning. Hasty, last minute preparations to persevere over these disasters are typically of little value. Therefore, a condition of readiness that allows for an instantaneous appropriate response in order to prevail over such disasters.]

b. (U) Assumptions

(1) (U) [*Commentary:* Efforts to limit the effects of various potentially destructive weather conditions and natural disasters must be continuous in order to minimize the harmful effects on mission capability and loss to human life and property.]

(2) (U) [*Commentary:* Emergency management capabilities are limited with respect to manning and equipment. Therefore, in order to satisfactorily prevail over the most devastating hazardous weather and other natural or man-made disasters, MOU/MOA must be established with external agencies to allow for cooperative use of local county, state, and Federal agencies' equipment and expertise.]

2. (U) CONCEPT OF OPERATIONS. [*Commentary:* Per the basic plan. Pre-incident operations include such tasks as conducting preventive hurricane measures during May, or preparing snow removal plans during November. Specific pre-incident, incident response and consequence management operations will be executed as set forth in tabs A, B, C, D and E.]

3. (U) EXECUTION. [*Commentary:* Destructive weather and natural disasters include, but are not limited to the following phenomena:

a. (U) Hurricanes, Tornadoes, Thunderstorms and Lightning, and High Wind Conditions. See TAB A.

b. (U) Flooding. See tab B.

c. (U) Blizzards/Heavy Snowfall. See tab C.

d. (U) Forest Fires. See tab D.

e. (U) Earthquakes. See tab E.]

4. (U) ADVISORIES AND CONDITIONS. [*Commentary:* Alert conditions are tailored to meet the requirements necessary for addressing severe weather or fire conditions. Appropriate conditions will be set as information is received. Examples of fire and weather information sources include: higher headquarters, the National Weather Service (NWS), or local organizations.]

a. (U) Weather advisories will be issued by the NWS or the local weather office. Specific destructive weather readiness conditions are listed in tabs A, B, and C.

b. (U) [Fire conditions are listed in TAB D.]

5. (U) TASKS. [*Commentary:* During the execution of all tasks coordinate as appropriate. List organization and specific tasks assigned for pre-incident and incident response and consequence management phases as necessary.] Any assistance to civilian agencies will be done in accordance with annex J (Command Relationships).

6. (U) NOTIFICATIONS. Will be conducted in accordance with annex K (Communications and Information Systems) and annex V (References).

Tabs:

A - Hurricanes, Tornadoes, Thunderstorms and Lightning, and High Wind Conditions
B - Flooding
C - Blizzards/Heavy Snowfall
D - Forest Fires
E - Earthquakes

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 2 (HAZMAT) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) References: (a) [Installation Hazardous Material Plan]

(U) Time Zone: Lima (Local)

1. (U) GENERAL

a. (U) [*Commentary:* HAZMAT incidents ranging in scope from minor spills to catastrophic incidents involving the rupture of fuel tanks or chemical spills originating after a train derailment will occur from time to time. This appendix is used synchronize existing HAZMAT procedures with the AT/FP plan.]

b. (U) Assumptions.

(1) (U) Reference (a) is the primary base document for resolving HAZMAT incidents.

(2) (U) HAZMAT material i.e., chemical, radiological, and biological agents will be addressed in appendix 6 (Weapons of Mass Destruction (WMD)) to annex C (Operations).

2. (U) CONCEPT OF OPERATIONS. Per the basic plan.

3. (U) TASKS. [List organization and specific tasks assigned as necessary.]

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) References: (a) MCO 3302.1D
(b) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93
(c) SECNAVINST 3300.2A (NOTAL) of 21 Mar 01
(d) DOD Directive 2000.16 (NOTAL) of 14 Jun 01

1. (U) SITUATION

a. (U) General. [*Commentary:* AT measures include those defensive measures used to reduce the vulnerability of individuals and property to terrorism, to include limited response and containment by local military forces. AT measures seek to diminish the likelihood that DOD affiliated personnel, facilities, and property will be attacked, and to mitigate the effects of such attacks should they occur. AT efforts build on the foundation of physical security, crime prevention, industrial health, safety, and hygiene programs and military and civil construction programs. These efforts are designed to reduce a broad range of physical dangers faced by DOD affiliated personnel. The terrorist threat is a significant danger that many DOD force protection initiatives can mitigate. This appendix augments the information contained in the references, which are DOD and Naval directives, orders and instructions pertaining to AT.]

b. (U) Enemy Forces. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Assumptions. See basic plan.

2. (U) MISSION. [*Commentary:* On a continuing basis implement active and passive security measures in order to deter terrorist incidents, employ counter measures, mitigate the effects of a terrorist attack, and recover from a terrorist incident. On order implement the Force Protection Conditions (FPCONS) and random antiterrorism measures (RAM) contained herein.]

3. (U) EXECUTION

a. (U) Commander's Intent. See the Basic Plan. [*Commentary:* The commanders intent is to maintain the ability to smoothly transition from a normal security posture to an appropriate advanced security posture in which base-wide security efforts are integrated and synchronized, there is a heightened individual/unit awareness toward antiterrorism, and all prudent passive/active countermeasures are employed to protect the lives of Marines, Sailors, civilians, and their families as well as facilities and government property.]

b. (U) Concept of Operations

(1) (U) Pre-Incident Phase. [*Commentary:* This phase consists of an active PSC and AT/FP working group, ongoing AT training, regularly exercising procedures and personnel, conducting physical security and crime prevention surveys, identifying and correcting physical security deficiencies, and implementing basic RAM. This phase transitions to the incident response and consequence management phase when the FPCON level increases above FPCON Normal.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary;* This phase involves the implementation of higher FPCONs and continuing RAM measures due to the escalation from FPCON Normal. RAM may be implemented at any time at the discretion of the commander. This phase includes those actions taken to return to pre-incident conditions. During this phase recommended improvements to the AT/FP plan should be considered for adoption. This phase is complete upon returning to FPCON NORMAL, and operations, facilities, and missions are returned to their pre-incident state.]

c. (U) Coordinating Instructions. [*Commentary:* All personnel must be familiar with the information set forth in the following tabs, and be prepared to execute duties as appropriate.]

(1) (U) Tab A (Mission Essential Vulnerable Areas (MEVA) identifies the mission essential vulnerable areas.

(2) (U) Tab B (Potential Terrorist Targets) identifies locations, other than MEVA, that may be targeted by terrorists for attack.

(3) (U) Tab C (Threat Levels) is an overview on how terrorist threat levels are determined and can be used as a planning tool.

(4) (U) Tab D (Force Protection Conditions (FPCONS)) are levels of readiness that outline specific tasks that must be executed to prepare for terrorist attack(s).

(5) (U) Tab E (Random Antiterrorism Measures (RAM)) contains procedures for implementing RAM.

d. (U) Training. AT/FP training requirements are outlined in annex O (Training).

4. (U) ADMINISTRATION AND LOGISTICS. See annexes D (Logistics), E (Fiscal), and O (Personnel).

5. (U) COMMAND AND SIGNAL. See annexes A (Task Organization), K (Communications and Information Systems), and J (Command Relationships).

Tabs:

A - Mission Essential Vulnerable Areas (MEVA)
B - Potential Terrorist Targets
C - Threat Levels
D – Force Protection Conditions (FPCONS)
E - Random Antiterrorism Measures (RAM)

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

TAB A (MISSION ESSENTIAL VULNERABLE AREA (MEVA)) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

1. (U) [*Commentary:* Mission essential vulnerable areas (MEVAs) are determined by combining the vulnerability assessment and the threat assessment together and analyzing them through a criticality assessment. The criticality assessment identifies assets that are vulnerable (vulnerability assessment) to a terrorist threat (terrorist threat assessment) and critical to mission accomplishment (criticality assessment). The assets that match the above criteria are proposed as MEVA and recommend to the PSC, AT/FP working group, or the commander for approval.]

2. (U) [*Commentary:* The MSHARPP target analysis tool is one method that can be used to assess the facilities of an installation when calculating the vulnerability. "CARVER" and "DSHARPP" are other systems that can be used for in the calculation of vulnerabilities. MSHARPP is thoroughly discussed in enclosure (2). It is recognized as a valuable tool for security planning and potential high value target determination by many military installations.]

a. (U) [*Commentary:* Using MSHARPP, the AT/FP working group determines values for critical facilities. The values are combined in a decision matrix to identify the facilities most likely disrupt the mission if subject to terrorist attack. These facilities are then designated as the installation/unit's MEVA.]

b. (U) [*Commentary:* The MEVA, combined with the potential threats that have been identified, will be used to determine actions for improving the AT/FP posture for all FPCONs.]

3. (U) [*Commentary:* While MSHARPP, DSHARPP, CARVER or some other methodology may be used, it is important that a systematic approach to developing MEVA is applied.]

4. (U) [*Commentary:* The AT/FP working group will reevaluate MEVA annually and amend its recommendations accordingly.]

5. (U) Mission essential vulnerable areas are designated as follows:

a. (U) [List MEVAs]

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

TAB B (POTENTIAL TERRORIST TARGETS) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) References: (a) [Criticality Assessment]

1. (U) [*Commentary:* Some facilities analyzed will not have a high enough MSHARPP rating combined with criticality to qualify them as MEVA. However, based on the potential for loss of life and damage if attacked, they merit consideration during security planning.]

a. (U) Per reference (a), the top terrorist targets on are outlined below:

(1) (U) [List of facilities.]

b. (U) Additional potential targets that merit consideration during security planning are outlined below:

(1) (U) [List of facilities]

2. (U) The AT/FP working group will review this list annually.

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

TAB C (THREAT LEVELS) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

1. (U) [*Commentary:* Terrorism threat levels are the intelligence community's system for articulating and categorizing the terrorist threat worldwide. They represent a DOD-developed methodology for assessing the terrorist threat to personnel, material and interests based on a combination of the threat analysis factors. The terrorism threat level is determined for a particular area based on the presence or absence of these threat assessment factors:

a. (U) Operational capability. The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.

b. (U) Intentions. Actions indicative of preparations for specific terrorist operations.

c. (U) Activity. Recently demonstrated anti-U.S. activity, or stated or assessed intent to conduct such activity.

d. (U) Operating environment. The circumstances of the country under consideration (HN security, legal system, terrain features, etc.).]

2. (U) [*Commentary:* The DOD terrorist threat analysis community has developed a notional system used to describe the country specific results of terrorist threat analysis methodology. Within the U.S., commanders may assign local threat levels in accordance with the DOD terrorist threat level notional system. NCIS is the primary agency for managing and analyzing threat information. Accordingly, NCIS will advise when changes in local threat condition/security postures may be prudent.]

3. (U) [*Commentary:* Terrorism threat levels are determined from a combination of the above threat assessment factors. On 1 October 2000 the DIA changed the previous five-level system into one that has four levels:]

a. (U) High. An anti-U.S. terrorist group is operationally active and uses large casualty producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

b. (U) Significant. An anti-U.S. terrorist group is operationally active and attacks personnel as their preferred method of operation, or a group uses large casualty producing attacks as their preferred method and has limited operational activity. The operating environment is neutral.

c. (U) Moderate. Terrorist groups are present but there is no indication of anti-U.S. activity. The operating environment favors the HN or U.S.

d. (U) Low. No terrorist group is detected or the group activity is non-threatening.

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

TAB D (FORCE PROTECTION CONDITIONS) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

1. (U) [*Commentary:* The FPCON system describes the progressive level of protective measures that are implemented by all DOD components in response to terrorist threats. The FPCON system complements the national level intelligence community assessment of terrorist intentions and capabilities.]

2. (U) [*Commentary:* The FPCON level can be established by commanders at any level, and subordinate commanders can establish a higher FPCON if local conditions warrant so doing.]

3. (U) FPCONS. [*Commentary:* The decision to execute FPCON levels and associated security measures should be based on multiple factors that may include, but are not limited to:

a. (U) Intelligence. See annex B (Intelligence).

a. (U) Terrorist threat levels. See tab C (Threat Levels).

b. (U) Target vulnerability. See tab A (MEVA).

c. (U) Criticality of assets.

d. (U) Security resources availability.

e. (U) Operational and morale impact of security measures.

f. (U) Damage control and recovery procedures.

g. (U) International relations.

h. (U) Planned U.S. Government actions that may serve as a catalyst for a terrorist response.]

4. (U) [*Commentary:* RAM is the implementation of multiple security measures in a random fashion. When activated, RAMs provide a "different look" at security procedures in effect, to deny the terrorist surveillance team the opportunity to accurately predict security actions. The plan is used throughout all FPCONs and consists of using selected security measures from higher FPCONs, as well as other measures not associated with FPCONs. Using a variety of additional security measures in a normal security posture prevents overuse of security forces, as would be the case if a higher FPCON were maintained for an extended period of time. RAMs are implemented in a strictly random manner, never using a set time frame or location for a given measure. Additional information regarding RAM are identified in tab E (Random Antiterrorism Measures).]

5. (U) [*Commentary:* The RAM and FPCON measures should be followed except when exceptional circumstances dictate otherwise. The FPCON measures listed after each FPCON level are listed as an enclosure 1 (FPCON Measures Integration Action Sets) to this tab.] FPCON levels are defined as follows:

a. (U) FPCON Normal. FPCON NORMAL applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

b. (U) FPCON Alpha. FPCON ALPHA applies when there is an increased general threat of possible activity against personnel or facilities, the

nature and terrorist extent of which are unpredictable. *ALPHA measures must be capable of being maintained indefinitely.* (FPCON Measures 1-10).

c. (U) FPCON Bravo. FPCON BRAVO applies when an increased or more predictable threat of terrorist activity exists. *Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.* (FPCON Measures 11-29).

d. (U) FPCON Charlie. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. *Implementation CHARLIE measures will create hardship, and affect the activities of the unit and its personnel.* (FPCON Measures 30-40)

e. (U) FPCON Delta. 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 or person is imminent. *Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.* (FPCON Measures 41-51)

Enclosures:

1 - FPCON Integrated Actions Sets

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ENCLOSURE 1 (FPCON INTEGRATED ACTION SETS) TO TAB D (FORCE PROTECTION CONDITIONS) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-99 (U)

(U) FPCON INTEGRATED ACTION SETS

Force Protection Condition	Measure	Action Set	Coordination
ALPHA	Consult with local authorities on the threat and mutual antiterrorism measures	The installation senior intelligence officer will use all available means to determine the operational capability, intentions, activity, and operating environment of terrorist groups [illegible] the threat to the installation. If capabilities are listed, the threat assessment will likely be classified. The classified threat assessment will be maintained at X office by X. Dissemination will be based on a strict need to know basis, with appropriate security clearances.	Interface with local law enforcement agencies. Conduct interagency coordination to obtain terrorist capabilities and intentions. Coordinate with diplomatic missions, as applicable. Coordinate with MI and security personnel to establish the appropriate security controls and need to know.

FPCON Alpha	Installation Actions
Definition: A general threat of possible terrorist activity against personnel and installations exists, the nature and extent of which is unpredictable. Circumstances do not justify full implementation of FPCON BRAVO measures; however, it	Convene FPWG and develop courses of actions. This planning session should consider implementation of higher FPCONs. Further, sequential implementation of FPCONs cannot be assumed.

may be necessary to implement certain selected measures from higher FPCON'S. This decision may be based on intelligence received, or the need to provide a specific deterrent. The measures in FPCON ALPHA must be capable of being maintained for an indefinite period of time.	Complete all required actions for previous FPCONs. Report actions complete to the EOC. Be prepared to implement higher FPCONs.
Measure 1: Remind all personnel, including family members, at regular intervals to: (1) Be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. (2) Be alert for unidentified vehicles on, or in the vicinity of U.S. installations, units, or facilities. (3) Be alert for abandoned parcels, suitcases, potential location for explosive devices or any unusual activity. Combatant Commander, Service, or other mandated measures: Brief all personnel on the current threat, and those measures enacted to increase security. Remind all duty personnel to be especially alert for suspicious or unusual activity, strangers, or unidentified vehicles. Combatant Commander, Service, or other mandated measures: Conduct unit level terrorism awareness training.	PAO: Advertise in the installation paper that all personnel should be alert and inquisitive about strangers. Be aware of items that don't belong in the area and be alert to abandoned parcels. This information needs to be disseminated to all personnel who work or reside on the Installation. All Units: Regularly brief all personnel on the current terrorism threat as part of the troop information program. EOD: Conduct suspicious packages/IED training for all mail handlers. Unit AT/FP Officers: Advise FPWG that all personnel have received an antiterrorism brief.

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

TAB E (RANDOM ANTITERRORISM MEASURES) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

1. (U) Random Antiterrorism Measures (RAM). [*Commentary:* RAM are used to enhance local FPCON measures. The implementation of RAM serve three purposes:

a. (U) RAM can be used as a tool to determine the productivity costs for individual antiterrorism measures. A RAM program can help identify which measures that they are capable of being sustained and those measures that may be more stressful on personnel and material resources.

b. (U) RAM provide security forces with training and stimulation, making the job of providing security more challenging, interesting and exciting. RAM programs increase security because the security forces are more attentive to their regular assignments.

c. (U) RAM change the security atmosphere. Such programs, when implemented in a truly random fashion, alter the external appearance or security "signature" to would-be terrorists and their supporters who may be providing surveillance assistance. RAM confuse the terrorist's assessment of security posture. RAM causes terrorists wonder, "do they know we are here, and have we been compromised?" Terrorists must also consider the impact that the base security practices may have on their ability to achieve their operational goals. The impact of RAM programs on terrorists is difficult to measure, but such programs are clearly capable of introducing uncertainty for planners and organizers of terrorist attacks.]

2. (U) [*Commentary:* RAM are procedures that are normally executed at specific FPCON levels. The establishment of RAM consists of using selected security measures from higher FPCONs, as well as other measures not associated with FPCONs to supplement the basic FPCON measures already in place.]

3. (U) [*Commentary:* At any given FPCON level, implementing certain measures from higher FPCONs conveys an impression of increased vigilance and awareness to observers. Conducting random searches of vehicles, increasing foot patrols, and removing trash cans and waste receptacles from around buildings demonstrate that security forces are aware of the possibility of a terrorist intrusion and are taking steps to minimize that possibility.]

4. (U) [*Commentary:* The commander will determine when, where, and what RAM measures will be implemented. RAM will be executed in the action sets prescribed in enclosure 1 (RAM Action Set Matrix). Area commanders, unit commanders, division directors, and building managers are encouraged to autonomously implement their own RAM action sets.]

5. (U) Tasks. [*Commentary:* List organization and specific tasks as assigned.]

6. (U) Coordinating Instructions

a. (U) [*Commentary:* Coordinating instructions should include scheduling and implementation instructions of RAM as well as the duration of RAM action sets.

b. (U) Autonomously implement unit/building level RAM as deemed prudent.

c. (U) Provide feedback on the effectiveness of the RAM.]

7. (U) Administration. [*Commentary:* RAM will be assessed to determine effectiveness, cost of action, feasibility of long-term implementation, and coordination necessary (i.e. coordination to ensure smooth traffic flow and safe conditions.]

Enclosures:

1 - RAM Action Sets

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ENCLOSURE 1 (RAM ACTION SETS) TO TAB E (RANDOM ANTITERRORISM MEASURES) TO APPENDIX 3 (ANTITERRORISM) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) RAM MATRIX[1]

THREATCON MEASURES	0001 - 0400	0401 - 0800	0801 - 1200	1201 - 1600	1601 - 2000	2001 - 0000
Alpha						
1						
2						
3						
4[2]						
5						
6						
7						
8						
9						
10						
Bravo						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
Charlie						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
Delta						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						

[1] (U) Refer to Enclosure 1 (FPCON Integrated Action Sets) to Tab D (Force Protection Conditions) to Appendix 3 (Antiterrorism) for specific duties.
[2] (U) When conducted during peak traffic hours, implement decal monitoring only. Discontinue if traffic congestion causes an unsafe condition. Continue when congestion has abated.

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 4 (BOMB THREAT PROCEDURES) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) References: (a) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

(U) Time Zone: Romeo (Local)

1. (U) SITUATION

a. (U) General

(1) (U) [*Commentary:* Briefly describe the employment techniques and design concepts that make homemade explosive devices (Improvised Explosive Devices or IEDs) a preferred method for carrying out attacks against DOD personnel, facilities, and assets.]

b. (U) Information

(1) (U) [*Commentary:* Provide any definitions or amplifying information that helps to explain the purpose, methodology or construct of this appendix.]

c. (U) Enemy Forces. See basic plan.

d. (U) Friendly Forces. See basic plan.

e. (U) Assumptions

(1) (U) [*Commentary:* Describe the basic assumptions that have been made in the planning phase for this appendix.]

2. (U) MISSION. [*Commentary:* Generally, the mission for this appendix can be described as those activities required to prepare to prevent, deter, and/or mitigate the potential loss of life, destruction to government/personnel property, and disruption to normal operations caused by the effects of threatened or actual bombings aboard the installation.]

3. (U) EXECUTION

a. (U) Commander's Intent. Preservation of human life is paramount! [*Commentary:* Describe the commander's intent. Generally, this will be to prevent, deter, and mitigate the potentially harmful effects of threatened or actual bombing incidents through individual/unit awareness and training, integration of this appendix with other portions of the AT/FP plan, and sound crisis response/consequence management planning and procedures. WMD have the potential to produce catastrophic damage and require substantial state and Federal assistance.]

b. (U) Concept of Operations

(1) (U) Pre-Incident Phase. [*Commentary:* Detail the plans, procedures and training needed to protect against and search for explosive devices. Require force protection principals to be applied to new construction projects, and measures to mitigate blast effects to be widely implemented. This phase will end when there is a bomb threat or actual detonation.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary:* Describe the crisis response and consequence management

procedures to resolve the incident. This phase is complete when the incident site is returned to normal operations. Activities include, collecting/preserving evidence, site cleanup, and compilation of lessons learned.]

c. (U) Tasks

(1) (U) [*Commentary:* Specify tasks for each activity expected to participate in bomb threat response, such as: Command Duty Officer, Security Battalion, Fire Service or ARFF Crews, On-Scene Commander, Installation Operations Division, EOD Team, Installation Facilities Division, Medical Clinic, NCIS, and other personnel.]

d. (U) Coordinating Instructions

(1) (U) [*Commentary:* Specify coordinating instructions such as: requiring all Mission Essential Vulnerable Areas (MEVA) to receive an annual physical security surveys conducted by a physical security specialist. See appendices 3 (Antiterrorism) and 7 (Physical Security) to annex C (Operations).]

(2) (U) [*Commentary:* Unit bomb threat plans criteria]

(3) (U) [*Commentary:* Requirements for periodic practice evacuation and search drills under the supervision of the commanding officer and unit ATO.]

(4) (U) [*Commentary:* Requirement to ensure security battalion and operation division are notified prior to conduct of drills or exercises associated with this appendix.]

(5) (U) [*Commentary:* Specify procedures for mail handlers and other worker who routinely handle/receive mail or package deliveries shall be trained to recognize suspected IEDs and understand the procedures for handling them.]

(6) (U) [*Commentary:* Encourage heightened awareness for personnel to be suspicious of unidentified personnel and encourage personnel to query those persons to learn their intention.]

(7) (U) [*Commentary:* Encourage personnel to report anything that seems “out of the ordinary”.]

4. (U) ADMINISTRATION AND LOGISTICS. See annexes D (Logistics), E (Fiscal), and P (Personnel Services).

5. (U) COMMAND AND SIGNAL.

a. (U) Command. [*Commentary:* Specify command and control structure. Typically, the provost marshal or military police personnel will be in control of the scene unless NCIS or the FBI has assumed jurisdiction.]

b. (U) Signal. [*Commentary:* Methods of communications such as: Land-lines, runners, or hand and arm signals.]

TABS:

A – Bomb Threat Mitigation Planning Guidance

B – Evacuation Procedures
C - Search Procedures
D – Telephonic and Mail Bomb Data Card

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 6 (WEAPONS OF MASS DESTRUCTION (WMD)) TO ANNEX C (OPERATIONS) TO AT/FPP 02 (U)

(U) Ref: (a) Occupational Safety & Health Administration 29 CFR 1910.120
(b) Environmental Protection Agency 40 CFR 311
(c) DOD Instruction 2000.16 (NOTAL) of 14 Jun 01
(d) MCO 3302.1D
(e) Presidential Decision Directive 39
(f) NFPA, National Fire Protection Agency
(g) FM 3-9
(h) Chemical Agent Data Sheets, V.1, Dec. 1974, EO-SR-74001
(i) Merck Index
(j) Material Safety Data Sheets (MSDS)
(k) CHPPM Detailed Fact Sheets

1. (U) SITUATION

a. (U) General

(1) (U) [*Commentary:* Briefly describe the threat of the use of WMD by terrorists against US personnel and assets and why positive, proactive measures should be in place to help lessen the effects of a WMD attack should one occur.

b. (U) Enemy. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Assumptions

(1) [*Commentary:* Describe the basic assumptions that have been made in the planning phase for this appendix.]

2. (U) MISSION. [*Commentary:* The mission can generally be described as being 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 once they occur.]

3. (U) EXECUTION

a. (U) Commander's Intent. [*Commentary:* Describe the commander's intent. Generally this will be to maintain the capability to respond to a WMD incident and develop comprehensive plans to marshal base, DOD, state, Federal and civil resources to assist in the response. The cornerstone of this appendix lies in the ability to conduct proactive measures prior to a WMD incident. Plans should specifically address how state, Federal, and civilian resources will be incorporated into the plan. Measures that can mitigate the effects of a WMD attack will be implemented where prudent. Endstate: develop viable plans and train and equip personnel to properly execute their responsibilities. Periodically exercise the plan.]

b. (U) Concept of Operation

(1) (U) Pre-incident phase:

(a) (U) [*Commentary:* Delineate actions taken during this phase such as: coordination with internal and external agencies, military construction, training, education and acquisition of necessary equipment. This phase ends when a WMD attack occurs.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary:* Describe duties/actions of 1st responders such as: performance of consequence management actions (containing and controlling the incident site, rescuing survivors, performing hasty decontamination, triage and evacuation, and identifying, if possible, the agent). After the immediate threat has been abated and surviving victims have been evacuated for treatment, the incident site must be searched for evidentiary material. 1st responders may require post-incident psychological counseling. Response agencies should conduct a comprehensive review of actions taken in order to improve procedures. This phase is complete when the area is restored to normal operations.]

c. (U) Tasks

(1) (U) [*Commentary:* Describe and assign tasks for all units, offices and positions affected by or responding to the WMD incident. This includes but is not limited to operations, 1st response (assignment of on-scene commander), medical, security, facilities, logistics, PAO, and communications.]

d. (U) (U) Coordinating Instructions

(1) (U) [*Commentary:* Incident coordination including delineate and prioritize consequence management actions for incident responders, decontamination, identification of agents used during a chemical attack, removal and transportation of victims to area medical facilities with the ability to treat nuclear, biological or chemical (NBC) contaminated victims, and development of MOU/MOA that support this appendix.]

4. (U) ADMINISTRATION AND LOGISTICS

a. (U) Administration. See annex P (Personnel Services).

b. (U) Logistics. See annexes D (Logistics) and E (Fiscal).

5. (U) COMMAND AND SIGNAL

a. (U) Command. See annexes A (Task Organization) and J (Command Relationships).

b. (U) Signal. See annex K (Communications and Information Systems).

c. (U) Command Post Location:

(1) (U) Base: See basic plan.

(2) (U) On-scene: TBD.

Tabs:

A - Potential NBC Agents

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 7 (PHYSICAL SECURITY) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) Ref: (a) MCO P5530.14
(b) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

1. (U) SITUATION

a. (U) General. [*Commentary:* An active installation physical security program is the bedrock on which many other security programs are rested. The physical security program is designed to prevent or mitigate the potentially deleterious effects of criminal activity. This appendix establishes physical security guidance to support this plan.]

b. (U) Enemy. See annex B (Intelligence).

c. (U) Friendly. See annexes A (Task Organization) and J (Command Relationships).

d. (U) Assumptions. See basic plan.

2. (U) MISSION. [*Commentary:* Describe how the installation/unit implements active and passive physical security measures presenting a security profile commensurate with the threat. Each AT/FP plan must contain a physical security annex or appendix.]

3. (U) EXECUTION.

a. (U) Commander's Intent. [*Commentary:* Describe the commander's intent to implement aggressive active and passive security measures to elevate the installation/unit security posture commensurate with the threat.]

b. (U) Concept of Operation

(1) (U) Pre-Incident. [*Commentary:* Describe how physical security measures are designed to establish a baseline physical security posture. These measures will include physical security surveys, elevating individual awareness, developing and practicing good security procedures, considering AT/FP concerns into new building design, training security forces, implementing RAM, and varying security routines. This phase is complete when a terrorist event or criminal activity has occurred.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase describes steps taken to immediately correct an identified security deficiency or implement security measures, commensurate with the threat, which reduce the likelihood of criminal activity. Deficiencies shall be examined, security measures developed to lessen the likelihood the deficiency will occur again. This phase is complete when lessons learned have been applied to correct the deficiency.]

c. (U) Tasks

(1) (U) [*Commentary:* Describe tasks for the installation PSC and the AT/FP working group.]

d. (U) [*Commentary:* Additional issues that may be included in the physical security plan are: perimeter controls, access controls, identification systems, visitor control, commercial deliveries, building access control and physical security, lighting, physical security evaluations,

building design and military construction considerations, barrier plan, containment plan, guidance on unit movement and transportation, loss reporting, and the use of electronic security systems.]

Tabs:

A - Installation Barrier Plan
B - Installation Containment Plan
C – Crisis/Consequence Management Plan

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 8 (LAW ENFORCEMENT) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) Ref: (a) Title 18, U.S.C.
(b) Uniform Code of Military Justice (Article 7)
(c) R.C.M. 302, Manual for Courts Martial
(d) MCO P5580.2A

1. (U) SITUATION

a. (U) General. [*Commentary:* Law enforcement plays a crucial role in the Marine Corps AT/FP program. Military police provide security against a broad spectrum of potential threats. By serving as a visible deterrent, military police are the initial response force to most security related incidents, and have the responsibility for conducting criminal investigations of any serious crimes. Military police also serve as a valuable resource for the collection and dissemination of criminal intelligence.]

b. (U) Enemy Forces. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Attachments/Detachments. See annex A (Task Organization) and annex J (Command Relationships).

e. (U) Assumptions

(1) (U) [*Commentary:* Describe assumptions used in the development of this annex.]

2. (U) MISSION. [*Commentary:* Detail a brief overview of the law enforcement mission such as law enforcement and criminal investigative support in order to protect lives, protect property and enforce regulations. Security forces provide initial response and elements of a CMF for incidents.]

3. (U) EXECUTION

a. (U) Commander's Intent. [*Commentary:* Describe the commander’s intent to support law enforcement operations; apply proactive, creative law enforcement techniques to situational criminal problems; and complete thorough, professional criminal investigations.]

b. (U) Concept of Operations

(1) (U) Pre-Incident Phase. [*Commentary:* This phase consists of ongoing law enforcement and physical security training, routine military police patrols and performing crime prevention surveys. This phase is complete when an infraction of the law has been observed or reported.]

(2) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase involves the initial response to the complaint or observance, contact with the parties involved, investigation, subsequent actions taken by the military police, and actions taken to reconstitute after the incident occurs including victim and witness assistance and the repair or reimbursement of damages. This phase is complete upon reimplementing pre-incident phase.]

c. (U) Tasks

(1) (U) [*Commentary:* Describe and assign tasks to the security force, NCISRA, and subordinate/tenant commanders.]

d. (U) Coordinating Instructions

(1) (U) [*Commentary:* Provide coordinating instructions as necessary.]

4. (U) ADMINISTRATION AND LOGISTICS. See annexes D (Logistics), E (Fiscal), and P (Personnel Services).

5. (U) COMMAND AND SIGNAL

a. (U) Signal. [*Commentary:* Provost marshal instructions will dictate all military police communication procedures. Annex K (Communications and Information Systems) covers communications to implement this plan.]

b. (U) Command

(1) (U) [*Commentary:* The installation provost marshal shall maintain operational command of the installation CMF. The line of succession is typically: Provost marshal, deputy provost marshal, operations officer, and watch commander as appropriate.]

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 9 (HIGH RISK PERSONNEL (HRP)) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) Ref: (a) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

1. (U) SITUATION

a. (U) General. [*Commentary:* The rank, position, and/or political importance of some DOD personnel, U.S. and foreign dignitaries, make them and their families potential targets of criminal activity. It is imperative that those persons, designated as high-risk personnel (HRP), receive the personnel protection commensurate with their position and the existing threat level. Security Battalion, assisted by NCIS, will provide/coordinate HRP protective services.]

b. (U) Enemy Forces. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Attachments/Detachments. [*Commentary:* To be task organized as required by the mission.]

e. (U) Assumptions. [*Commentary:* Most political and foreign dignitaries will travel with a security element that will provide close in personal protection.]

2. (U) MISSION. [*Commentary:* Typical mission will be to implement security measures in order to reduce threats directed against HRP assigned to or visiting the base.]

3. (U) EXECUTION

a. (U) Commander's Intent. [*Commentary:* Detail the commander's directive to detect and reduce threats directed at HRP and their families.]

b. (U) Concept of Operations

(1) (U) [*Commentary:* Assign primary agency to perform personal security detachment (PSD) services and describe coordination with NCISRA, PSDs, and the United States Secret Service as necessary.]

(2) (U) [*Commentary:* Discuss the two categories of HRP: permanently assigned or visiting.]

(3) (U) Pre-Incident Phase. [*Commentary:* Describe ongoing risk reduction actions taken to improve the personal security of HRP. This phase is complete when the HRP has been targeted or attacked.]

(4) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase involves the execution of the PSD or the targeting and or attack upon the HRP or their family. Additional security measures will be implemented based on the threat and actions taken to reconstitute after the incident. This phase will include compiling after action data, implementing compensatory security measures, and implementing measures to reinstitute the pre-incident phase.]

(6) (U) [*Commentary:* The Office of the Secretary of Defense (OSD) is the primary agency for coordinating U.S. dignitary visits. This office will advise of pending visits.]

(10) (U) [*Commentary:* The Foreign Disclosure Office, HQMC is the primary agency for coordinating foreign dignitary visits. (DSN 227-3608). This office will advise of pending visits and determine the security clearance of the visitor(s).

c. (U) Tasks

(1) (U) [*Commentary:* Define tasks for operations, security, NCIS, PAO, Aide-de-Camps, drivers, PSDs, and associated tenants and activities.]

d. (U) Coordinating Instructions

(1) (U) [*Commentary:* Assign coordinating instructions as necessary. Consider developing coordinating instructions that vary dependant upon FPCONs, and site-specific or specialized training.]

4. (U) ADMINISTRATION AND LOGISTICS. See annex D (Logistics).

5. (U) COMMAND AND SIGNAL

a. (U) Signal. [*Commentary:* Provost marshal instructions will dictate all communication procedures during the mission.]

b. (U) Command

(1) (U) [*Commentary:* Describe the relationship between security forces, PSDs and the United States Secret Service.]

Tabs:

A - High Risk Billets

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 13 (SPECIAL SECURITY AREAS) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) Ref: (a) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

1. (U) SITUATION

a. (U) General. [*Commentary:* Special security areas are those areas normally contained within the perimeter of an installation or a unit's area of responsibility that because of the nature of the operations conducted require additional security measures under normal conditions. Examples of these areas are: airfield security, port security, embarkation/arrival areas, brigs, and buildings that contain special assets. Special security areas will often have their own dedicated security force maintained by the commander of the special security area.]

b. (U) Enemy Forces. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Attachments/Detachments. [*Commentary:* To be task organized as required by the mission.]

e. (U) Assumptions. [*Commentary:* Security at special security areas is generally maintained at a higher level than the surrounding area, nevertheless, circumstances may arise that require a heightened security posture. Security is typically provided by a tenant commander.]

2. (U) MISSION. [*Commentary:* Typical mission description would be to provide additional security assets to supplement special security area dedicated security forces as necessary, or to provide first response assets as needed to special security areas.]

3. (U) EXECUTION

a. (U) Commander's Intent. [*Commentary:* Detail the commander's directive to detect and reduce threats directed at special security areas.]

b. (U) Concept of Operations

(3) (U) Pre-Incident Phase. [*Commentary:* Describe ongoing risk reduction actions taken to improve special security area security and coordination between tenant and installation commands as necessary. This phase is complete when an incident occurs in the Special Security Area.]

(4) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase involves incident response actions taken during an incident and consequence management actions taken to reconstitute after incident response. It includes compiling after action data, implementing compensatory security measures, and implementing measures to reinstitute the pre-incident phase.]

c. (U) Tasks

(1) (U) [Define tasks.]

d. (U) Coordinating Instructions

(1) (U) [*Commentary:* Assign coordinating instructions as necessary (for instance how would the fire department gain entry to the airfield if responding to a structural fire). Consider developing coordinating instructions that vary dependant upon Force Protection Conditions, and site-specific or specialized training.]

(2) (U) [*Commentary:* Describe any MOA/MOUs that exist that would provide additional assets to the facility operator during an incident.]

(3) (U) [*Commentary:* If the special security area has its own AT/FP plan, it can be attached to this appendix as a supplement.]

(4) (U) [*Commentary:* A representative of the special security area should be on the installation/unit physical security council for coordination.]

4. (U) ADMINISTRATION AND LOGISTICS. See annex D (Logistics).

5. (U) COMMAND AND SIGNAL

a. (U) Signal. [*Commentary:* Describe the alert system to be used and how it will be activated.]

b. (U) Command

(1) (U) [*Commentary:* Describe the relationship between the special security area and the overarching installation/unit.] See annex J (Command Relationships).

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

APPENDIX 14 (CRITICAL INFRASTRUCTURE PROTECTION (CIP)) TO ANNEX C (OPERATIONS) TO AT/FPP-02 (U)

(U) Ref: (a) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

1. (U) SITUATION

a. (U) General. [*Commentary:* Typically, each unit or installation will have internal or external infrastructures that are critical to mission accomplishment. Examples include power grids, wastewater plants, drinking water supply, natural gas or petroleum product pipelines and many others. Three points make critical infrastructure different than most issues that face the commander. First, is that these infrastructures may or may not be located on government property; second, the infrastructure will often be owned by a third party; and third, critical infrastructures, under the right circumstances, could become a means of attack against the installation or unit.]

b. (U) Enemy Forces. See annex B (Intelligence).

c. (U) Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. (U) Attachments/Detachments. [*Commentary:* To be task organized as required by the mission.]

e. (U) Assumptions. [*Commentary:* Mission accomplishment is highly dependent upon continued functioning of critical infrastructures.]

2. (U) MISSION. [*Commentary:* Typical mission description would be to provide means to protect or return to operation those critical infrastructures under the commanders control, and to execute MOU/MOAs with operators of external infrastructures that prioritize the operations of infrastructures necessary for the installation/unit to function. This will also serve to heighten the awareness of infrastructure operators as to the vulnerability of their property to a terrorist attack.]

3. (U) EXECUTION

a. (U) Commander's Intent. [*Commentary:* Detail the commander's directive to detect and reduce threats directed at critical infrastructure under his control and work with infrastructure operators to protect external infrastructures.]

b. (U) Concept of Operations

(3) (U) Pre-Incident Phase. [*Commentary:* Describe ongoing risk reduction actions taken to improve CIP. List possible "points of total failure". A matrix of jurisdiction over key infrastructure elements is useful for delineation responsibilities. This phase is complete when an incident occurs that reduces the or eliminates the functioning of the infrastructure affected.]

(4) (U) Incident Response and Consequence Management Phase. [*Commentary:* This phase involves actions taken during the incident and actions taken to reconstitute after the incident. This phase will normally consist of compiling after action data, implementing compensatory security measures, and implementing measures to reinstitute the pre-incident phase.]

c. (U) Tasks

(1) (U) [Define tasks.]

d. (U) Coordinating Instructions

(1) (U) [*Commentary:* Assign coordinating instructions as necessary. Consider developing coordinating instructions that vary dependant upon Force Protection Conditions, and site-specific or specialized training.]

(2) (U) [*Commentary:* Describe any MOA/MOUs.]

(3) (U) [*Commentary:* Include representatives of military and civilian infrastructure operators on the installation/unit PSC for coordination.]

4. (U) ADMINISTRATION AND LOGISTICS. See annex D (Logistics).

5. (U) COMMAND AND SIGNAL

a. (U) Signal. [*Commentary:* Describe the alert system to be used and how it will be activated.]

b. (U) Command

(1) (U) [*Commentary:* Describe the relationship between infrastructure operators and the installation/unit.] See annex J (Command Relationships).

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ANNEX F (PUBLIC AFFAIRS) TO AT/FPP-02

(U) References: (a) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93

1. SITUATION

GENERAL. [*Commentary:* This annex establishes internal public affairs procedures and requirements for support of public affairs operations across the spectrum of crisis communications. Public affairs operations are organized into three functional areas: internal communications, community relations and media relations. Each phase of the force protection plan in this annex (pre-incident, incident and post-incident) will be broken down further into these categories to simplify planning and execution of each phase.]

2. MISSION. [*Commentary:* The PAO will provide timely and accurate release and management of information to the public and news media.]

3. EXECUTION. [*Commentary:* Provide public affairs guidance for pre-incident, incident, and post-incident phases for internal communications, community relations, and media relations. Also provide coordinating instructions as necessary.]

4. ADMINISTRATION AND LOGISTICS. See appendix 2.

5. COMMAND AND SIGNAL.

a. Command Information Bureau Locations.

(1) [*Commentary:* Primary and alternate locations of the command information bureau.]

b. Succession of Command.

(1) [*Commentary:* Describe the public affairs succession of command.]

Appendices:

1 - Command Information Bureau Organization
2 - Command Information Bureau Requirements
3 - Public Affairs External Support and Coordination Relationships
4 - Local/Regional Media Contacts

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ANNEX H (LEGAL) TO AT/FPP-02

Ref: (a) 18 U.S.C. 1385 "Posse Comitatus Act"
(b) DOD Directive 5210.56 (NOTAL) of 25 Feb 92
(c) CJCS Instruction 3121.01A (NOTAL) of 15 Jan 00
(d) DOD Directive 5240.1 (NOTAL) of 25 Apr 88
(e) DOD 5240.1-R of (NOTAL) 7 Dec 82
(f) DOD Directive 5200.27 (NOTAL) of 7 Jan 80

1. SITUATION

a. General. [*Commentary:* In implementing all phases of the AT/FP plan, local commanders will face a myriad of legal issues. These issues may deal with MOU/MOA rules of engagement (ROEs), jurisdiction, use of deadly force, search and seizure, claims, etc. The Office of the Staff Judge Advocate (OSJA) provides a full range of legal services and assistance to local commanders as well as to certain other authorized personnel on a wide variety of issues. Early consultation with the OSJA, before an incident occurs, can help identify potential legal problems. During or after an incident, the OSJA can provide continuing legal advice, and assistance to commanders and their personnel.]

b. Enemy. See annex B (Intelligence)

c. Friendly. See annex A (Task Organization) and annex J (Command Relationships).

d. Assumptions. None.

2. Mission. [*Commentary:* The OSJA, in conjunction with the internal legal assets of subordinate and tenant commands, will provide legal advice and assistance to local commanders on all aspects of the AT/FP plan beginning in the pre-incident phase and continuing through the post incident phase until the restoration of normal activities is complete.]

3. Execution.

a. Concept of Operations.

(1) [*Commentary:* Describe the legal resources available to the commander.]

b. Tasks

(1) [*Commentary:* Describe the tasks assigned to each of the legal resources available such as civil law, military justice, administrative law, and tenant command legal officers.]

c. Special Consideration

(1) Jurisdictional Issues. [*Commentary:* This section should discuss the jurisdictional responsibilities of Federal, state, and local officials (or U.S. and HN official overseas) who may have overlapping responsibilities for the detection, investigation, and prosecution of criminal offenses.]

(a) Installation Commander. [*Commentary:* The installation commander has jurisdiction over all incidents that occur within the boundaries of the installation except for those incidents of a terrorist/hostage situation. In such cases, the FBI will be immediately notified. The FBI may

or may not accept jurisdiction. Should the FBI decline jurisdiction, the installation commander will retain jurisdiction. See appendix 2 (Jurisdiction for Acts of Terrorism) to this annex.]

(b) State/Local or Host-Nation Government. [*Commentary:* Whenever the possibility exists that the effects or consequences of a crisis situation could effect surrounding counties or states, the appropriate officials for those jurisdictions should be notified.]

(2) Rules of Engagement (ROE)/Rules for the Use of Force (RUF). See Appendix 1 (Rules of Engagement/Rules for the Use of Force) of this annex. [*Commentary:* Inside the U.S., security and law enforcement personnel are expected to follow the guidance in reference (b) in their rules for the use of force. Outside the U.S., Reference (c) applies.]

(3) Posse Comitatus Act. [*Commentary:* The Posse Comitatus Act, reference (a), generally prohibits the direct use of military personnel, including military law enforcement personnel, as well as elements of the CMF and other security forces in support of this order to enforce Federal, state, and local criminal laws. This prohibition includes searches, seizures, arrests, or similar coercive encounters with civilians. It does not include actions taken for the primary purpose of protecting military facilities, property, and personnel.]

(4) Intelligence Collection. [*Commentary:* Domestic intelligence collection by military personnel is limited by references (d), (e) and (f). However, intelligence and law enforcement agencies are authorized to collect, retain, and disseminate information for the protection of departmental facilities, property and personnel. Given constitutional guarantees of free speech, free association, and privacy, however, intelligence and law enforcement agencies must scrupulously adhere to the applicable policies and procedures. Generally speaking, the proposed collection must be within the unit's mission, approved by the proper authority, within an authorized category, and by the least intrusive means available. Information regarding U.S. persons may be retained and disseminated only for an authorized purpose.]

4. COMMAND POST LOCATIONS

a. Primary. [*Commentary:* Specify the primary location for the command post, its address, secure and non-secure communications methods.]

b. Alternate. [*Commentary:* Specify the alternate location for the command post, its address, secure and non-secure communications methods.]

Appendices:

1 - Rules of Engagement/Rules for the Use of Force
2 - Jurisdiction for Acts of Terrorism
3 - Jurisdictional Boundaries (Pictorial)

Official:

//Signature//
[Name
Rank and Service

Title]

ANNEX L (HEALTH SERVICES) TO MCB AT/FPP-02

Ref: See annex V (References).

Time Zone: Lima (Local)

1. SITUATION

a. General. [*Commentary:* This annex outlines medical responses to potential situations resulting from all types of natural disasters (forest fires, flooding, snow, and destructive winds) and man-made incidents (HAZMAT, mass casualty incidents, bomb threats, and hostage/barricaded suspect). It should be developed by local medical authorities (typically in the form of a disaster preparedness plan) in cooperation with the AT/FP working group to ensure adequate integration of the health services plan with the rest of the AT/FP plan.]

b. Friendly Forces. See annex A (Task Organization) and annex J (Command Relationships).

c. Attachments/Detachments. [Per MOU/MOA.]

d. Assumptions.

(1) [*Commentary:* Local based medical services will not be able to function independently in performing its mission in response to major disaster situations without outside support from civil authorities.]

(2) [*Commentary:* Mass casualties and other situations requiring the activation of the disaster preparedness plan or any portion of it will normally be preceded by some warning that will allow an undetermined amount of time to prepare an effective response.]

(3) [*Commentary:* Certain situations, such as heavy weather or facility damage, may impede the ability to provide rapid response, treatment, and transportation of injured persons.]

2. MISSION. [*Commentary:* Local medical facilities will provide or coordinate medical support in order to execute this plan and be prepared to execute procedures for handling mass casualty incidents as necessary.]

3. EXECUTION

a. Commander’s Intent

(1) [*Commentary:* Generally, the commander’s intent will be to respond to AT/FP incidents in a coordinated manner supported by local medical assets.

(2) [*Commentary:* Support local community disaster response operations by providing medical personnel, medical transportation, and other items as needed.]

(3) [*Commentary:* Establish a disaster preparedness plan; train personnel within the context of that plan; and execute the provisions of the plan in response to disaster situations in keeping with the overall mission of the command.]

b. Concept of Operations

(1) [*Commentary:* Per the disaster preparedness plan.]

c. Tasks

(1) [*Commentary:* Per the disaster preparedness plan.]

d. Coordinating Instructions

(1) [*Commentary:* Per the disaster preparedness plan.]

4. ADMINISTRATION AND LOGISTICS

a. Administration. See annex P (Personnel Services).

b. Logistics

(1) See annexes D (Logistics) and E (Fiscal).

(2) [*Commentary:* Medicinal or other medical supplies will be obtained through appropriate Navy supply systems.]

5. COMMAND AND SIGNAL

a. Command. [*Commentary:* Defined by medical authorities.]

b. Signal. See annex K (Communications).

c. Command Post Locations

(1) [*Commentary:* EOC and medical facilities as contained in the disaster preparedness plan.]

d. Succession of Command

(1) [*Commentary:* Per the disaster preparedness plan.]

Appendices:

1 – Mass Casualty Procedures
2 – Supporting Medical Facilities
3 - Emergency Air Medical Evacuation Services
4 – Local Health Departments
5 – Ambulance Request Worksheet
6 – Pre-hospital Patient Care Report

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ANNEX O (TRAINING) TO AT/FPP-02

Ref: (a) MCO 3302.1D

1. GENERAL

a. Purpose. [*Commentary:* Detail the conduct of AT/FP related training activities to support the AT/FP plan.]

b. Assumptions

(1) [*Commentary:* Extensive use of mobile training teams (MTT) should be used whenever possible.]

(2) [*Commentary:* Maximize the use of local resources.]

(3) [*Commentary:* Unit level training, which focuses on individual awareness and procedural measures, is a low cost, effective means to elevate unit readiness.]

2. MISSION. [*Commentary:* On a continuing basis, provide and conduct AT/FP and disaster preparedness related training in order to prepare individuals, units, and task organized groups to successfully implement this plan. Be prepared to conduct regular training to validate and exercise this plan.]

3. EXECUTION

a. Commander's Intent. [*Commentary:* Maximize every training opportunity available. Safety will be intricately woven into training scenarios. Units responsible for implementing this plan will aggressively train their personnel. Training should follow a logical progression of complexity. The cornerstone of training will be individual training. Those that are required to execute this plan should be trained to do so. Those individuals will train their units and the task organized groups. Small pieces of the plan will be exercised gradually increasing the scenarios in scope and complexity. ENDSTATE: Personnel and tasked organized groups are trained and prepared to execute any part of this plan in a safe, competent manner.]

b. Concept of Operations

(1) Pre-Incident Phase. [*Commentary:* This phase focuses on the training of key individuals and units required to execute the plan. Units will exercise their operational responsibilities and actively participate in training events. Emphasis should be placed on the ability to smoothly and effectively transition from normal operations to an increased readiness posture with minimal delay. This phase is complete when units are properly and efficiently employed per this plan.]

(2) Incident Response and Consequence Management Phase. [*Commentary:* Individuals and units apply skills developed during the pre-incident phase. Performance is measures and analyzed. The lessons learned are used to refine procedures and future training. This phase is complete upon returning to the pre-incident phase, and all lessons learned are incorporated into this plan.]

c. Tasks

(1) [*Commentary:* Specify tasks for the personnel and offices that will be coordinating training events. This would include operations, AT/FP

working group, installation, tenant and/or staff representatives, and safety office personnel.

d. Coordinating Instructions

(1) [*Commentary:* Provide coordinating instructions pertaining to training objectives and requirements, scenarios, standards of achievement, and an appropriate exercise cycle.]

Appendices:

1 - AT/FP Levels of Training
2 - AT/FP Videos
3 - AT/FP Base Training Objectives Matrix
4 - Exercise Cycle

OFFICIAL:

//Signature//
[Name
Rank and Service
Title]

ANTITERRORISM TRAINING PROGRAMS AND REQUIREMENTS

1. General. The cornerstone of the Marine Corps antiterrorism/force protection (AT/FP) 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, dynamic, and integrated training program has been developed to ensure all Marines, family members, and civilian employees receive appropriate instruction relative to their grade/position, location and the terrorist threat.

2. Training. Commanders will ensure all assigned personnel receive appropriate training to advance AT/FP awareness as outlined below. Individual records will be maintained and updated accordingly.

a. Level I Antiterrorism (AT) Awareness Training

(1) As directed in Department of Defense (DOD) Instruction 2000.16 (NOTAL) of 14 Jun 01, all Marine Corps personnel will receive initial AT awareness training during initial service entry or during a period of AT awareness training used to establish an AT training baseline.

(2) Thereafter, all Marine Corps personnel and civilian employees will receive level I AT awareness training at least annually if they are deployed or eligible for deployment or if the terrorism threat level within the U.S. and its territories rises above moderate. All active duty Marines will receive level I AT awareness training at least annually.

(3) Web based level I AT awareness training is currently available at http://www.at-awareness.org. Use access code "AWARE" (no quotes). From there, proceed using a self-generated user ID and password. Upon completion of the training, print the completion certificate and forward to your security manager for placement in your official record.

(4) All Marine Corps personnel and civilian employees shall be provided an area of responsibility (AOR) update and threat brief within 3 months of deployment overseas.

(a) Commanders will ensure that personnel departing to or transiting a geographical Combatant Commander’s AOR are exposed to and execute the requirements of the gaining Combatant Commander’s AOR update. This information will be available through the chain-of-command and may be provided through multiple means including Combatant Commander publications, messages, and computer homepages.

(b) Additional pre-deployment specific AT/FP training requirements such as high-risk of capture, code of conduct/survival evasion resistance and escape, or others may be required. Therefore, contact should be made as soon as the requirement for travel becomes known.

(c) To fulfill all pre-travel briefing requirements when traveling overseas, personnel must be briefed in accordance with the highest terrorism threat level established by DOD or the AOR Combatant Commander for each individual country. Failure to understand and comply with briefing requirement in advance of travel requests may result in rejection of area/country clearance requests. Current terrorism threat level information

for AOR Combatant Commanders can be obtained at the following numbers: JFCOM (800) 542-08646; CENTCOM (813) 828-6289/90/91; EUCOM 011-441-480-84-1414; PACOM (808) 477-7309; SOUTHCOM (888) 547-4025 EXT 3720.

(d) State Department travel advisories that reflect a security concern (terrorist, insurgency/political instability, or criminal threat) can be obtained from the nearest State Department office, embassy and/or consulate, via the internet (http://www.state.gov), or by calling (202) 647-5225.

(e) The Navy MTAC 24-hour watch center point of contact: (STU-III capable) is DSN: 288-9490/18, COMM (202) 433-9490/18. MTAC watch can also be reached via:

1. SIPRNET homepage: www.ncis.navy.smil.mil

2. SIPRNET email: atac@mcismail.ncis.navy.smil.mil

3. SCI homepage: www.ncis.nmic.ic.gov

4. DODIIS email: atac@ncis.nmic.ic.gov

MTAC summaries, supplements, warning reports, and Naval Criminal Investigative Service (NCIS) threat assessments are available on interlink via the NCIS homepage.

(4) Family members of Marine Corps personnel and civilian employees 14 years of age or older traveling overseas on official business will receive level I AT awareness training. Furthermore, all family members will be encouraged to receive level I AT awareness training prior to any overseas travel.

(5) Contactor employees shall be offered level I AT awareness training under the terms and conditions specified in the contract.

(6) Individuals may become qualified to administer level I AT awareness training via two methods:

(a) Attending a formal level II antiterrorism officer (ATO) training course.

(b) Individuals who are subject-matter experts and who have received formal training in AT and individual protection may be individually exempted by the commander from the level II ATO training requirement outlined below provided they receive additional training that reviews current AT publications and identifies the methods for obtaining AOR-specific updates.

(7) Table 11-1 outlines level I AT awareness training requirements.

b. Level II ATO Training

(1) Level II ATO training is designed to produce an AT advisor to the Commander. Each installation and/or deploying unit will be assigned at least one level II ATO trained individual. The installation/unit ATO shall be assigned in writing and will have completed level II AT training.

(2) Table 11-2 outlines the level II ATO training requirements.

c. Level III Pre-Command AT Training

(1) Level III pre-command AT training is designed to expose the prospective commander to AT issues. Pre-command training tracks will provide Level III pre-command AT training to prospective commanders. In particular, this training shall be tailored to provide prospective commanders the depth and breath of knowledge necessary to perform the full spectrum of AT responsibilities.

(2) Table 11-3 outlines the level III pre-command AT training requirements.

d. Level IV AT Executive Seminar

(1) The level IV AT executive seminar is designed to expose senior officers (O-6/O-8) to AT issues. The Joint Staff Directorate for AT/FP (J-3) conducts the level IV executive seminar. The purpose is to create a senior-level forum for the presentation and discussion of prevailing AT issues as they affect military operations. The objectives for the seminar are to enhance the understanding among commanders and senior officers of AT issues and their responsibilities in developing appropriate programs. This includes: informing attendees of the information sources available to assist them in risk management decisions; providing a forum for the exchange of ideas and problems on AT related subjects; providing a better understanding of the terrorist, including profiles, targets, tactics, training, and equipment; and enhancing the understanding of consequence management (CM) issues. For further information, contact CMC (PS) at (703) 692-4495.

(2) Table 11-4 outlines level IV AT executive seminar training requirements.

e. Training for High-Risk Personnel and High-Risk Billets. High-risk personnel, and in some cases their family members, are eligible for advanced AT training. Whenever possible, training for high-risk personnel and high-risk billets will be completed prior to arrival in theater.

3. Assignment to Formal AT Training

a. The following specialized training courses are available for Marines involved in physical or personnel security programs. CMC (PS) or CG MCCDC (T&E) will allocate quotas and funding.

(1) Course Title: Antiterrorism Instructor Qualification Course (A05M9L1)

Location: U.S. Army, John F. Kennedy Special Warfare Center, Ft. Bragg, North Carolina (11 Days)

Purpose/Scope: Terrorism and terrorist operations; individual protective measures; hostage survival techniques; and terrorist surveillance detection.

(2) Course Title: Antiterrorism Officer Course (ATO)
(A16HBS3)

Location: U.S. Army, Military Police School,
Fort Leonard Wood, Missouri (2 weeks)

Purpose/Scope: To train students on the role and responsibilities of an ATO. Training includes the threat assessment, preparation of the AT plan, and certification to conduct unit level AT training.

(3) Course Title: Individual Terrorism Awareness Course
A05M9D1

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

Purpose/Scope: Terrorism and terrorist operations; self-protection measures; hostage survival techniques.

(4) Course Title: Dynamics of International Terrorism
F19HBT1

Location: U.S. Air Force, Hurlburt Field,
Florida (5 days)

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.

(5) Course Title: High Risk Personnel (HRP) Course
M02M429

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

Purpose/Scope: Designed to train Marines with defensive pistol techniques and procedures while traveling abroad in countries with a high threat level of terrorist activity. This course is restricted to personnel actually designated to fill overseas high-risk billets.

(6) Course Title: Antiterrorism Training Officer Level II
N03M9R1

Location: Expeditionary Warfare Training Group, (Atlantic),
NAB Little Creek, Virginia (2 days)

Purpose/Scope: Contains seven core subjects: Introduction to Terrorism, Terrorism Operations, Detecting Terrorist Surveillance, Individual Protective Measures, Hostage Survival, Threat Levels, Force Protection Condition Measures and WMD.

(7) Course Title: Antiterrorism Officer Level II
N03M9L1

Location: Expeditionary Warfare Training Group, (Atlantic), NAB Little Creek, Virginia (5 days)

Purpose/Scope: The ATO course incorporates the level II training requirements contained in DOD Instruction 2000.16 of 14 Jun 2001 and provides the ATO with the necessary skills and knowledge to manage their command's antiterrorism program ashore and afloat.

(8) Course Title: Antiterrorism Level III Commander's Course

Location: Expeditionary Warfare Training Group, (Atlantic), NAB Little Creek, Virginia (2 days)

Purpose/Scope: The AT level III course incorporates the level III training requirements contained in DOD Instruction 2000.16 of 14 Jun 2001 and provides the commanding officer with the necessary skills and knowledge to direct their command's AT program ashore or afloat.

(9) Course Title: Evasive Driving for General Officers and Select Personnel

Location: Winchester, VA (1.5 days)

Purpose/Scope: Terrorism threat recognition, self-protection measures, overview of historical events, and extensive vehicle handling techniques to include skid control, vehicle handling, evasive maneuvers, ramming techniques, and vehicle capabilities.

(10) Course Title: Evasive Driving for Senior Officer Driver & Protective Service Personnel

Location: Ft. Leonard Wood, MO (3 days)

Purpose/Scope: Terrorism threat recognition, self-protection measures, overview of historical events, and extensive vehicle handling techniques to include skid control, vehicle handling, evasive maneuvers, ramming techniques, and vehicle capabilities.

(11) Course Title: Intelligence in Combating Terrorism (A12HCZ1)

Location: Ft. Huachuca, AZ (12 days)

Purpose/Scope: Identification and assessment of the terrorist threat to specific installations and to deployable units during pre-deployment, deployment and redeployment, and application to counterespionage and counter narcotics.

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

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

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

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

4. Additional Sources of AT Training

a. Marine Corps Institute correspondence courses such as MCI 02.10b, Terrorism Awareness for Marines.

b. Mobile training teams from a variety of Marine Corps and external sources.

c. Innovative use of news and production media by public affairs office, and training and audiovisual support center personnel.

d. AT websites and other internet sites related to international terrorism.

LEVEL OF TRAINING	TARGET AUDIENCE	MINIMUM TRAINING STANDARD
Level I AT Awareness Training provided annually to: 1. Overseas-based DOD personnel 2. All Active uniformed Domestic U.S.-based members of the Combatant Commander's and Services 3. All Domestic U.S.-based DOD personnel eligible for official Overseas travel on Government orders 4. All Domestic U.S.-based DOD Personnel regardless of duty status if the Domestic U.S. Terrorism Threat Level is promulgated above "MODERATE." **Graduates will have requisite knowledge to remain vigilant for possible terrorist actions and employ AT tactics, techniques, and procedures, as discussed in DOD O-2000.12-H and Joint Pub 3-07.2	*DOD Personnel accessions during initial training *Military, DOD civilians, their family members 14 years old and greater (when family members are deploying or traveling on Government orders), and DOD-employed Contractors.	Component-provided instruction; incorporates Component-standardized POI consisting of the following minimum topics: 1. Viewing the Service-selected personal awareness video provided under the instruction of a qualified Level I AT Awareness instructor and/or DOD-sponsored, and Component-certified, computer-based and/or distance learning (DOD personnel accessions must receive initial training under instruction of a qualified Level I AT Awareness Instructor) 2. Instruction on the following: *Introduction to Terrorism *Terrorist Operations *Individual Protective Measures *Terrorist Surveillance Techniques *Improvised Explosive Device (IED) Attacks *Kidnapping & Hostage Survival *Explanation of Terrorism Threat Levels and Force Protection Condition System 3. Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" and "Antiterrorism Individual Protective Measures" folding card. (Local reproduction for both is authorized.) 4. Receipt of AOR updates three months prior to travel to include current threat brief and AOR-specific requirements as provided by the receiving geographic Combatant Commander.

Table 11-1.--AT/FP Training Requirements for Level I AT and Pre-Deployment Training.

LEVEL OF TRAINING	TARGET AUDIENCE	MINIMUM TRAINING STANDARD
Level II AT Officer (ATO) Training ** Graduates shall have requisite knowledge and materials to manage a comprehensive AT Program and advise the commander in all AT areas.	Officers/NCOs/civilian staff officers, who are tracked and command-designated to serve as the AT advisor to the Commander and provide Level I Instruction in coded billets.	1. Component-provided instruction (resident or MTT); incorporates Component-standardized POI consisting of the following minimum topics: *Understanding AT Roles and Responsibilities - Understanding Policy & Standards - Access Reference Sources *Organize for AT - Command/Staff Relationships - FP Working Groups *Assess Vulnerabilities - Baseline Unit FP Posture - Conduct Assessment *Assess Threat - Intel/CI Integrations - Information OPS *Create and Execute AT Programs - Use of Terrorism Threat *Level/Force Protection Conditions - Unit/Installation Protective Measures - Mitigating Vulnerabilities *Prepare AT Plans - Templates & Planning Tools - How to Develop & Write Plans - WMD Considerations - Use of RAM to protect the Installation *AT Resource Management - Requirements Generation & Prioritization - CbT RIF *Conduct AT Training - Exercise Unit AT Plans - Obtain AOR-specific updates - Oversee AT Level I Training 2. Review of DOD Directive 2000.12, Instruction 2000.16, DOD O -2000.12-H, and other applicable DOD/Service/Agency publications. 3. Methods available for obtaining AOR-specific updates for deployment/travel areas. 4. Component-directed modules on other aspects of AT such as physical security requirements, technology updates, etc.

Table 11-2.--AT/FP Training Requirements for Level II ATO Training.

LEVEL OF TRAINING	TARGET AUDIENCE	MINIMUM TRAINING STANDARD
Level III Pre-Command AT Training ** Graduates shall have requisite knowledge and materials to supervise a comprehensive AT Program and manage AT issues.	0-5/0-6 Commanders	Component-provided instruction during pre-command pipelines; incorporates Component-standardized POI consisting of the following minimum topics: 1. Viewing the SECDEF/CJCS Video 2. Directive/reference review *Understanding AT responsibilities - Understanding Policy - Assessments - Off-Installation Housing *Ensuring Preparation of AT Plans - Baseline FP Posture - Mitigating WMD Attack - MOUs/MOAs *Ensuring Conduct of AT Planning - AT Plans & Training - Level I Training *Organizing for AT *Understanding the Local Threat Picture - Fusion of Intelligence *Building a Sustainable AT Program - Terrorism Threat Levels *Executing Resource Responsibilities - AT Resource Programming - Construction Standards *Understanding Use of Force and ROE - Terrorist Scenarios & Hostile Intend Decision making 3. Review DoD Directive 2000.12, DoD Instruction 2000.16, DoD O-2000.12-H, and other applicable DoD/Service/Agency publications. 4. Issuance of Commander's Handbook (Joint Pub 5260).

Table 11-3.--AT/FP Training Requirements for Level III Pre-Command AT Training.

LEVEL OF TRAINING	TARGET AUDIENCE	MINIMUM TRAINING STANDARD
Level IV Executive Seminar ** Graduates shall have requisite knowledge and materials to provide oversights to AT Programs and Policies.	Officers in the grade of 0-6/0-8 and Department of Defense civilians in equivalent grades selected by Services/ Combatant Commanders/DoD agencies who are responsible for AT policy, planning and execution.	CJCS Executive-level seminar hosted by the Joint Staff Directorate for Antiterrorism/Force Protection (J-3). Provides pertinent current updates, briefings, and panel discussion topics. Seminar includes 3 tabletop AT wargames aimed at facilitation interaction and discussion among seminar participants.

Table 11-4.--AT/FP Training Requirements Level IV AT Executive Seminar.

TERRORISM/LAW ENFORCEMENT/SECURITY INTERNET WEBSITES
AND TELEPHONE HELPLINES

1. The far-reaching capability of the internet, or world wide web, makes it an invaluable source for additional information. Below are suggested links for both unclassified (NIPRNET) and classified (SIPRNET) platforms.

a. NIPRNET (Non-secure Internet Protocol Router Network) links:

MILITARY:	
DTRA AT/FP non-secure helpline	http://ATFPhelp@dtra.mil
DefenseLINK	http://www.defenselink.mil/
Defense Threat Reduction Agency (DTRA)	http://www.dtra.mil/
Joint Center for Lessons Learned	http://www.jtasc.acom.mil/dodnato/jcll/
Joint Electronic Library	http://www.dtic.mil/doctrine/jel
Joint Staff, J-3	http://www.dtic.mil/jcs/force_protection/main.html
Washington Headquarters Services, Directives and Records Branch	http://www.dtic.mil/whs/directives
UNIFIED COMMANDS	
Central Command (CENTCOM)	http://www.centcom.mil/
European Command (EUCOM)	http://www.eucom.mil/
Joint Forces Command (JFCOM)	http://www.jfcom.mil/
JFCOM Civil Support	http://www.jfcom/mil/jtfcs/index.html/
Pacific Command (PACOM)	http://www.pacom.mil/
Special Operations Command (SOCOM)	http://www.socom.mil/
Southern Command (SOUTHCOM)	http://www.southcom.mil/home/index.cfm/
Space Command (SPACECOM)	http://www.spacecom.af.mil/usspace/
Strategic Command (STRATCOM)	http://www.stratcom.mil/
Transportation Command (TRANSCOM)	http://www.transcom.mil/
SERVICES	
Army	http://www.army.mil/
U.S. Army Soldier and Biological Chemical Command (SBCCOM)	http://www.sbccom.army.mil/
U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) Medical Management of Biological Casualties Handbook	http://www.usamriid.army.mil/education/bluebook.html
U.S. Army Center for Health Promotion & Preventive Medicine, Anthrax Factsheet	http://chppm-www.apgea.army.mil/homelandsecurity/anthraxfactsheet.pdf
U.S. Army Center for Health Promotion & Preventive Medicine, Checking Suspicious Mail	http://chppm-www.apgea.army.mil/homelandsecurity/suspiciousmail.pdf
Army National Guard WMD	http://www.ngb.dtic.mil/
Air Force	http://www.af.mil/
Air Force Office of Special Investigations (AFOSI)	http://www.dtic.mil/afosi/
Force Protection C2 Systems Program Office	http://www.hanscom.af.mil/ESC-FD/default.asp/
USAF Battlelabs	http://www.xo.hq.af.mil/afbattlelab/
USAF Security Forces	http://afsf.lackland.af.mil/
Navy	http://www.navy.mil/
Naval Criminal Investigative Service (NCIS)	http://www.ncis.navy.mil/

Physical Security Knowledge Center	http://dodpse.spawar.mavy.mil/
Marine Corps	http://www.usmc.mil/
Marine Corps Lessons Learned System	http://greenshirt.nalda.navy.mil/mclls.html/
MARCORPSYSCOM	http://www.marcorsyscom.usmc.mil/
Marine Corps Intel Activity	http://ismo-www1.mpq.usmc.mil/mcia/index.htm/
Coast Guard	http://www.uscg.mil/
Coast Guard Maritime Security	http://www.uscg.mil/overview/maritimesecurity.htm/

GOVERNMENT:

Federal Web Locater	http://www.law.vill.edu/fed-agency/fedwebloc.html/
Congressional Action	http://thomas.loc.gov/
National Communications System	http://www.ncs.gov/
National Domestic Preparedness Office	http://www.ndpo.gov/
CDC -- Center for Disease Control, Health Advisory, How to Handle Anthrax and Other Biological Agent Threats	http://www.bt.cdc.gov/documentsapp/anthrax/10122001handle/10122001handle.asp/
CIA -- Central Intelligence Agency	http://www.odci.gov/
DOJ -- Department of Justice	http://www.usdoj.gov/
Federal Bureau of Investigation	http://www.fbi.gov/
National Domestic Preparedness Office (NDPO)	http://www.ndpo.gov/
DOS -- Department of State	http://www.state.gov/
Office of the Coordinator for Counterterrorism	http://www.state.gov/s/ct/
Bureau of Diplomatic Security	http://www.ds.state.gov/index_n.htm/
DOS - Counterterrorism	http://state.gov/www/global/terrism/index.html/
Travel Warnings and Consular Information Sheets	http://travel.state.gov/travel_warnings.html/
Response to Terrorism	http://usinfo.state.gov/topical/pol/terror/
EPA -- Environmental Protection Agency	http://www.epa.gov/
Chemical Emergency Preparedness Office	http://www.epa.gov/ceppo/
FEMA -- Federal Emergency Management Agency	http://www.fema.gov/
Federal Response Plan	http://www.fema.gov/r-n-r/frp/
Disaster Preparedness (Fact Sheets)	http://www.fema.gov/library/lib07.htm/
Treasury Department	http://www.treas.gov/
Office of Foreign Assets Control	http://www.treas.gov/ofac/
Abbreviations and Acronyms of the U.S. Government	http://www.ulib.iupui.edu/subjectareas/gov/docs_abbrev.html/

REFERENCE:

Acronym Finder	http://www.acronymfinder.com/
Army Acronyms	http://www.army.mil/aps/97/acro.htm/
Central Intelligence Agency	http://www.odci.gov/
CIA Factbook	http://www.odci.gov/cia/publications/factbook/index.html/
CIA Maps	http://www.odci.gov/cia/publications/factbook/docs/ref.html/
Dictionary.com	http://dictionary.com/
DoD Dictionary of Military Terms	http://www.dtic.mil/doctrine/jel/doddict/index.html/
FirstGov	http://firstgov.gov/

GovSpot	http://www.govspot.com/
Joint Acronyms and Abbreviations	http://www.dtic.mil/doctrine/jel/doddict/acronym_index.html/
US Armed Forces Abbreviations	http://www.globemaster.de/html/dictionary.html/
Navy Acronyms	http://www.cnet.navy.mil/netpdtc/acronyms.htm/
The Reference Desk	http://www.refdesk.com/
Thesaurus.com	http://thesaurus.com/
The Weather Channel	http://www.weather.com/
Unique Strategy, Research & Thought	http://www.anglefire.com/journal2/howie137/Main.htm/

TECHNOLOGY:

MILITARY	
Defense Technical Information Center - Joint Acronyms and Abbreviations	http://www.dtic.mil/doctrine/jel/doddict/acronym_index.html/
DoD Explosive Detection Equipment Program Home Page	http://www.explosivedetection.nfesc.navy.mil/
DoD Joint Non-Lethal Program Office	http://iis.marcorsyscom.usmc.mil/jnlwd/
Government Sponsored Labs	http://www.dtic.mil/lablink/
U.S. Air Force, Electronic System Center, Force Protection	http://www.hanscom.af.mil/esc-fd/
U.S. Army Corps of Engineers - Identification and Evaluation of COTS Blast Mitigation Products	http://bmag.nwo.usace.army.mil/
U.S. Army Program Manager, Physical Security Equipment	http://www.monmouth.army.mil/smc/pmpse/
SPAWAR Charleston	http://www-chas.spawar.navy.mil/
GOVERNMENT	
Extranet for Security Professionals	http://isp.hpc.org/
National Institute of Standards and Technology	http://www.nist.gov/
National Institute of Standards and Technology - Computer Resource	http://csrc.nist.gov/
National Institute of Standards and Technology Rainbow Series	http://csrc.ncsl.nist.gov/secpubs/rainbow/
Technical Support Working Group	http://www.tswg.net/
COMMERCIAL	
Federation of American Scientists	http://www.fas.org/man/index.html/
Terrorism Research Center	http://www.terrorism.com/
National Institute of Justice	http://www.nlectc.org/
American Society for Industrial Security	http://www.asisonline.org/
CardTech/SecurTech	http://www.ct-ctst.com/
Smart Card Industry Association	http://www.scia.org/
Security Products Magazine	http://www.secprodonline.com/

TERRORISM RELATED WEBSITES:

J34 Homepage on gccw	http://nmcc20a/~jdcleap/j34.htm/
FEMA Fact Sheet on Terrorism	http://www.fema.gov/library/terrorf.htm/
FBI "Terrorism in the United States"	http://www.fbi.gov/publications/terror/terroris.htm/
DOS "Patterns of Global Terrorism"	http://www.state.gov/global/terrorism/1997Report/1977index.html/
DOD AT Page	http://www.dtic.mil/jcs/force_protection/
Terrorism Research Center	http://www.terrorism.com/terrorism/index.

	shtml/
Terrorism/Antiterrorism	http://www.dtic.mil/
Rand Homepage	http://www.rand.org/
Kroll Associates	http://www.krollassociates.com/
ANSER Institute for Homeland Security	http://www.homelandsecurity.org/
Center for Nonproliferation Studies	http://cns.miis.edu/
Center for Strategic and Int'l Studies	http://www.csis.org/
Johns Hopkins Center for Civilian Biodefense Studies	http://www.Hopkins-biodefense.org/
Institute for the Prevention of Terrorism	http://www.mipt.org/
Stormfront White Nationalist Page	http://www.stormfront.org/
HateWatch Guide to Hate Groups	http://hatewatch.org/
The Counterterrorism Page	http://www.terrorism.com/
Terrorism	http://www.milnet.com/milnet/terror.htm/
Terrorist Profiles	http://nsi.org/Library/Terrorism/profterr.txt/
Terrorist Use of Chemical Weapons	http://www.uberhip.com/people/godber/research/cwpaper.html/
MCI Link	http://www.mci.hqi.usmc.mil/support_files/mci_news/terrorism/main.htm/
CDT's Counterterrorism Issues Page	http://wwwcdt.org/policy/terrorism/
International Policy Institute for Counterterrorism	http://www.ict.org.il/

SECURITY AND LAW ENFORCEMENT:

Provost Marshal/Intelligence Link	http://www-ioc.army.mil/dm /DMPWEB/links.htm
US Army MP School	http://www.mcclellan.army.mil/usamps/dots/aletd
NCIS Webpage	http://www.ncis.navy.mil
Air Force Security Forces Home Page	http://www.kirtland.af.mil/organizations/AFSF/
Security Management Online	http://www.secutitymanagement.com/
Law Enforcement Product News	http://www.law-enforcement.com/
Justice Information Technology Network	http://www.nlectc.org/
Scotti School Homepage	http://www.ssdd.com/sscschd97/html
Code 7 Café, Firearms Information	http://www.av.qnet.com/~harv/index.htm

b. SIPRNET (Secure Internet Protocol Router Network) links:

MLITARY (SIPRNET):

DTRA AT/FP Secure Helpline	ATFPhelp@snet.dswa.smil.mil/
Acronym Lookup	http://157.224.120.250/acronym.nsf/$$search?openform/
Armed Forces Medical Intelligence Center (AFMIC)	http://www.dia.smil.mil/intel/afmic/afmic.html/
Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD SOLIC)	http://webhost.policy.osd.pentagon.smil.mil/solic/at/index.htm/
Defense Intelligence Agency (DIA)	http://delphi-s.dia.smil.mil/
Early Bird	http://delphis.dia.smil.mil/admin/EARLYBIRD/eb.html/
Joint Center for Lessons Learned	http://JCLL.jwfc.jfcom.smil.mil/

Joint Electronic Library	http://nmcc20a.nmcc.smil.mil/users/dj9j7ead.doctrine/jel/index.html/
Joint Personnel Recovery Agency (JPRA)	http://www.jpra/jfcom/smil.mil
Joint Staff, J-34	http://www.nmcc.smil.mil/j34/terrorism/index.html/
Red Switch Directory	http://157.224.120.250/staffs.nsf/mainframeset
Unified Commands	
Central Command (CENTCOM)	http://www.centcom.smil.mil/
European Command (EUCOM)	http://www.eucom.smil.mil/eucom.html/
Joint Forces Command (JFCOM)	http://157.224.120.250/
Pacific Command (PACOM)	http://164.213.23.19/
Special Operations Command (SOCOM)	http://www.socom.smil.mil/
Southern Command (SOUTHCOM)	http://www.southcom.smil.mil/
Space Command (SPACECOM)	http://www.usspace.spacecom.smil.mil/
Strategic Command (STRATCOM)	http://www.gccs.stratcom.smil.mil/
Transportation Command (TRANSCOM)	http://www.transcom.smil.mil/index.cfm/
SERVICES (SIPRNET):	
Army	http://134.11.207.212/index.htm/
Center for Army Lessons Learned (CALL)	http://call.army.smil.mil/
Air Force	http://c2www.af.pentagon.smil.mil/
Air Combat Command (ACC) Center for Lessons Learned	http://www.acc.af.smil.mil/do/doj/acccll/index.htm/
Air Force Center for Knowledge Sharing Lessons Learned (AFCKSLL)	http://knowledge.langley.af.smil.mil/afcks/
Air Force Office of Special investigations (AFOSI)	http://www.afosi.af.smil.mil/
Navy	http://www.cno.navy.smil.mil/
Navy Lessons Learned System (NLLS)	http://www.nwdc.navy.smil.mil/navagation1/nlls.htm
Naval Criminal Investigative Service (NCIS)	http://www.ncis.navy.smil.mil/
Marine Corps	http://www.usmc.smil.mil/
HQMC AT/FP Home Page	http://www.hqmc.usmc.smil.mil/pos-10.htm
Coast Guard	http://204.36.191.2/index.html

GOVERNMENT (SIPRNET):

CIA -- Central Intelligence Agency	http://205.137.222.140/index.html/
FBI -- Federal Bureau of Investigation	http://fbihq.adnet.sgov.gov/index.html/
ANSIR	http://fbihq.adnet.sgov.gov/ansir/ansir.html/
Intelink Central	http://www.ismc.sgov.gov/
NSA	http://www.nsa.smil.mil/

2. The following helplines are offered to fulfill pre-travel briefing requirements. When traveling overseas, personnel must be briefed in accordance with the highest terrorism threat level established by the Department of Defense or the area of responsibility (AOR) of the geographic combatant commander for each individual country. Failure to understand and comply with briefing requirement in advance of travel requests may result in rejection of area/country clearance requests. Current terrorism threat level information for AOR combatant commanders can be obtained at the following numbers: JFCOM (800) 542-08646; CENTCOM (813) 828-6289/90/91; EUCOM 011-441-480-84-1414; PACOM (808) 477-7309; SOUTHCOM (888) 547-4025 EXT 3720.

a. State Department travel advisories that reflect a security concern (terrorist, insurgency/political instability, or criminal threat) can e obtained from the nearest State Department office, embassy and/or consulate, via the internet (http://www.state.gov), or by calling (202) 647-5225.

b. The Navy MTAC 24-hour watch center point of contact: (STU-III capable) is DSN: 288-9490/18, COMM (202) 433-9490/18. MTAC watch can also be reached via:

(1) SIPRNET homepage: www.ncis.navy.smil.mil

(2) SIPRNET email: atac@mcismail.ncis.navy.smil.mil

(3) SCI homepage: www.ncis.nmic.ic.gov

(4) DODIIS email: atac@ncis.nmic.ic.gov

MTAC summaries, supplements, warning reports, and Naval Criminal Invesigative Service (NCIS) threat assessments are available on interlink via the NCIS homepage.

SECURITY SCREENING AND SPECIALIZED TRAINING FOR MARINES SELECTED FOR ASSIGNMENT TO HAZARDOUS BILLETS

1. General

a. Training

(1) Marines selected for assignment to certain hazardous or high-risk billets are required to complete additional antiterrorism/force protection (AT/FP) training.

(2) Marines selected for assignment to certain hazardous or high-risk billets may also be required to complete additional code of conduct (CoC)/survival evasion resistance and escape (SERE) training according to established Combatant Commander requirements.

(3) The CG, MCCDC (TE) conducts antiterrorism (AT) training for Marines assigned to high-risk billets where the threat warrants (such as Saudi Arabia).

(4) Prior to transferring to an overseas assignment, all Marines, their dependents and civilian employees will be provided an area of responsibility (AOR) specific threat brief by their transferring command.

b. The following factors are criteria for assigning certain billets as "hazardous" or high-risk.

(1) Long-term threat potential of a designated country.

(2) Special threat situation of unknown duration of a country or geographic area.

(3) Type of duties to be performed by the incumbent, such as UN observer, counterintelligence, or similar.

2. Responsibilities

a. Deputy Commandant for Manpower and Reserve Affairs (DC M&RA) (MMOA/MMEA)

(1) Not later than 120 days prior to the desired date of transfer, and prior to the issuance of orders:

(a) Select Marines to be assigned to a high-risk billets listed in the MCBul published by DC PP&O that identifies high-risk billets and required training.

(b) Provide a history, when requested, of the individual's previous duty assignments to the appropriate billet sponsor indicating that prescreening is required.

(c) Coordinate pre-deployment training requirements with CG, MCCDC for Marines to be assigned to security assistance sponsored billets abroad.

(2) Use the assessment provided by the billet sponsor in addition to all other assignment factors to arrive at a final decision regarding the assignment of the Marine to the billet in question. When an unfavorable assessment is received from the billet sponsor and a decision is reached not to assign the originally considered Marine to a hazardous billet, identify

another Marine for assessment and screening by the billet sponsor. The final decision for assignment to a hazardous billet rests with DC M&RA (MMOA/MMEA).

(3) Not later than 100 days prior to the desired effective date of transfer, and prior to the issuance of orders, provide the CG, MCCDC and DC PP&O (PS) the names of Marines being assigned to hazardous billets, and the specific training required.

(4) Upon receipt of the training quota(s) and course date(s) from CG MCCDC, issue orders assigning the appropriate AT/FP training to the designee.

(5) In coordination with MCCDC; DC PP&O (PS & POE); and the Joint Personnel Recovery Agency (JPRA) ensure SERE School (U.S. Navy and/or JPRA) quota availability for designees and issue orders assigning them to training as required.

(6) When requested by Director, Intelligence (I), a list of Marines serving in external billets will be provided.

b. Deputy Commandant for Plans, Policies, and Operations (DC PP&O) (PS):

(1) Not less than annually or on an as needed basis publish MCBul that identifies all external high-risk billets and associated required training for those billets (both AT/FP and CoC/SERE).

(2) Upon receipt of a request from DC M&RA (MMEA or MMOA) to determine whether a proposed new billet should be added to the MCBul identifying high-risk billets, obtain guidance from the appropriate billet coordinator and Director Intelligence (I). If appropriate, add billet to the MCBul.

(3) During February of each year, coordinate a review of the MCBul, and all other billets external to the Marine Corps located in areas where the terrorist threat level has increased to significant or high. If applicable, publish changes to the MCBul by April of that year.

(4) When notified by Director, Intelligence (I) of a change of threat levels affecting required training per the MCBul, coordinate with CG, MCCDC to ensure training is modified to meet the new threat.

(5) When notified by Director, Intelligence (I) of an increase in the terrorist threat to either significant or high for a given location, coordinate with DC M&RA, (MMEA/MMOA), CG, MCCDC, and the cognizant HQMC billet sponsors to ensure appropriate action is initiated.

(6) During the month of August of each year, provide CG, MCCDC a by-month listing of billets and associated required AT training for the following fiscal year. Additionally, provide projected AT/FP training quota requirements by course for the following 4 fiscal years.

c. Commanding General, MCCDC (T&E)

(1) Upon receipt of requested quotas from appropriate school controlling agencies, provide DC PP&O (PS) and the DC M&RA (MMEA/MMOA) with appropriate training quota memoranda (TQM) containing class seats, convening dates, prerequisites, and administrative instructions.

(2) Provide additional TQM data, as required, not later than 16 days after receipt of the names of Marines to be assigned to hazardous billets.

(3) Manage the high-risk personnel (HRP) course, per MCO 1553.1B.

(4) Review programs of instruction at other service and civilian schools, per enclosure (11) of this Order.

(5) Review Marine Corps AT training requirements for high-risk billets on an annual basis. Budget for appropriate amounts of training quotas, considering unforeseen requirements.

(6) Upon establishment of a new billet external to the Marine Corps, request a determination from DC PP&O (PS) whether the billet should be identified as a high-risk billet.

(7) When notified by DC PP&O (PS) that a billet external to the Marine Corps now requires security screening and/or specialized training, ensure billet sponsors make appropriate annotations to the respective tables of organization (T/O).

d. Director, Intelligence (I)

(1) Upon receipt of the name of a Marine considered for assignment to a billet listed in the MCBul, review that Marine's previous assignments to determine:

(a) If any special security access was previously held.

(b) To what, if any, information affecting national security the prospective assignee may have been exposed.

(2) Not later than 10 days after receipt of the name of a Marine considered for assignment to a billet listed in the MCBul, develop and provide to the DC M&RA (MMEA/MMOA) an assessment of the intelligence vulnerability of the prospective assignee. This assessment should be based on the prospective assignee's past history of sensitive billets, and a verification of the current threat level germane to the area in which the billet is located.

(3) Maintain a current listing of all significant and high terrorist threat areas for dissemination to DC PP&O (PS), DC M&RA (MMEA/MMOA), and the HQMC billet coordinators, as required.

(4) Immediately notify DC PP&O (PS), DC M&RA (MMOA/MMEA), and the HQMC billet coordinators when the terrorist threat levels increase to either significant or high for a given billet.

e. Billet Coordinators

(1) Ensure that T/O's listing billets requiring specialized training are annotated and updated, as required.

(2) When notified by DC PP&O (PS) or Director, Intelligence (I) of an increase in the terrorist threat levels to either significant or high for a given location, take the following action:

(a) Identify all external billets to the Marine Corps located in the subject significant or high threat area.

(b) Recommend whether security screening and/or specialized training are required for Marines filling billets.

(3) Conduct frequent reviews of the AT training required by coordinated billets, and make changes on the T/O as necessary.

REFERENCES

(a) JPUB 1-02 of 12 Apr 01 (Dictionary of Military and Associated Terms)
(b) SECNAVINST 3300.2A (NOTAL) of 21 March 01 (DON Antiterrorism/Force Protection (AT/FP) Program)
(c) DOD Instruction 2000.16 (NOTAL) of 14 Jun 01 (DOD Antiterrorism Standards)
(d) JPUB 5-03.2 of 15 Mar 92 (Joint Operations Planning and Execution System, Volume II (Planning and Execution Formats and Guidance))
(e) JPUB 3-07.2 of 17 Mar 98 (Joint Tactics, Techniques, and Procedures for Antiterrorism)
(f) FMFM 7-14 (Combating Terrorism)
(g) MCO 5000.17A (Marine Corps Lessons Learned System)
(h) MCO 5500.14A (Flightline Security (FLS) Program)
(i) MCRP 3-02E (The Individual's guide for Understanding and Surviving Terrorism)
(j) MCO P5530.14 (Marine Corps Physical Security Program Manual)
(k) MCO 5740.2F (OPREP-3 SIR Serious Incident Response)
(l) DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93 (Protection of DOD Personnel and Assets from Acts of Terrorism)
(m) MCI 02.10b (Terrorism Awareness for Marines)
(n) CJCS Instruction 5261.01 (NOTAL) of 1 Jul 01 (Combatting Terrorism Readiness Initiative Fund)
(o) MCO P5580.2A (Law Enforcement Manual)
(p) CJCS Instruction 3610.01A (NOTAL) of 1 Jun 01 (Aircraft Piracy (hijacking) and Destruction of Derelict Airborne Objects)
(q) MCO 1553.1B (Marine Corps Training and Education System)
(r) DOD Directive 4500.54G (NOTAL) of 5 Jan 92 (DOD Foreign Clearance Guide)
(s) CJCS 5260 (NOTAL) of 1 Jan 97 (Service Members Self Protection Guide: A Selp-Help Guide to Combat Terrorism While Overseas)
(t) MCO 3460.1A (Training and Education Measures Necessary to Support the Code of Conduct)
(u) MCRP 5-12.1C (Risk Management)
(v) DTRA FP Security Classification Guide (NOTAL) of Feb 01
(w) DOD Directive 2310.2 (NOTAL) of 30 Jun 97 (Personnel Recovery (PR))
(x) DOD Directive 1300.7 (NOTAL) of 8 Dec 00 (Training and Education to Support the Code of Conduct)
(y) DOD Instruction 1300.21 (NOTAL) of 8 Jan 01 (Code of Conduct (CoC) Training and Education)

INSPECTOR GENERAL'S 480 CHECKLIST

ANTITERRORISM/FORCE PROTECTION

480H01H000H

Installation/Unit Functional Areas

Function #	Reference #	Audit Statement
480H01H001H	MCO 3302.1D, Par. 4a(2)(a)	HAS THE INSTALLATION/UNIT DEVELOPED WITHIN IT'S AT/FP PLAN PRESCRIPTIVE MEASURES/ACTIONS TO SUPPLEMENT THE MINIMUM NUMBER OF DOD FPCON MEASURES/PROCEDURES?

Par. 4a(2)(a) Commanders at all levels are required to develop prescriptive AT/FP standards based on the type of unit, installation location, potential threat and operating environment. These standards shall include the minimum force protection condition (FPCON) measures listed in enclosure (7) as well as unit/installation threat specific FPCON measures.

480H01H002H	MCO 3302.1D, Par. 4a(2)(b)	DOES THE AT/FP PLAN CLEARLY DESCRIBE AT/FP OPERATIONAL RESPONSIBILITIES FOR ALL UNITS/INDIVIDUALS WHETHER PERMANENTLY OR TEMPORARILY ASSIGNED?

Par. 4a(2)(b) Commanders at all levels shall clearly establish AT/FP operational responsibility for all units and individuals whether permanently or temporarily assigned. When responsibilities for AT/FP overlap and are not otherwise governed by law, a specific DOD policy, or appropriate memorandum of agreement/memorandum of understanding (MOA/MOU), the geographic Combatant Commander's force protection policies will take precedence over all force protection policies or programs within the Combatant Commander's area of responsibility. Commanders in overseas locations shall coordinate their AT/FP efforts with the Combatant Commander, host-nation authorities, and the U.S. embassy as appropriate. Reference (c), DOD Antiterrorism Standards applies.

480H01H003H	MCO 3302.1D, Par. 4a(2)(b)	WHERE RESPONSIBILITIES FOR AT/FP OVERLAP, ARE THERE EXISTING MOUS/MOAS WITH LOCAL ORGANIZATIONS (I.G., FIRE, POLICE, MEDICAL) AS PART OF THE INSTALLATION AT/FP PLAN?

Par. 4a(2)(b) Commanders at all levels shall clearly establish AT/FP operational responsibility for all units and individuals whether permanently or temporarily assigned. When responsibilities for AT/FP overlap and are not otherwise governed by law, a specific DOD policy, or appropriate memorandum of agreement/memorandum of understanding (MOA/MOU), the geographic Combatant Commander's force protection policies will take precedence over all force protection policies or programs within

the Combatant Commander's area of responsibility. Commanders in overseas locations shall coordinate their AT/FP efforts with the Combatant Commander, host-nation authorities, and the U.S. embassy as appropriate. Reference (c), DOD Antiterrorism Standards applies.

480H01H004H	MCO 3302.1D, Par. 4a(2)(b)	IF INSTALLATION IS OVERSEAS, HAS THE COMMAND COORDINATED AT/FP EFFORTS AND PLAN WITH THE HOST NATION AND U.S. EMBASSY?

Par. 4a(2)(b) Commanders at all levels shall clearly establish AT/FP operational responsibility for all units and individuals whether permanently or temporarily assigned. When responsibilities for AT/FP overlap and are not otherwise governed by law, a specific DOD policy, or appropriate memorandum of agreement/memorandum of understanding (MOA/MOU), the geographic Combatant Commander's force protection policies will take precedence over all force protection policies or programs within the Combatant Commander's area of responsibility. Commanders in overseas locations shall coordinate their AT/FP efforts with the Combatant Commander, host-nation authorities, and the U.S. embassy as appropriate. Reference (c), DOD Antiterrorism Standards applies.

480H01H005H	MCO 3302.1D, Encl. (2) Par. 1c	HAS THE INSTALLATION/UNIT VULNERABILITY ASSESSMENT BEEN CLASSIFIED IN ACCORDANCE WITH THE DTRA CLASSIFICATION GUIDE?

Par. 1c Commanders shall conduct vulnerability assessments at least annually. Incoming commanders should acquire and familiarize themselves with the most recent vulnerability assessment available and conduct a new vulnerability assessment upon assumption of command. Assessments will be classified in accordance with the Defense Threat Reduction Agency (DTRA) Force Protection (FP) Security Classification Guide (NOTAL) of Feb 01.

480H01H006H	MCO 3302.1D, Encl. (2) Par. 2d	ARE VULNERABILITY ASSESSMENTS BEING CONDUCTED AT LEAST ANNUALLY AND DO VULNERABILITY ASSESSMENTS APPROPRIATELY REFLECT THE SPAN OF CONTROL OF THE COMMANDER?

Par. 2d Vulnerability self-assessments (local assessments) shall be conducted by all installations and units (squadron/battalion and above) at least once per year. A unit's AT/FP program should be subject to continual assessment to avoid complacency and to benefit from experience. It should also appropriately reflect the span-of-control of the commander and focus on critical items the commander may be able to influence. Evolving terrorism threats, changes in security technology, development and implementation of alternative concepts and changing local conditions make periodic assessments essential.

480H01H007H	MCO 3302.1D, Encl. (2) Par. 4	PRIOR TO DEPLOYMENT, HAS THE UNIT PERFORMED AN AT/FP PREDEPLOYMENT VULNERABILITY ASSESSMENT?

Par. 4 Pre-Deployment AT/FP Vulnerability Assessment. Pre-deployment AT/FP vulnerability assessments shall be conducted for all units prior to deployment. These assessments should form the basis for unit AT/FP plans as well as appropriate force protection measures to reduce risk and vulnerability. Assessment of unit vulnerabilities shall be subject to continual evaluation once deployed.

480H01H008H	MCO 3302.1D, Encl. (2) Par. 4b	HAS THE COMMANDER SUBMITTED A CBT RIF REQUEST FOR EMERGENT AT/FP REQUIREMENTS?

Par. 4b Deploying commanders shall utilize AT/FP measures to reduce risk and vulnerability before, during, and after deployment. If warranted, commanders faced with emergent AT/FP requirements prior to movement of forces should submit Combatting Terrorism Readiness Initiatives Fund requests in accordance with CJCS Instruction 5261.01A (NOTAL) of 1 Jul 01 to produce necessary materials or equipment for required protective measures. Assessments and implementation of standards should occur in a timely manner and should be incorporated in pre-deployment planning and training. Pre-deployment assessments should assist commanders in updating area of responsibility (AOR)-specific training and in obtaining necessary physical security materials and equipment. Coordination with the applicable Marine forces ATO is required.

480H01H009H	MCO 3302.1D, Encl. (3) Par. 1b	ARE TERRORISM THREAT ASSESSMENTS CONDUCTED ANNUALLY?

Par. 1b Commanders will prepare a terrorist threat assessment at least annually and for every overseas exercise/deployment that will identify the full spectrum of known or estimated terrorist capabilities including weapons and tactics. The threat assessment will integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources. This information shall be incorporated into the unit's antiterrorism/force protection awareness program.

480H01H010H	MCO 3302.1D, Encl. (3) Par. 4	ARE TERRORIST THREAT ASSESSMENTS THE BASIS FOR ASSESSING VULNERABILITIES, PLANNING AT PHYSICAL SECURITY MEASURES, AND JUSTIFYING AT ENHANCEMENTS AND BUDGET PROPOSALS?

Par. 4 Threat-Based Assessment. Department of Defense (DOD) Instruction 2000.16 (NOTAL) of 14 Jun, 2001, DOD Antiterrorism Standards, requires that AT programs be threat-based; that threat assessments of feasible terrorist capabilities be the basis for assessing vulnerabilities, planning AT physical security measures, and justifying AT enhancements and budget proposals.

480H01H011H	MCO 3302.1D, Encl. (3) Par. 4c	HAS THE THREAT MATRIX BEEN USED AS THE BASELINE THREAT FOR PLANNING PURPOSES?

Par. 4c The Threat Matrix, located at appendix (A) to enclosure (2), identifies a range of minimum terrorist threat capabilities and will be used as the baseline for planning purposes. Should the installation's threat analysis identify additional or greater threats, they will be added to the matrix.

480H01H012H	MCO 3302.1D, Encl. (3) Par. 6a	HAS THE NCIS BEEN ADEQUATELY USED TO ACQUIRE A TERRORIST THREAT ASSESSMENT?

Par. 6a The Naval Criminal Investigative Service (NCIS) is the Department of the Navy (DON) component with primary responsibility for law enforcement, counterintelligence (counter intelligence operations, and security policy matters). NCIS maintains a worldwide structure to ensure operational readiness of Marine Corps commands by preventing terrorist attacks against DON forces, protecting against compromise of DON sensitive info/systems, and reducing crime against the DON. To fulfill this responsibility, NCIS has established the Multiple Threat Alert Center (MTAC), which serves as the fusion point and production center within the DON for all terrorist, criminal, cyber, and counterintelligence information indicative of a threat to DON assets throughout the world. The MTAC processes real time information and operates on a 24-hour basis to provide commanders with a timely and common operational picture of security threats and vulnerabilities to reduce risks to Marine Corps forces and assets.

480H01H013H	MCO 3302.1D, Encl. (5) Par. 4a	BASED ON INFORMATION OBTAINED AND ANALYZED IN THE RISK ASSESSMENT HAVE POTENTIAL COUNTERMEASURES BEEN IDENTIFIED AND CONSIDERED?

Par. 4a Based on the information obtained and analyzed in the risk assessment, potential countermeasures to reduce vulnerabilities can be identified and considered. Countermeasures generally fit into one of the following five categories: intelligence, procedures, equipment, physical and manpower.

480H01H014H	MCO 3302.1D, Encl. (5) Par. 4c	HAVE PROCEDURES, PROCESSES, TRAINING AND MANPOWER BEEN UTILIZED TO THE FULLEST EXTENT POSSIBLE TO REDUCE VULNERABILITIES?

Par. 4c Commanders should ensure that appropriate procedures, processes, training and manpower (assets that are most readily available and normally offer the most immediate and least expensive remedy available to the commander) have been utilized to the fullest extent possible.

480H01H015H	MCO 3302.1D, Encl. (5) Par. 5c	HAS A MONITORING SYSTEM BEEN DEVELOPED TO DETECT CHANCES IN CRITICALITY OF ASSETS, THREATS, AND OR VULNERABILITIES THAT MIGHT CHANGE THE RISK ASSESSMENT?

Par. 5c Once the appropriate countermeasures have been selected and are in place, they must be tested and evaluated to ensure they are as effective as anticipated in the risk assessment. A monitoring system should be established to detect any

changes in criticality of assets, threats and/or vulnerabilities that might change the risk assessment.

480H01H016H	MCO 3302.1D, Encl. (7) Par. 1b	DOES THE AT/FP PLAN INCLUDE A PROCESS TO RAISE OR LOWER FORCE PROTECTION CONDITIONS?

Par. 1b Commanders at all levels will develop a process to raise or lower FPCONs. FPCON transition procedures and measures will be disseminated and implemented by subordinate commanders. Local commanders will develop measures to support transition between FPCONs.

480H01H017H	MCO 3302.1D, Encl. (7) Par. 2a	DOES THE AT/FP PLAN DESCRIBE THE SPECIFIC ACTION THAT WILL BE TAKEN TO IMPLEMENT EACH REQUIRED MEASURE?

Par. 2a The FPCON measures identified in this enclosure are the minimum measures that will be implemented by an installation when an FPCON is prescribed. Therefore, the installation AT/FP plan must describe the specific action that will be taken to implement each required measure. An effective means to perform this function is the development of synchronization matrices for each measure for FPCON NORMAL through DELTA; additional measures addressing weapons of mass destruction (WMD) may also be included. To make the matrix efficient, each measure must answer the questions of who, what, where, when, and how each measure is going to be implemented. In addition to the general increased protection afforded by implementing these measures, measures should be developed to, at a minimum, allow an installation to specifically detect, deter, defend, and defeat those weapons and tactics identified in the threat matrix. The implementation guidance provided by these measures will also serve as the basis for determining required resources to implement the plan and the cornerstone of the table topping and exercise programs. Two examples of FPCON synchronization matrices are shown in tables 7-1 and 7-2 of this enclosure.

480H01H018H	MCO 3302.1D, Encl. (7) Par. 2b	IF THE AT/FP PLAN CONTAINS SITE-SPECIFIC AT MEASURES LINKED TO FPCONS, IS THE AT/FP PLAN CLASSIFIED “CONFIDENTIAL” AT A MINIMUM?

Par. 2b An AT/FP plan with a complete listing of site-specific antiterrorism (AT) measures, linked to a Force Protection Condition, will be classified, as a minimum, CONFIDENTIAL. When separated from the AT/FP plan, specific AT measures and FPCONs remain unclassified but shall be handled as FOR OFFICIAL USE ONLY (FOUO) documents. Site-specific AT measures should be:

480H01H019H	MCO 3302.1D, Encl. (9) Par. 1a	DOES THE AT/FP PLAN CONTAIN PROCEDURES TO ENHANCE AT/FP PROTECTION; IDENTIFY REQUIREMENTS AND PROGRAM RESOURCES BASED ON KNOWN TERRORIST THREAT CAPABILITIES, VULNERABILITIES AND ASSESSMENTS.

Par. 1a General Development of Antiterrorism (AT) Standards. Commanders shall develop and maintain a comprehensive antiterrorism/force protection (AT/FP) program for personnel and assets for which they have AT/FP responsibility. At a minimum AT/FP programs will address the following general areas:

(1) Procedures will be developed to collect and analyze current terrorist threat information, threat capabilities, and vulnerabilities to terrorist attack.

(2) Terrorism threat assessment, vulnerability assessments, terrorist incident response measures, and terrorist consequence management measures.

(3) Plans and procedures to enhance AT/FP protection.

(4) Procedures to identify AT/FP requirements and program resources.

(5) Construction considerations.

(6) Exercise/deployment considerations.

480H01H020H	MCO 3302.1D, Encl. (9) Par. 1b	HAS THE INSTALLATION/UNIT (BATTALION/ SQUADRON LEVEL AND HIGHER) APPOINTED (IN WRITING) A QUALIFIED ORGANIZATION AT/FP OFFICER?

Par. 1b AT Officers (ATOs). ATOs, responsible to the commander, shall be assigned in writing and shall be trained in AT procedures in a formal Level II AT Training course. This may be an additional duty. Enclosure (11) identifies recommended training for assigned ATOs.

480H01H021H	MCO 3302.1D, Encl. (9) Par. 1c(1)	HAS THE INSTALLATION/UNIT ESTABLISHED AN AT/FP INFORMATION AND AWARENESS PROGRAM TO ENSURE ALL ASSIGNED PERSONNEL (MILITARY, CIVILIAN, AND DEPENDENTS) ARE AWARE OF THE GENERAL TERRORIST THREAT AND THE PERSONAL PROTECTION MEASURES THAT COULD REDUCE INDIVIDUAL VULNERABILITIES?

Par. 1c(1) Establish command AT/FP information and awareness programs to ensure all assigned and sponsored 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 taken and implemented. FMFM 7-14, MCRP 3-02E, MCO 3460.1A, MCI 02.10b, CJCS 5260 (NOTAL) of 1 Jan 97, DOD Directive 1300.7 (NOTAL) of 8 Dec 00, and DOD Instruction 1300.21 (NOTAL) of 8 Jan 01 will be used as guidance in developing these programs.

480H01H022H	MCO 3302.1D, Encl. (9)	HAVE ALL PERSONNEL PLANNING TO TRAVEL OUTSIDE THE CONTINENTAL U.S., REGARDLESS

	Par. 1c(1)(a) & Par. 1c(3)	OF THREAT LEVEL, RECEIVED PREDEPLOYMENT LEVEL I AT/FP TRAINING TO INCLUDE AN AOR/ COUNTRY SPECIFIC THREAT INFORMATION BRIEF?

Par. 1c(1)(a) At least annually, provide level I AT awareness training to all Marine Corps personnel and civilian employees if they are deployed or eligible for deployment or if the terrorism threat level within the U.S. and its territories rises above moderate. All active duty Marines will receive level I AT awareness training at least annually. Ensure all deploying Marines are level I qualified prior to overseas deployment. Enclosure (11) applies.

and

Par. 1c(3) Provide area of responsibility (AOR)/country specific threat information brief for all personnel planning to travel outside the U.S. regardless of threat level.

480H01H023H	MCO 3302.1D, Encl. (9) Par. 1c(1)(b)	DURING PERIODS OF ELEVATED THREAT CONDITIONS, HAS THE COMMAND ENSURED A COPY OF MCRP 3-02E "THE INDIVIDUALS GUIDE FOR UNDERSTANDING AND SURVIVING TERRORISM", OR AN ALTERNATIVE HANDOUT WAS DISTRIBUTED TO ALL PERSONNEL?

Par. 1c(1)(b) During periods of elevated threat conditions, issue a copy of MCRP 3-02E, The Individual's Guide for Understanding and Surviving Terrorism, or a handout containing essential information derived from that Order, to all personnel.

480H01H024H	MCO 3302.1D, Encl. (9) Par. 1c(2)	DOES THE INSTALLATION/UNIT AT/FP PLAN CONTAIN PROCEDURES TO IMMEDIATELY NOTIFY PERSONNEL IN CASE OF ACTUAL EMERGENCY IMPLEMENTATION AND/OR ELEVATION OF FPCONS?

Par. 1c(2) Develop a means of mass notification of unit and installation personnel of actual emergency or implementation of higher FPCONs via systems, methods, or alarms for potential emergencies. The systems, methods, or alarms used should possess a capability to immediately notify personnel of the emergency, should have their own set of reactions, and should be drilled frequently to familiarize all personnel with individual responsibilities and actions.

480H01H025H	MCO 3302.1D, Encl. (9) Par. 1d	HAVE THE VULNERABILITY OF PERSONNEL AND ASSETS TO TERRORIST USE OF WMD BEEN ASSESSED?

Par. 1d Weapons of Mass Destruction (WMD). Commanders will assess the vulnerability of personnel and assets for which they have AT responsibility to terrorist use of WMD including the use of chemical, biological, radiological and nuclear weapons, and high yield explosives (CBRNE). Assessments will address potential use of WMD as well as measures to protect and reduce vulnerability to terrorist use of WMD.

480H01H026H	MCO 3302.1D, Encl. (9) Par. 1e(5)	DO INSTALLATION/UNIT PLANS, PROCEDURES, ASSESSMENTS, AND TRAINING ADDRESS THE POTENTIAL THREATS TO INFORMATION SYSTEMS AND POTENTIAL USE OF WMD?

Par. 1e(5) Ensure plans, procedures, assessments, and training address potential threats to information systems and the potential use of WMD. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

480H01H027H	MCO 3302.1D, Encl. (9) 1e(7)	DOES THE INSTALLATION/UNIT AT/FP PHYSICAL SECURITY PLAN PROVIDE PROCEDURES TO REPORT TERRORIST, CRIMINAL OR OTHER INCIDENTS OR OBSERVATION OF PRE-OPERATIONAL ACTIVITIES TO HIGHER HEADQUARTERS?

1e(7) Contain procedures for notification of higher headquarters in the event of terrorist, criminal or other incidents or the observation of pre-operational activity (e.g., probing, surveillance, bomb threat) through appropriate channels (i.e., OPREP3/SIR, law enforcement, AT/FP working group, etc.) for follow on action.

480H01H028H	MCO 3302.1D, Encl. (9) Par. 1e(7)(a)	IS THE INSTALLATION/UNIT AWARE OF THE REQUIREMENT TO IMMEDIATELY NOTIFY THE SERVICING FIELD OFFICE OF THE FBI (IF THE INCIDENT OCCURS WITHIN THE U.S. OR POSSESSIONS) OR THE DEPARTMENT OF STATE (DOS) (IF INCIDENT OCCURS ON FOREIGN TERRITORY) VIA THE COMBATANT COMMANDER WHENEVER AN ACTUAL TERRORIST INCIDENT OCCURS?

Par. 1e(7)(a) Whenever an actual terrorist incident occurs, immediately notify the following agency (as appropriate):

1. If the incident occurs within the U.S. or its possessions, notify the servicing field office of the Federal Bureau of Investigation (FBI) and the Naval Criminal Investigative Service (NCIS).

2 If the incident occurs on foreign territory, notify the Combatant Commander who will in turn notify the Department of State (DOS) and host-nation (HN) authorities. Installation commanders will implement applicable provisions of the Status of Forces Agreement (SOFA) or other agreements between the HN and the U.S.

480H01H029H	MCO 3302.1D, Encl. (9)	DOES THE INSTALLATION/UNIT INCLUDE THE PUBLIC AFFAIRS OFFICER (PAO) IN ALL

	Par. 1e(8)	PLANNING, TRAINING, EXERCISES, AND OPERATIONAL ACTIVITIES RELATED TO TERRORIST EVENTS?

Par. 1e(8) Because incidents of terrorism generate considerable media interest, include the Public Affairs Officer (PAO) in all planning, training, exercises, and operational activities related to terrorist events. PAOs will be guided by chapter 5 and Appendix R of FMFM 7-14 (currently under review for publication as MCRP 3-02D) and Appendix 3 of DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism.

480H01H030H	MCO 3302.1D, Encl. (9) Par. 1g(1)	IF LOCAL INFORMATION INDICATES GAPS, HAS ADDITIONAL INFORMATION BEEN REQUESTED VIA APPROPRIATE INTELLIGENCE COLLECTION AND PRODUCTION CHANNELS?

Par. 1g(1) Where local information indicates gaps, additional information should be requested via the appropriate intelligence collection and production channels.

480H01H031H	MCO 3302.1D, Par. Encl. (9) Par. 1h	DOES THE UNIT'S AT/FP PHYSICAL SECURITY PLAN COMPLIMENT THE OVERALL INSTALLATION EFFORT?

Par. 1h Physical Security Measures. In order to ensure an integrated approach to AT/FP, tenant commanders must publish a physical security plan that encompasses measures to enhance security, especially during periods of heightened FPCONs, and compliments the overall installation effort. Where there are multiple commanders at an installation, the installation commander will be responsible for coordinating and integrating the various physical security measures into the AT/FP plan.

480H01H032H	MCO 3302.1D, Encl. (9) Par. 1h(2)	DOES THE INSTALLATION/UNIT PHYSICAL SECURITY AT/FP PLAN CONTAIN PROVISIONS FOR SECURITY OF MEVAS, INCLUDING USE OF PHYSICAL SECURITY EQUIPMENT, SECURITY PROCEDURES, RESPONSE FORCES, CRISIS/ CONSEQUENCE MANAGEMENT AND EMERGENCY RESPONSE?

Par. 1h(2) Plans shall identify and include provisions for the security of mission essential vulnerable areas (MEVAs) as identified in the criticality assessment, including use of physical security equipment, security procedures, response forces, crisis/consequence management and emergency response.

480H01H033H	MCO 3302.1D, Encl. (9) Par. 1h(4)	IS THE UNIT AN ACTIVE PARTICIPANT IN THE INSTALLATION PHYSICAL SECURITY COUNCIL/ INSTALLATION CRISIS MANAGEMENT TEAM?

Par. 1h(4) Major tenant commands shall actively participate in the installation physical security council and the installation crisis management team (CMT). FMFM 7-14 (currently under review for publication as MCRP 3-02D) applies.

480H01H034H	MCO 3302.1D, Encl. (9) Par. 1i(1) & Par. 2d	DOES THE INSTALLATION/UNIT MAINTAIN, AND AT A MINIMUM, REVIEW, UPDATE, AND EXERCISE THE PHYSICAL SECURITY/AT/FP PLAN(S) ANNUALLY?

Par. 1i(1) Commanders shall conduct field and staff AT/FP training exercises at least annually in order to familiarize personnel with the implementation of the AT/FP plan and to identify requirements and provide justification for budget requests for resources as necessary. AT/FP training shall include: AT/FP physical security measures, terrorist incident response measures and terrorist consequence management measures.

and

Par. 2d Conduct an AT/FP exercise at least annually to evaluate the installation's ability to counter or contain a terrorist threat.

480H01H035H	MCO 3302.1D, Encl. (9) Par. 1i(2)	HAS THE ORGANIZATION INTEGRATED TERRORISM SCENARIOS INTO PRE-DEPLOYMENT AND OTHER TRAINING EXERCISES THAT ARE OPERATIONAL IN NATURE AND AT A MINIMUM EVALUATE THE PROCEDURES PRIOR, DURING, AND SUBSEQUENT TO TERRORIST INCIDENTS?

Par. 1i(2) AT/FP training shall be incorporated into unit-level training plans and pre-deployment exercises. AT/FP training shall be evaluated by measurable standards that will include credible deterrence and response standards; deterrence specific tactics, techniques and procedures; terrorist scenarios and hostile intent decision-making. At a minimum these exercises should be operational in nature and should include the evaluation of:

(a) Procedures for collecting, analyzing and disseminating terrorist threat information.

(b) Procedures for analyzing threat capabilities, indications and warnings.

(c) Procedures for determining vulnerabilities to terrorist attack.

(d) Ability to deter incidents and enhance AT/FP protection through the dissemination and implementation of specific FPCON measures.

(e) Alarms and immediate action drills.

(f) Procedures for responding to, containing, mitigating, and recovering from the effects of terrorist incidents.

(g) Procedures for recognition, response, and reporting concealed improvised explosive devices (IEDs).

(h) At the conclusion of every AT/FP exercise, provide an after action report (AAR) for inclusion into the Marine Corps Lessons Learned System (MCLLS), per MCO 5000.17A.

480H01H036H	MCO 3302.1D, Encl. (9) Par. 1i(2)(h)	AT THE CONCLUSION OF EVERY AT/FP EXERCISE,HAS THE INSTALLATION/ UNIT PROVIDED AN AFTER ACTION REPORT (AAR) FOR INCLUSION IN THE MCLLS?

Par. 1i(2)(h) At the conclusion of every AT/FP exercise, provide an after action report (AAR) for inclusion into the Marine Corps Lessons Learned System (MCLLS), per MCO 5000.17A.

480H01H037H	MCO 3302.1D, Encl. (9) Par. 1i(3)	ARE RECORDS OF AT/FP TRAINING EXERCISES MAINTAINED FO AT LEAST ONE YEAR?

Par. 1i(3) Records of AT/FP training exercises shall be maintained for 1 year.

480H01H038H	MCO 3302.1D, Encl. (9) 1i(5)	ARE AT/FP PLANNING/MEASURES INCLUDED IN OPERATIONS ORDERS FOR PERMANENT/ TEMPORARY OPERATIONS AND EXERCISES?

Par. 1i(5) AT/FP plans shall be included in operations orders for permanent and temporary operations and exercises.

480H01H039H	MCO 1510.114	HAS THE INSTALLATION/UNIT INCORPORATED INDIVIDUAL TRAINING STANDARDS FOR AT/FP (MCO 1510.114) WITHIN THE COMMAND TRAINING PROGRAM AS THE BASIS FOR INDIVIDUAL TRAINING?

Installation Functional Areas

480H01H040H	MCO 3302.1D, Encl. (9) Par. 1k(1)	DOES THE INSTALLATION PROVOST MARSHAL OR OTHER COMPETENT AUTHORITY REVIEW INSTALLATION PLANNING AND DESIGN OF MILITARY CONSTRUCTION (MILCON) AND SPECIAL PROJECTS TO ENSURE THAT AT/FP PROTECTIVE FEATURES AND OTHER PHYSICAL SECURITY MEASURES ARE INCLUDED?

Par. 1k(1) Whenever possible incorporate AT/FP considerations into planning for new construction, renovation and rehabilitation to mitigate AT/FP vulnerabilities and terrorist threats. Ensure that AT/FP protective features and other physical security measures are included in the planning and design of military construction (MILCON) and special projects. The installation provost marshal or other competent authority shall review all MILCON, facility modifications, and special projects.

480H01H041H	MCO 3302.1D, Encl. (9)	HAS THE INSTALLATION ESTABLISHED AN INSTALLATION PHYSICAL SECURITY COUNCIL

	Par. 2a(1)	THAT CONVENES AT LEAST QUARTERLY, WITH MEMBERSHIP FROM MAJOR SUBORDINATE ACTIVITY REPRESENTATIVES AND KEY MEMBERS OF THE INSTALLATION STAFF?

Par. 2a(1) Establish and organize the installation physical security council, per MCO P5500.13A. The council assists the commander in gaining full community involvement and support in the planning for terrorist and other critical incidents. Membership should include major subordinate activity representatives and key members of the installation staff (such as the comptroller, staff judge advocate, provost marshal, operations security (OPSEC) personnel, intelligence officer and/or NCIS Resident Agent (NCISRA), medical representative, public affairs officer, logistics officer, and facilities engineer, and others). The physical security council shall be convened at least quarterly.

480H01H042H	MCO 3302.1D, Encl. (9) Par. 2a(2)	DOES THE INSTALLATION PHYSICAL SECURITY/ AT/FP PLAN INCLUDE ANNEXES FOR CRISIS/ CONSEQUENCE MANAGEMENT, BARRIERS, RANDOM ANTITERRORISM MEASURES (RAM), COUNTERSURVEILLANCE, OTHER TENANT PLANS AND CONTINGENCY PLANS AS REQUIRED BY UNIQUE LOCAL CONDITIONS?

Par. 2a(2) Contain a crisis/consequence management annex, barrier annex, countersurveillance annex, RAM annex, tenant unit plans and other contingency plans or annexes required by unique local conditions.

480H01H043H	MCO 3302.1D, Encl. (9) Par. 2a(3)	DOES THE INSTALLATION HAVE AN ESTABLISHED CRISIS MANAGEMENT TEAM THAT WILL BE ABLE TO COORDINATE THE INSTALLATION'S RESPONSE TO AND RECOVERY FROM A VARIETY OF CRITICAL INCIDENTS, INCLUDING TERRORISM?

Par. 2a(3) Establish an installation crisis management team (CMT), per FMFM 7-14 (currently under review for publication as MCRP 3-02D). The CMT coordinates the installation's response to and recovery from a variety of critical incidents, including terrorism. It identifies infrastructures and key assets critical to the installation's operation (e.g., MEVAs). The CMT and physical security council may be combined.

480H01H044H	MCO 3302.1D, Encl. (9) Par. 2a(3)(a)	HAVE MOA BEEN ESTABLISHED WITH LOCAL, STATE, FEDERAL, AND FOREIGN AUTHORITIES ON MATTERS PERTAINING TO A COORDINATED RESPONSE TO SECURITY THREATS, EMERGENCY MEDICAL RESPONSE, "POSSE COMITATUS' RESTRICTIONS, AND OTHER MUTUAL PHYSICAL SECURITY AND LOSS PREVENTION ISSUES.

Par. 2a(3)(a) Maintain liaison with local, state, Federal, and foreign authorities. As applicable, memorandum of agreement/memorandum of understanding (MOA/MOU) shall be established on matters pertaining to a coordinated response to security threats, emergency medical response, communications interface with

cooperating agencies, intelligence sharing, "posse comitatus" restrictions, and other mutual physical security and loss prevention issues.

480H01H045H	MCO 3302.1D, Encl. (9) Par. 2a(4)	IS THE INSTALLATION CRISIS MANAGEMENT FORCE ESTABLISHED, TRAINED, AND UNDER THE OPERATIONAL CONTROL OF THE PROVOST MARSHAL?

Par. 2a(4) Establish and train an installation crisis management force (CMF), per FMFM 7-14 (currently under review for publication as MCRP 3-02D). The CMF provides an organic response capability for crisis situations and falls under the operational control of the installation provost marshal.

480H01H046H	MCO 3302.1D, Encl. (9) Par. 2a(5)(b)	HAS THE INSTALLATION PROVIDED FOR SPECIALIZED EQUIPMENT TO COMBAT THE TERRORIST THREAT?

Par. 2a(5)(b) Provide for specialized equipment to combat the terrorist threat, such as SRT equipment, lights/mirrors for vehicle undercarriage inspections, portable metal detectors, and similar devices.

480H01H047H	MCO 3302.1D, Encl. (9) Par. 2a(6)	ARE INSTALLATION FIRST RESPONDERS (MILITARY POLICE, FIRE, MEDICAL PERSONNEL) TRAINED AND EQUIPPED TO RESPOND TO BOTH CONVENTIONAL AND WMD TERRORIST ATTACK?

Par. 2a(6) First responders (military police, fire, and medical personnel) shall be trained and equipped to respond to both conventional and WMD attack.

480H01H048H	MCO 3302.1D, Encl. (9) Par. 2a(7)	DOES THE INSTALLATION PHYSICAL SECURITY/ AT/FP PLAN CONTAIN RESPONSE PROCEDURES TO A VARIETY OF TERRORIST AND OTHER CRISIS INCIDENTS (E.G., HOSTAGE/BARRICADE, BOMB THREAT, KIDNAPPING, SABOTAGE, ENVIRONMENTAL DISASTERS, MASS CASUALTY RESPONSE, WEAPONS OF MASS DESTRUCTION, ETC.)?

Par. 2a(7) Contain response procedures for a variety of terrorist and other crisis incidents (e.g., hostage/barricade, bomb threat, kidnapping, sabotage, environmental disasters, mass casualty response, weapons of mass destruction etc.) JPUB 3-07.2 of 17 Mar 98, FMFM 7-14 (currently under review for publication as MCRP 3-02D), and enclosure (8) apply.

480H01H049H	MCO 3302.1D, Encl. (9) Par. 2a(8)	DOES THE INSTALLATION PHYSICAL SECURITY/ AT/FP PLAN CONTAIN PROCEDURES TO PROVIDE ENHANCED AT/FP PROTECTION FOR AREAS OF HIGH POPULATION DENSITY?

Par. 2a(8) Contain procedures to provide enhanced AT/FP protection for areas of high population density.

480H01H050H	MCO 3302.1D, Encl. (9) Par. 2b(1)	IF IN A SIGNIFICANT OR HIGH THREAT LEVEL AREA, HAS A PHYSICAL SECURITY REVIEW OF OFF-INSTALLATION HOUSING BEEN CONDUCTED?

Par. 2b(1) Periodic physical security reviews of off-installation housing shall be conducted in significant and high threat level areas. Commanders shall provide AT/FP recommendations to residents and facility owner, facilitate additional mitigating measures, and, as appropriate, recommend to appropriate authorities the construction or lease of housing on an installation or in safer areas.

480H01H051H	MCO 3302.1D, Encl. (9) Par. 2b(3)	IS PRIVATE RESIDENTIAL HOUSING COVERED IN THE AT/FP PLAN WHERE IT MUST BE USED IN MODERATE, SIGNIFICANT, OR HIGH THREAT LEVEL AREAS?

Par. 2b(3) Commanders shall include coverage of private residential housing in AT/FP plans where private residential housing must be used in moderate, significant, or high threat level areas.

480H01H052H	MCO 3302.1D, Encl. (9) Par. 2b(5)	DO TERRORISM INCIDENT RESPONSE PLANS CONTAIN CURRENT RESIDENTIAL LOCATION INFORMATION FOR DOD PERSONNEL AND THEIR DEPENDENTS ASSIGNED TO MODERATE, SIGNIFICANT, OR HIGH TERRORISM THREAT LEVEL AREAS?

Par. 2b(5) Ensure terrorism incident response plans contain current residential location information for all DOD personnel and their dependents assigned to moderate, significant or high terrorism threat level areas. Such plans should provide for enhanced security measures and/or possible evacuation of DOD personnel and their dependents. DOD Handbook 2000.12-H (NOTAL) of 19 Feb 93, Protection of DOD Personnel and Assets from Acts of Terrorism, applies.

480H01H053H	MCO 3302.1D, Encl. (9) Par. 2d	HAS THE INSTALLATION CONDUCTED AN AT/FP EXERCISE WITHIN THE PREVIOUS 12 MONTHS WHICH TESTS THE INSTALLATION'S ABILITY TO COUNTER, CONTAIN, AND/OR MITIGATE A TERRORIST THREAT AS PER THE REFERENCE?

Par. 2d Exercises and Training. Conduct an AT/FP exercise at least annually to evaluate the installation's ability to counter or contain a terrorist threat.

480H01H054H	MCO 3302.1D, Encl. (9) Par. 3a	IF APPLICABLE, HAS A FLIGHT LINE SECURITY PROGRAM BEEN ESTABLISHED ASSIGNING FLIGHT LINE SECURITY PRIORITIES BASED ON THE THREAT LEVEL AND THE NATURE OF ASSETS

BEING PROTECTED?

Par. 3a Assign flight line security (FLS) priorities based on the threat level and the nature of assets being protected. The FLS Program was established to increase the level of physical security of assets within the flight line restricted area through systematic employment of security personnel and equipment designed to detect, delay, and/or deny access to unauthorized personnel. The level of security inherent at the installation determines the extent of the FLS effort required, and must be considered when distributing resources for the execution of the FLS program, as per MCO 5500.14A

480H01H055H	MCO 3302.1D, Encl. (2) Par. 3b	WHEN THE INSTALLATION CONDUCTS ITS ANNUAL COMMAND VULNERABILITY ASSESSMENT DOES IT USE THE INTEGRATED TEAM APPROACH?

Par. 3b Team composition and level of expertise must support the assessment of functional areas described above. Team members shall have expertise in the following areas: physical security; civil, electrical or structural engineering; special operations; operational readiness; law enforcement; medical operations; infrastructure; intelligence/counterintelligence; and consequence management. Commanders may tailor team composition and scope of the assessment but must meet the intent of providing a comprehensive assessment.