

measures must be fiscally achievable. Given limited resources and budgetary constraints, ATOs should provide commanders with alternatives for timely, cost-effective AT resources that still permit the successful execution of the AT plan. Additionally, ATOs should determine the staffing, operations, training, and equipment needed at all FPCONs. It is essential that the on hand resources and mitigation measures applied meet the minimum security requirements for baseline FPCON procedures.

1. Cost-Benefit Analysis. ATOs need to employ cost-benefit analysis twice in the risk management and resource management process: first, during consideration of executable mitigation measures with available resources; and second, in prioritizing resource requirements in an ATWG forum with other program managers. Cost-benefit analysis is an analytical tool used to weigh the total expected costs against the total expected benefits of one or more actions in order to choose the most effective option. For AT, the cost should include more than monetary and resource expenses; it should also incorporate the reduction of risk from implementing the measure in the near term and the long term through the Planning, Programming, Budgeting and Execution System (PPBES). The residual risk from one measure should be compared to the residual risk of other potential mitigation measures to help determine which measures will provide the greatest impact. Employing a comprehensive cost-benefit analysis of each potential mitigation measure will assist the Commander with managing risk and prioritizing funding requests.

9002. DOCUMENTING RESOURCE REQUIREMENTS. Once the resources needed to execute an AT plan are determined, an ATO must formally document those needs based on DOD and USMC benchmark requirements as justification to initiate the funding process. ATOs must understand that Financial Managers and their PPBES products are sensitive but not classified. While their CVAMP entries documenting vulnerabilities and observations and their readiness assessments in DRRS address risk related resource requirements, discussion of criticality, vulnerability, and consequences are classified and cannot be used in funding requests. ATWG discussions with other program managers and the financial manager can refer to these in a classified environment, but unfunded requirement documents should contain only the Commander's priority for resourcing. Formally, continuously, and clearly documenting the resource requirements and maintaining records of those requirements at every level of command is crucial to compete successfully for AT funding and to

leverage supplemental funding available on short notice. A well defined and standardized resourcing process at the MARFOR level allows for installations and units to articulate, track, and defend AT requirements as they compete for funding. Writing a strong justification is important for securing AT funding. Often, the omission or poor quality of the justification and impact statement is the principal cause for losing budget battles. AT resource requirements at the unit and installation level should be documented using a prescribed Excel spreadsheet format. It is important that MEF and MCI ATOs work closely with their Financial Managers to provide all pertinent data identifying the specific resources needed and the fiscal codes used to program funding and track budget execution. Spreadsheets or databases should include the following information: project number (from ESSIMS, 1391s, etc.), installation/unit, MCI/MARFOR, appropriation type, Commander's priority, requirement title, requirement description (equipment, personnel, or management and planning), type, and fiscal codes (AGSAG, MCPC, PE, PEN, BEA, BESA, etc.). Chapter 16, section 3 of Department of Defense (DoD) O-2000.12-H provides additional information on how to correctly document AT resource requirements.

9003. PRIORITIZING RESOURCE REQUIREMENTS. Once requirements have been generated and documented, ATOs and the ATWG should analyze the justification data (threat, vulnerabilities, asset criticality, AT program effectiveness, and Commander's risk) and prioritize requirements based on the most critical and important needs. Resources required to mitigate a major or high-risk situation should be given priority. Emphasis should be placed on acquiring resources that deter, detect, and defend against threats from an area of significant importance. Additionally, priority should be given to resource requirements needed to meet minimal security standards and to adhere to Marine Corps directives, standards, instructions, or regulations.

While prioritizing resource requirements, ATOs and the ATWG should place each requirement in one of four categories of importance: 1) critical, 2) high priority, 3) medium priority, and 4) low priority.

1. A critical-priority resource should include the majority of these criteria: a serious threat, an asset that is critical to the continuity of essential military missions, major vulnerabilities, and a lack of resources to execute baseline FPCON measures. A critical-priority resource addresses an

unacceptable risk and is in the top 20% of the commander's funding priorities.

2. A high-priority resource does not need to address every criterion, but should include the majority of these criteria: a serious threat, an asset that is critical to the mission, major vulnerabilities, and a lack of resources to execute baseline FPCON measures. A high-priority resource usually addresses an unacceptable risk and is in the top 21-40% of funding priorities.

3. A medium-priority resource does not need to address every criterion, but should include the majority of these criteria: a moderate to high threat, an asset that is moderately critical to the mission, moderate vulnerabilities, and resources that may be needed to execute elevated FPCON measures. A medium-priority resource usually addresses a considerable risk.

4. A low-priority resource does not need to address every criterion, but should include the majority of these criteria: all threat levels, an asset that is important to the mission, less significant vulnerabilities, and resources that would enhance/improve an AT program. A low-priority resource usually addresses a low risk.

9004. FUNDING RESOURCES. Once requirements are generated, documented, and prioritized, a realistic and affordable budget and procurement strategy should be developed. Budget planning should capture all life-cycle costs, including staffing needs, logistics, maintenance, and replacement costs. Before the unit or installation Financial Managers and program managers submits Marine Corps Operations and Maintenance (OOMC) resource requirements to their Higher Headquarters as unfunded requirements, the Commander will determine if the resource can be funded locally. If funding is not OMMC or is OMMC and cannot be reallocated internally, the chain of command will submit the appropriate documentation to compete for funding from the appropriate funding source.

1. Planning, Programming, Budgeting, and Execution System (PPBES). PPBES is the business process of allocating resources within the DoD. The PPBES is a cyclic process that provides the mechanisms for decisionmaking and the opportunity to reexamine previous decisions in light of changes in the environment (e.g., evolving threat, changing economic conditions). The ultimate objective of the PPBES is to provide COCOMs with capabilities

that include the best mix of forces, equipment, and support attainable within established fiscal constraints to accomplish their mission. It is important for Program Managers and their staff to be aware of the milestones for the Financial Managers during the PPBE process to ensure critical information is provided at the appropriate time to the appropriate agencies for both programming future funding and executing the budget. Failing to provide punctual information during the PPBE process will result in the loss of potential funding. Planning and programming resources is done through the Program Objective Memorandum (POM) process and budgeting and execution is done in the execution of the Five Year Development Plan (FYDP)+.

a. The POM process is the primary method of programming resources. The POM process does not address the current year funding; rather, it addresses the programming of funding execution 2 years in advance of the current FYDP. For example, planning and submission for POM 12 is done in FY10. POM submissions are evaluated by different Program Evaluation Boards (PEBs) for each type of appropriation.

(1) The Installation PEB evaluates POM nominations for the installation Marine Corps Program Codes (MCPCs) such as MCPC 630104 Security. POM nominations are submitted by the MARFOR level G8 and or the appropriate HQMC Program Manager.

(2) Construction requirements associated with installation perimeter security requirements are submitted by the G4 Facilities Engineers either as a Facilities, Sustainment, Restoration and Modernization (FSRM) or MILCON request.

(3) Procurement funding is done exclusively by MARCORSYSCOM, but submitted by Program Managers in Marine Corps Combatant Development Command (MCCDC) or by PP&O PSM for ESS requests. Resource requirements for ESS are submitted through the ESSIMS portal and PSM prepares POM initiatives based on those needs. The other way to POM for material solutions for new capabilities is the Universal Needs Statement submitted to MCCDC. Non-material capability documentation to recognize and resource staff structure, for example, would also be worked through MCCDC.

b. It is the responsibility of the ATO as a subject matter expert to properly document the basis of justification and articulate the specifics and criticality of the requirement to other program managers, the financial manager, and the

commander. Failure to do so will show lack of program prioritization, thus dismissing the need for funding.

c. A completed Universal Needs Statement (UNS) is the most important information component in the Expeditionary Force Development System (EFDS) and is a component of the planning and programming element of PPBES. As the primary means of entry into the EFDS, the UNS acts as a "work request" for current and future capabilities within the EFDS. The UNS identifies operational enhancement opportunities and deficiencies in capabilities. Opportunities include new capabilities, improvements to existing capabilities, and elimination of redundant or unneeded capabilities. "Universal" highlights its common use by any Marine Corps organization to capture both current needs and future needs developed through analysis, assessment, and experimentation with future warfighting concepts.

2. Current Year Funding Sources. There are three sources for current year funding for existing, emergent, and emergency resource requirements: the Combating Terrorism Initiative Fund (CbT-RIF), the Combatant Commander Initiative Fund (CCIF), and supplemental funding obtained through the budget execution process at the MARFOR level or HQMC.

a. Combating Terrorism Readiness Initiative Fund (CbT-RIF). CbT-RIF is an emergency funding line designed for emergent high-priority CbT requirements. This line of funding provides Combat Commanders the flexibility to react to unforeseen requirements from changes to threat levels, terrorist threats, and force protection doctrine/standards, as well as unanticipated requirements as a result of vulnerability assessments, tactical operations, and execution of AT plans. CbT-RIF can be used to fund maintenance costs for CbT-RIF-funded items during the year of purchase and the subsequent year as a stop-gap measure to allow the Marine Corps adequate time to program life-cycle costs if maintenance funds are not programmed and provided by the Marine Corps. The funds do not subsidize ongoing projects, supplement budget shortfalls, or support routine activities. CbT-RIF funds are not used to fund weaponry, ammunition, military table of organization and equipment, or table of distribution and allowances equipment normally acquired through Marine Corps logistics channels.

(1) Emergent requirements are typically the result of a change in mission, policy, or threat, or from a vulnerability

assessment that is less than 2 years old. For emergent requirements, the requestor must have an approved, executable, and exercised AT plan before submitting a CbT-RIF request unless the plan is not executable because of the requested item. As the foundation for determining AT requirements, the AT plan is a prerequisite for an emergent CbT-RIF request.

(2) The Joint Staff (DD AT/HD) is the steward of this funding line. Combatant Commands must validate and forward CbT-RIF requests to the Joint Staff/J-3, Deputy Director of Antiterrorism/Homeland Defense (DDAT/HD), AT/FP Division, in accordance with CbT-RIF submission, approval, and reporting procedures. CJCSI 5261.01E provides more information on CbT-RIF submission, approval, and reporting procedures.

(3) CVAMP is a web-enabled application residing within ATEP on AKO that captures results of vulnerability assessments, prioritizes Area of Responsibility (AOR) observations, identifies deficiencies, and lists corrective actions needed or completed. CVAMP allows ATOs to submit and track UFRs associated with CbT-RIF requests. Before submitting a CbT-RIF request via CVAMP, justification information must be provided, the Combatant Commander or Deputy Combatant Commander must approve the request, and it must be coordinated through the Combatant Command Comptroller and legal counsel. Capability gaps in protection of the force documented during Vulnerability Assessments are entered by the unit or installation in the Core Vulnerability Assessment Management Program (CVAMP). Those critical requirements that meet CbT-RIF guidelines can be submitted to COCOMs to compete for current year Joint Staff funding with an Unfunded Requirement (UFR). More information on CVAMP, including official briefings, reference materials, and training materials, can be found on ATEP on AKO.

b. Urgent Universal Needs Statement (UUNS). An accelerated UNS is known as an Urgent UNS. An UUNS submitted to MCCDC is another means to seek current year funding for capability gaps that threaten mission accomplishment or pose a life threatening condition. The nature of the UUNS process is to provide rapid acquisition of a capability to meet an urgent requirement in support of combat and contingency operations that threatens mission accomplishment or is life-threatening.

c. Combatant Commander (COCOM) Initiative Fund (CCIF). The primary focus of the CCIF is to support unforeseen contingency requirements critical to Combatant Commands' joint warfighting

readiness and national security interests. The strongest candidates for approval are initiatives that support Combatant Command activities and functions, enhance interoperability, and yield high benefits at a low cost. The funds do not subsidize ongoing projects, supplement budget shortfalls, or support routine activities. Initiatives submitted for funding under CCIF must fall under one of the following authorized activities: joint exercises and force training, contingencies and selected operations, civil and humanitarian assistance, command and control, military education and training, or personnel expense of defense personnel for bilateral or regional cooperation programs.

d. Current Year Deficiency Requests. Units and installations should also prepare Current Year Deficiency (CYD) requests to fund critical and high priority resource requirements.

3. Material Weakness Report. A process must be maintained through audits, investigations, and management control evaluations to identify, report, and correct material weaknesses. Weaknesses may be classified as deficiencies that significantly impair the execution of a mission or objective, deprive personnel of needed services or resources, violate requirements, weaken safeguards, or mismanage funds and assets.

4. Marine Corps Systems Command (MARCORSYSCOM). MARCORSYSCOM is the Commandant of the Marine Corps principal agent for acquisition and sustainment of systems and equipment used by the operating forces to accomplish their warfighting mission. MARCORSYSCOM controls procurement funding. MARCORSYSCOM works to provide quality systems and equipment to the operating forces, then expertly manages the systems and equipment during their entire life cycle. MARCORSYSCOM employs several AT technology systems.

a. Research, Development, Test, and Evaluation (RDT&E). RDT&E provides for the modernization and production of improved technologies, weaponry, and defense systems. The goal of RDT&E is to ensure and maintain a technological advantage over potential adversaries. RDT&E work for the Marine Corps is conducted at several locations, including the Office of Naval Research (ONR), Marine Corps Warfighting Laboratories (MCWL), Space and Naval Warfare Systems Command (SPAWAR), the Naval Surface Warfare Center (NSWC) Dahlgren, and the Technical Support Working Group (TSWG).

(1) Office of Naval Research (ONR). ONR "coordinates, executes, and promotes the science and technology programs of the United States Navy and Marine Corps through schools, universities, government laboratories, and nonprofit and for-profit organizations. It provides technical advice to the Chief of Naval Operations and the Secretary of the Navy and works with industry to improve technology manufacturing processes." Additional information on ONR can be found at <http://www.onr.navy.mil/>.

(2) Marine Corps Warfighting Laboratory (MCWL). MCWL, originally known as the Commandant's Warfighting Laboratory, was established in 1995. Located in Quantico, VA, MCWL is part of the Marine Corps Combat Development Command. Its purpose is to improve current and future naval expeditionary warfare capabilities across the spectrum of conflict for current and future operating forces. Additional information on MCWL can be found at <http://www.mcwl.usmc.mil/>.

(3) Space and Naval Warfare Systems Command (SPAWAR). SPAWAR's mission is to invent, acquire, develop, deliver, and support integrated and interoperable Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); business IT; and space capabilities in the interest of national defense. SPAWAR conducts field activities in Charleston, New Orleans, Norfolk, and San Diego, and in coordination with the National Reconnaissance Office. Additional information on SPAWAR can be found at <http://enterprise.spawar.navy.mil/>.

(4) Naval Surface Warfare Center (NSWC) Dahlgren. NSWC Dahlgren's mission is to provide research, development, test and evaluation, analysis, systems engineering, integration, and certification of complex naval warfare systems related to surface warfare, strategic systems, and combat and weapons systems associated with surface warfare. In addition, NSWC provides system integration and certification for weapons, combat systems, and warfare systems. NSWC's expertise extends to homeland and force protection. Their homeland and force protection division has an Infrastructure Assurance Program that identifies domestic assets crucial to support DoD, and assesses and remedies their vulnerabilities. Additional information on the NSWC can be found at <http://www.nswc.navy.mil/>.

(5) Technical Support Working Group (TSWG). TSWG is the national interagency research and development program for combating terrorism requirements at home and abroad. TSWG operates under the Combating Terrorism Technology Support Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities. TSWG works closely with many agencies to provide products that address blast effects and mitigation; CBRNE countermeasures; explosive detection; improvised device defeat; investigative support and forensics; physical security; surveillance, collection, and operations support; tactical operations support; training technology development; and VIP protection. Additional information on TSWG can be found at <http://www.tswg.gov/>.

9005. TYPES OF APPROPRIATIONS.

1. Appropriations.

a. Operations and Maintenance (O&M). Generally, O&M funds are used to predeploy, deploy, and redeploy. These funds are used to purchase fuel, barriers, forklifts, bulldozers, sensors, and warning equipment; pay utility bills; hire custodial services; etc. The Marine Corps is authorized to use annual O&M funds for construction projects costing less than \$750,000 (\$1.5 million to correct a life-threatening condition or for new construction and \$3 million for maintenance and repair of existing facilities).

b. Procurement. Procurement is a 3-year appropriation that finances the purchase of weapons, tracked combat vehicles, guided missiles and equipment, communications and electronic equipment, support vehicles, and contracts. Procurements made with nonappropriated funds should aid in obtaining products and services through purchasing and contracting operations. Items purchased with procurement funds are investment items subject to the limitations of the current expense/investment threshold.

c. Military Construction (MILCON). MILCON funds are obtained through a formal process using DD Form 1391 and must be approved by Congress under applicable procedures. These funds are used to prepare ground for construction; purchase bricks, mortar, concrete, and other construction materials; and pay construction labor, crane rental, and other expenses related to the construction of buildings, locks, dams, and roadways.

2. Supplemental. Supplemental appropriations generally fund emergencies deemed too urgent to be postponed for financing by other funds.

a. Global War on Terrorism (GWOT). GWOT funding aims at providing resources and equipment to ensure U.S. military forces can successfully carry out appropriate missions, build efforts to train proper foreign military units, and promote national reconciliation and economic growth.

9006. RESOURCE APPLICATION SUPPORT. Throughout the resource application process, an ATO should work closely with the comptroller. Comptrollers acquire, control, and certify funds in accordance with fiscal law. They are the only individuals who can legally certify and deliver funds for payment to a vendor. As the ATO works to articulate and justify the requirements, the comptroller is responsible for identifying the correct appropriation and funding amounts and submitting the funding requirement at the appropriate time to the organization responsible for funding the requirement.

a. Legal/Staff Judge Advocate (SJA). When seeking funding for a particular project, an ATO should obtain advice and assistance from the servicing command or SJA on appropriate funding sources for the current and coming year, as well as any fiscal or legal restraints on the proposed project. Advice from the SJA should complement, not replace, an ATO's collaboration with the Comptroller.

b. Contracting. As unit personnel make plans for any operation, competing requirements make demands on limited resources. A shortage of resources generally results in a need for some form of contracting to meet a mission and fulfill necessary requirements. The joint mission of resource management and contracting is to fairly allocate scarce resources across a theater of operations. With command approval, resource management allocates funds to contracting, enabling it to obtain those supplies, services, and construction that a unit does not currently possess but must have to perform its mission.

CHAPTER 10
PROGRAM REVIEW

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	1010	10-1
STANDARDS AND BENCHMARKS.....	1011	10-1

CHAPTER 10

PROGRAM REVIEW

1010. GENERAL. Successful AT programs hinge on a collective, proactive effort focused on sustaining the Marine Corps mission through prevention, detection, and preparation for any incident. In order for AT programs to be successful, comprehensive AT program review assessments must be conducted that comply with Department of Defense (DoD), and Marine Corps standards and benchmarks. Comprehensive program reviews evaluate the effectiveness and adequacy of AT plans and AT program implementation. They are vital to maintaining the cyclical and progressive nature of an AT program. Without comprehensive program reviews, AT programs suffer from complacency and stagnancy, which are serious flaws when trying to combat a constantly evolving terrorist threat. In compliance with one of the five mandatory AT program elements, all AT program areas must be reviewed annually. Marine Corps installations and units should define a process to conduct comprehensive program reviews and designate a specific individual to lead program review teams. Program review teams should include a sufficient number of individuals with functional expertise to successfully evaluate an AT program. This chapter describes the standards and benchmarks that are the foundation of an AT program and, consequently, that are used to conduct program reviews.

1. Frequency of Program Reviews. Subordinate commands must undergo an external AT program review at least once every 3 years. Triennial AT program reviews are intended to identify and address AT program deficiencies and vulnerabilities. Commanders at all levels will review their own AT Program and supporting plans, including special event plans, at least annually to ensure compliance with HHQ directives and to continuously improve their AT Program. For the same purpose, commanders at all levels will likewise conduct a documented compliance review of the AT Programs and supporting plans of their immediate subordinates within the chain of command, at least annually.

1011. STANDARDS AND BENCHMARKS. Numerous standards and benchmarks are available to assist key personnel with the development of a sound AT program. An AT program should be reviewed against the following standards and benchmarks:

1. Marine Corps Mission Assurance Assessment Program (MCMAAP). HQMC PSM, PP&O Security (PS) Division, established the MCMAAP for execution of higher headquarters (HHQ) assessments of mission assurance program elements of Marine Corps Bases, Stations, Camps AND Facilities. IAW HQMC PP&O PS implementation of the mission assurance all hazards concept, a HQMC Mission Assurance Assessment Team (MAAT) has been established to expand and standardize assessments across all elements of mission assurance.

a. Mission Assurance Assessments, (MAA) will be conducted on all Marine Corps Bases, Stations, Camps AND Facilities triennially, using the established MCMAAP standards and benchmarks. Responsibility and authority to conduct mission assurance assessments are assigned as follows:

1. HQMC PSM, PP&O Security (PS) Division, the office of primary responsibility (OPR), will be the responsible authority for conducting MAA on all Marine Corps bases, stations, camps and facilities.

2. Each MARFOR AND MARCORBASE, shall be the responsible authority for coordination and scheduling of triennial MAA for all assigned major subordinate commands within their area of command responsibility and operations. Coordination shall include geographical COCOMs to ensure their equities are considered.

3. Marine Corps installations, facilities, and stations will coordinate with all tenant commands to ensure their full participation in the assessment.

b. The MAAT will conduct and all hazard risk assessment and execute HHQ assessment of the installation's programs that support mission assurance. Specifically, the MAAT will assess installation security, Antiterrorism (AT), Critical Infrastructure Program (CIP), Chemical, Biological Radiological, Nuclear, and Explosive (CBRNE), Physical Security (PS), Law Enforcement (LE), Intel Support, Installation Emergency Management (IEM), Information Assurance (IA) and other protection related programs in accordance with applicable references.

c. MCMAA teams range from 10 -12 members. The core of the MAAT consist of an GS team leader and civilian/contractor specialists in the functional areas listed above. An representative from HQMC PSM will occasionally accompany the team.

d. The MCMAAP scheduling process starts in January each year, with nominations via message from HQMC PSM. After coordinating the scheduling and prioritization of nominations with MARFORs, the Mission Assurance Assessment Team releases the final MCMAAP schedule in July for the upcoming calendar year. Each installation must have a HHQ Assessment every 3 years, but they can occur more frequently by request or in response to emergent threats.

2. Higher Headquarters (HHQ) and Combatant Commander (COCOM) Requirements. HHQ and COCOM requirements build on DoD standards and MCMAAP benchmarks to ensure AT programs are sufficiently tailored toward the Marine Corps mission and protecting Marine Corps personnel. HHQ reviews are internal reviews that assess the unity of AT efforts throughout subordinate commands. At installations where the Marine Corps is a tenant, an HHQ vulnerability assessment completed by the installation satisfies the 3-year assessment requirement.

3. Inspector General (IG). The Marine Corps Inspector General Program provides candid, objective, and uninhibited internal analysis of the management, operation, and administration of the Marine Corps. The IG of the Marine Corps has jurisdiction to conduct an area visit to evaluate a variety of programs, including AT functions, at any geographical location. Surveys, focus groups, and interviews are usually conducted to provide commanders with the concerns and risks associated with particular programs. Inspectors rely most heavily on input from individuals to examine issues and reach conclusions. The IG will base AT inspections on the Automated Inspection Reporting System 480 checklist. Additional general information about the IG can be found at <http://hqinet001.hqmc.usmc.mil/ig/>.

4. Naval Audit Service. The Naval Audit Service has the jurisdiction to conduct performance audits. These audits are designed to assess a program's performance against its objectives. Performance audits may be conducted in a top-down (vertical) or across-the-department (horizontal) format. Top-down performance assessments look at the Department of the Navy's management of a specific function or program. Across-the-department performance assessments examine program effectiveness at a particular level. Auditors rely most heavily on data analysis and document review to examine issues and reach conclusions.

CHAPTER 11

PHYSICAL SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	1100	11-1
PHYSICAL SECURITY AND THE AT PROGRAM.....	1101	11-1
AT-RELATED PHYSICAL SECURITY MEASURES.....	1102	11-1
INSTALLATION AND EXPEDITIONARY SECURITY CONSIDERATIONS	1103	11-3

CHAPTER 11

PHYSICAL SECURITY

1100. GENERAL. Physical security is the use of active and passive security measures and management protocol that are designed to prevent unauthorized access to personnel, equipment, material, and documents, and safeguards against espionage, sabotage, acts of terrorism, damage, and theft. Physical security systems employ a layered "defense in depth" concept to provide graduated levels of protection from the installation boundary to identified critical assets. Physical security is a supporting element of AT and should thus be included in AT planning. A strong physical security posture is a crucial component of a robust AT program, and it is therefore vital that the Physical Security Specialist and ATO work closely together.

1101. PHYSICAL SECURITY AND THE AT PROGRAM. A physical security plan must be included in Annex C, Appendix 6, of the AT plan. The physical security plan should clearly identify all components of the physical security program. The physical security plan should provide detailed information concerning the installation barrier plan, installation curtailment plan, construction considerations, facility and site evaluation and/or selection, and AT guidance for off-installation housing. It should also identify and include provisions for the security of Mission-Essential Vulnerable Areas as identified in the criticality assessment; physical structures; physical security equipment; chemical, biological, or radiological detection and protection equipment; security procedures; random AT measures (RAMs); response forces; and emergency measures. Effective physical security measures integrate facilities, equipment, trained personnel, and procedures to maximize protection of personnel and assets.

1. The Physical Security(PSP) should be developed by the Physical Security Specialist with input and review by the ATO. The physical security plan should be reviewed annually in conjunction with the AT plan. Physical Security MCO 5530.14A (DRAFT) provides an ATO with additional guidance on physical security initiatives. The physical security plan should outline these initiatives and, at a minimum, incorporate the following.

1102. AT-RELATED PHYSICAL SECURITY MEASURES. There are many physical security measures that have a direct impact on the effectiveness of an AT program. This section describes several

of these physical security measures that should be considered when developing an AT plan, employing RAMs, and changing FPCON levels.

1. Barrier Plans. Physical barriers control, deny, impede, delay, and discourage access to restricted and non-restricted areas by unauthorized persons. They accomplish this by defining the perimeter of restricted areas; establishing a physical and psychological deterrent to entry and providing notice by signage that entry is not permitted; optimizing use of security forces; enhancing detection and apprehension opportunities by security personnel in restricted and non-restricted areas; and channeling the flow of personnel and vehicles through designated portals in a manner that permits efficient operation of the personnel identification and control system. Although effective physical barriers delay an intruder, they rarely can be depended on to stop one. To be effective, security force personnel or other means of protection and assessment must augment such barriers.

Installations should develop comprehensive barrier plans that take the following into consideration:

- Continuous protection along a perimeter by natural or structural barriers
- Criticality and vulnerability related to a given area
- The need for ease of entrance for emergency personnel based on Design Basis Threat and building construction.

Barrier plan developers should coordinate with structural engineering to ensure a barrier plan can be effectively and efficiently executed. A recommended best practice in developing a barrier plan is to download Google images of your base, insert the images into a Powerpoint, and draw the barrier staging areas and final positioning on the Powerpoint images.

2. Entry Control Facilities (ECFs). ECFs serve as the entry point to an installation for all personnel, visitors, and vehicles. The objective of the ECF is to prevent unauthorized personnel and vehicle access and maximize vehicular traffic flow.

- a) In essence, ECF design should consider four zones: an approach zone in which traffic speed and maneuver are limited and vehicle type is established; the access control zone where personnel and vehicle credentials are established and vehicle inspections occur (this area should be screened to protect from

surveillance by enemy forces); the safety zone extends from the passive and active barriers in all directions to protect installation personnel from an explosion at the Vehicle barricade; the response zone, which provides adequate reaction time for ECF personnel; and a final denial barrier that requires positive action to allow entry or exit from a compound.

b. ECF measures and procedures represent the first stage of access control. Access control measures may include identification scanners, access codes, personal identifier numbers, locks, vaults, etc. ECFs should channel approaching vehicles and personnel in order to maximize effectiveness and maintain adequate security.

c. Signage will be used to identify areas of certain importance such as entrance locations, restricted areas, etc. All restricted areas are clearly marked indicating that the area has restricted access. Signs will be posted at entrance of the restricted areas and will identify "Access to the area is restricted. Unauthorized presence within the area constitutes a breach of security.

3. Commercial Vehicle Inspections. When possible, truck/commercial and passenger vehicles should be separated and compartmentalized. Commercial vehicles should use the Commercial Vehicle Inspection Stations for entry. Commercial vehicles are subject to inspection of compartments and containers capable of concealing contraband cargo or personnel as may be directed during heightened FPCONS.

4. Mail Handling. Appendix 19 of DoD O-2000.12-H offers information to assist personnel in identifying suspicious envelopes and packages, and actions to take if hazardous or explosive content is detected. Although it is thorough, the list identifies typical indicators, and personnel should remain vigilant for not-so-typical indicators. If a suspicious envelope or parcel is located, personnel should perform the actions listed at the end of Appendix 19 of DoD O-2000.12-H.

1103. INSTALLATION AND EXPEDITIONARY SECURITY CONSIDERATIONS. Installation and expeditionary bases must implement physical security measures to help protect personnel. Physical security measures can be effective risk mitigation measures. As a result, the risk assessment should be consulted when planning and implementing physical security measures. Security measures to

be considered when developing physical security plans include, but are not limited to, the following:

- Personnel vetting, screening, and indoctrination
- Required security/protection for vulnerable points, assets, or critical infrastructure within the activity
- Security plans and procedures (FPCONS, RAMs)
- Security force organization, training, and response times
- Personnel identification and control systems
- Use of physical security hardware (e.g., Electronic Security Systems, barriers, access control systems, signage)
- Key and lock control
- Coordination with other agencies
- Designation of restricted areas

For fixed installations, ATOs should consult appropriate orders for additional information on physical security. For expeditionary bases, the Joint Forward Operations Base (JFOB) Force Protection Handbook provides an overview of physical security.

1. Installation Security. Physical security is an important part of an installation's ability to protect personnel, information, infrastructure, and equipment. Perimeter and internal protective measures are the first steps in providing defense-in-depth protection against security threats and unauthorized entries.

The security elements that comprise a perimeter security system include:

- Standoff
- Physical barriers
- Access control
- Entry control points
- Security lighting
- Hardened fighting positions/towers/overwatch
- Intrusion detection/surveillance systems and procedures
- Security forces
- Signage

Once perimeter security is established, installation forces can focus on internal security procedures. Internal security consists of those measures used to protect personnel or assets located on the interior of the base. Internal security includes:

- Security forces
- Access control facilities
- FPCON measures
- RAMs
- Mass notification and warning systems
- Site planning
- Building location considerations
- Structural design
- Electrical and mechanical design
- Building design elements and stand-off
- Signage

Access control points and signage are systems designed to restrict individuals from areas where they do not belong. Typically, the more restricted an asset, the more access control measures there will be.

Mass notification and warning is the capability to provide real-time information to all personnel during emergency situations. All installations and units are required to have a mass notification and warning system. Mass notification systems reduce the risk of a mass casualty outcome by providing a timely means to notify personnel of threats or incidents and what should be done to respond to the threat or incident.

Construction protective measures must be taken into consideration as they lead to the fortification of buildings and infrastructure ultimately resulting in the increased protection of personnel. Construction protective measures assess all aspects of building materials, construction, and placement.

Installation (CONUS) bases must also incorporate protective countermeasures as well as physical security measures. Protective countermeasures utilize both technology and human capabilities to aid in prevention, identification, and response to threats and attacks. Protective countermeasures employ:

- Identification checkpoints
- Systems to monitor and detect threats
- Barriers
- RAMs
- Military Working Dogs (MWD)

2. Expeditionary Security. Forces must earnestly focus on the physical security of expeditionary bases due to the increased

threat of attacks. Expeditionary forces must address and utilize the same physical security measures that are previously described in the installation security section. However, there are slight variances and enhancements of the security measures that OCONUS bases typically require due to greater threats in their geographic location.

Expeditionary bases may require stronger defenses within perimeter security systems in order to offer more support against the incursion of unique weaponry and enemies. The goal for expeditionary security is accomplished through the prevention, detection, and response to enemy-threat tactics, including dedicated attack; rocket, artillery, and mortar attacks; vehicle-borne improvised explosive devices; and acts of terrorism, sabotage, theft, pilferage, trespass, espionage, or other insurgent activity. A more robust defense-in-depth posture for expeditionary bases may be necessary to prevent these enemy-threat tactics.

The internal security of expeditionary bases may also require adjustments to building and construction considerations. Building materials and construction must be appropriate to the weather, climate, and soil conditions of the geographic area. Greater standoff distances between buildings may also be necessary in order to better protect against attacks as they may be more likely in some geographic areas outside of the U.S.

CHAPTER 12

ANTITERRORISM-RELATED CONSIDERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	1200	12-1
CRITICAL INFRASTRUCTURE PROTECTION (CIP).....	1201	12-1
INFORMATION ASSURANCE (IA).....	1202	12-1
CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVES (CBRNE).....	1203	12-1
CONSTRUCTION STANDARDS.....	1204	12-2
PUBLIC AFFAIRS OFFICE (PAO).....	1205	12-2
COMMAND, CONTROL, COMMUNICATION, AND COMPUTER SYSTEMS (C4).....	1206	12-3
HIGH-RISK BILLETS (HRBs).....	1207	12-3
FORCE TRACKING AND IN-TRANSIT SECURITY.....	1208	12-5
FORCE HEALTH PROTECTION (FHP).....	1209	12-5
PERSONNEL RECOVERY.....	1210	12-6
NON-LETHAL WEAPONS (NLWs).....	1211	12-6
BIOMETRICS.....	1212	12-7

CHAPTER 12

ANTITERRORISM-RELATED CONSIDERATIONS

1200. GENERAL. As the previous chapters reveal, AT is a broad discipline that includes a number of diverse but interrelated functions. In addition to the topics and processes outlined in the preceding chapters, Antiterrorism Officers (ATOs) should consider several other AT-related disciplines during the development and execution of an AT program. This chapter describes a number of AT-related disciplines that can assist an ATO in developing an effective and efficient AT program. It is strongly recommended that available ATOs consult personnel in these disciplines as the AT program is developed and executed.

1201. CRITICAL INFRASTRUCTURE PROTECTION (CIP). The Marine Corps CIP program is chartered to identify and protect mission-critical assets. Loss of a critical asset could result in failure to support a Combatant Commander mission or a Service mission. Given the criticality of the systems, networks, and assets, the protection of such infrastructure is essential. As the criticality assessment of the risk management process reveals, CIP and AT are inextricably linked. Protecting critical assets is an important part of an AT program, and therefore AT and CIP personnel should coordinate efforts. Just as an AT program should address all-hazards, critical infrastructures must do the same. An ATO should consult CIP when conducting the asset identification process of the criticality assessment described in Chapter 3 (3002.3) and implementing any critical infrastructure mitigation measures. The CIP Working Group described in Chapter 2 of the AT Manual provides an optimal platform for an ATO to work alongside CIP.

1202. INFORMATION ASSURANCE (IA). IA is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by information systems such as computer data networks. It is established to consolidate and focus efforts in securing information, including its associated systems and resources. IA works to increase the level of trust of the information and its originating source. Commanders must initiate a program to train operators at all levels and ensure information assurance guidance is followed in accordance with MCO 5239.2, Marine Corps Information Assurance Program (MCIAP) and DoDD 8500.01E, Information Assurance.

1203. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVES (CBRNE). Department of Defense Instruction

(DoDI) 2000.18 implements policy, assigns responsibilities, and prescribes procedures to establish and implement a program to manage the consequences of a CBRNE incident at all Department of Defense (DoD) installations. DoD installation emergency responders must be prepared to respond to the effects of a CBRNE incident to preserve life, prevent human suffering, mitigate the incident, and protect critical assets and infrastructure. ATOs should be familiar with DoDI 2000.18 and the proper procedures to respond to a CBRNE incident. The CBRNE Emergency Response Working Group described in Chapter 2 of this AT Manual provides an optimal platform for an ATO to ensure an AT plan adequately addresses CBRNE response measures.

1204. CONSTRUCTION STANDARDS. Unified Facilities Criteria (UFC) 4-010-01 promulgates the DoD minimum AT construction standards for all DoD facilities. Physical security specialists are experts on construction standards, which are important to their efforts. The Physical Security Working Group described in Chapter 2 provides an optimal platform for an ATO to consult physical security specialists.

1. Unified Facilities Criteria (UFC). UFCs are designed to minimize the likelihood of mass casualties from terrorist attacks against personnel in the buildings in which they work and live. UFCs are designed to maximize standoff distance, prevent building collapse, minimize hazardous flying debris, limit airborne contamination, provide mass notification, and facilitate future upgrades. The financial impact of implementing UFCs is significantly less than the economic and intangible costs of a mass casualty incident.

2. Protective Construction. Protective construction is related to UFC in that structures should be designed to protect personnel and other assets from the effects of threat-related courses of action and natural disasters. Protective construction structures include sidewall protection, compartmentalization, overhead cover, personnel and equipment bunkers, hardened fighting and observation positions, and the use of existing structures.

1205. PUBLIC AFFAIRS OFFICE (PAO). The PAO is responsible for forwarding reliable and accurate information concerning an incident beyond military channels. ATOs should coordinate with the PAO to establish a communication process to relay information as a situation/crisis develops. Unless authorized, media representatives should not have direct access to terrorists, victims, communication nets, or anyone directly

involved in a terrorist incident. DoD experience with media representatives has shown that bringing them in early under reasonable conditions and restrictions commensurate with the risk and gravity of the event and providing them with thorough briefings maintains DoD credibility and preserves freedom of information. Public affairs efforts should focus on informing the public of possible dangers and reinforcing public confidence in the installations' capabilities to respond to an event.

1206. COMMAND, CONTROL, COMMUNICATION, AND COMPUTER SYSTEMS (C4). C4 is the terminology for those information systems that enable leaders to effectively manage their areas of responsibility. C4 systems focus on the networks that allow voice and data communications among command posts, staffs, and critical components of FP activities. C4 systems enable commanders and staffs to effectively manage ongoing operations. Without a reliable, redundant means of communicating threat status, intelligence, and operations, the Commander and staff will not have a viable, common operating picture of the situation, nor will they be able to direct actions in a timely and coordinated manner. C4 assists ATOs in incident/event reporting and many other AT efforts.

1207. HIGH-RISK BILLETS (HRBs). Marine Corps HRBs are authorized personnel billets that make the personnel filling them an attractive or accessible terrorist target. HRBs are based on the following criteria: grade (usually General, Admiral, or Senior Executive Service), assignment (usually to a country with a Defense Intelligence Agency [DIA] terrorist level of "significant" or higher), geographic location, travel itinerary, and/or symbolic value.

1. Program Administration. In early January of each year, Headquarters Marine Corps Plans, Policies, and Operations (HQMC PP&O) will query commanders to identify billets in their command that are potentially high-risk. Commanders may nominate HRB or personnel at any time if changes occur, or if a new billet is established that has the potential to be an HRB. HQMC PP&O will forward a consolidated list of HRB nominees by the end of January to the Naval Criminal Investigative Service (NCIS) Protective Operations Department, Washington, DC, which has program oversight for all HRBs in the Department of the Navy.

a. In February of each year, the NCIS Protective Operations Department will convene an HRB board chaired by the Deputy Assistant Director for Protective Operations and staffed by two supervisory personnel from the department, as well as a

representative from HQMC PP&O. The HRB board then reviews the list of nominations, determines HRB eligibility/necessity, and subsequently validates HRB status.

2. High-Risk Personnel (HRP). HRP, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. HRP do not necessarily fill an HRB. There are three HRP Levels:

a. HRP Level I Protection signifies protective security detail support provided to an official who requires continuous protection as recommended by the Personal Security Vulnerability Assessments (PSVA).

b. HRP Level II Protection signifies protective security detail support to an official who requires protection during periods of official duty or travel as recommended by the PSVA.

c. HRP Level III Protection signifies support provided to an official who requires advanced individual AT awareness and personal protection training.

3. Personal Security Vulnerability Assessments (PSVAs). The purpose of an NCIS PSVA is to: (1) assess an HRB's level of risk and vulnerability to criminal or terrorist activities; (2) determine current weaknesses in security plans, programs, or protective operations; and (3) make recommendations to correct identified weaknesses and/or enhance the HRB's overall security posture. A PSVA may also list recommended protective operations support if deemed necessary. PSVAs are required for all Marine Corps HRBs.

a. A PSVA examines the following areas: specific and identified terrorist threats, command terrorist threat reporting and information flow, overall general criminal threat, the HRB's position, the HRB's personal and command security awareness, daily routine, route analysis, vehicle security, and the physical security of the office and residence.

b. Upon completion of a PSVA, approval of any recommendations and publication of the final report by the Protective Operations Department, which includes a copy of the PSVA along with a cover letter from DoD for Protective Operations, will be mailed to the responsible field office for delivery to the affected HRB. A senior representative from the field office will personally brief the HRB on the results of the PSVA and discuss security recommendations and the implementation of protective operations support if recommended.

4. Training. Marines selected for assignment to HRBs are required to complete additional AT training. The Training and Education Command will conduct AT training for Marines assigned to HRBs where the threat is warranted. Marines selected for assignment to HRBs may also be required to complete additional code of conduct/survival evasion resistance and escape training according to established Combatant Commander requirements.

5. AT Responsibilities. ATOs must develop AT measures for HRP and personnel occupying HRBs. HRB/HRP protective measures must be promulgated in the AT Plan and tied to the FPCON system. ATOs should also ensure HRP and appropriate family members complete suitable high-risk training; are properly cleared for assignment to HRBs, facilities, or countries requiring such protection; and have been thoroughly indoctrinated on the duties and responsibilities of protective service personnel. HRP designees and their family members should be familiar with treaty, statutory, policy, regulation, and local constraints concerning the application of supplemental security measures for certain high-ranking officials who are provided additional protection because of their positions.

1208. FORCE TRACKING AND IN-TRANSIT SECURITY. Commanders with FP responsibility for a transitioning force will ensure the development and execution of in-transit security plans and conduct of a predeployment AT vulnerability assessment. Commanders will implement appropriate AT measures to reduce risk and identified vulnerabilities. Deploying commanders will adhere to COCOM requirements for tracking and security while transitioning through or to the COCOM's area of responsibility. For exact guidance on force tracking and in-transit security, an ATO should see Combatant Commander and service component doctrine.

1209. FORCE HEALTH PROTECTION (FHP). FHP focuses on healthcare programs that protect personnel within a command. FHP is a command responsibility at all levels. FHP is a "total life cycle" health support system implementing the concepts described in the joint vision through an integrated and focused approach to protect and sustain DoD's most important resource—its service members and their families—throughout the entire length of service commitment. It includes all measures taken by commanders, leaders, individual service members, and the Military Health System to promote, improve, or conserve the mental and physical well-being of service members across the range of military operations.

Commanders must ensure health service support is integrated into their AT plan. The goal of health service support is to effectively and efficiently use medical capabilities and individual healthful practices to avoid any human condition that would prevent the Marine Corps from achieving its objectives. The health service support section of an AT plan should include mass casualty planning, WMD identification and risk management, food and water vulnerability assessments, pandemic prevention and other appropriate preventive medicine measures.

Updated information on health concerns in foreign countries can be found at the Centers for Disease Control and Prevention's Web site (<http://www.cdc.gov/travel>) and the World Health Organization's Web site (<http://www.who.int>), the Navy and Marine Corps Public Health Center's Web site (www.nmcpb.med.navy.mil), and the DoDs Force Health Protection and Readiness Web site (<http://fhp.osd.mil/>).

1210. PERSONNEL RECOVERY. Personnel recovery comprises military, diplomatic, and civil efforts to prepare for and execute the recovery and reintegration of isolated personnel. The ATO may be called on to assist the Personnel Recovery Officer in the preparation of the Isolated Personnel Report (ISOPREP) and Survival Evasion Resistance Escape (SERE) Training. In accordance with Department of Defense Directive (DoDD) 2310.2 and Marine Corps Order 3460.2, preserving the lives and well-being of U.S. military, DoD civilian, and contract service employees placed in danger of being isolated, beleaguered, detained, captured, or having to evade while participating in a U.S.-sponsored activity or mission is one of the highest priorities of DoD and the Marine Corps. This AT handbook is designed to improve AT programs by enhancing recovery and response efforts, and thereby protecting personnel.

1211. NON-LETHAL WEAPONS (NLWs). For military purposes, NLWs are specifically designed and primarily employed to incapacitate targeted personnel or materiel while minimizing fatalities, permanent injury to personnel, and undesired collateral damage in the target area or environment. NLWs deliver a level of force that achieves immediate target response and provide predictable and reversible effects. Unlike lethal counterparts, NLWs use means other than gross physical destruction to prevent the target from functioning. Per DoDD 3000.3, "Policy for Non-Lethal Weapons," NLWs, doctrine, and concepts of operation will be designed to reinforce deterrence and expand the range of options available to commanders. Non-lethal capabilities can enhance the ability of a commander to protect an installation from potential

threats. Per the January 2008 Joint Capabilities Document for Joint Non-Lethal Effects, NLWs can be used for counter personnel or counter materiel purposes. In a counter-personnel capacity, NLWs can be used to deny access in to or out of an area, move individuals or groups through an area, and disable or suppress individuals or groups. In a counter-material capacity, NLWs are used to disable, stop, neutralize, or deny an area to vehicles, vessels, and aircraft; disable particular items of equipment; or deny access to a facility.

The benefits of NLWs should not limit a commander's inherent authority and obligation to use all necessary means available and take all appropriate action in self-defense. NLWs should never be used as a stand-alone defense. Lethal overwatch should always be available when using NLWs.

Commanders and ATOs can find out more about NLWs' capabilities and how this technology can serve them from the Joint Non-Lethal Weapons Program (JNLWP) Web site (www.jnlwp.com). Instructors certified through the Interservice Non-Lethal Individual Weapons Instructor Course (INIWIC) can also serve as important assets by providing commanders and ATOs with critical information pertaining to the use of NLWs and legal/doctrinal considerations. INIWIC, based out of Fort Leonard Wood, MO, is the only course provided by DoD to certify NLW instructors. More information about this course can be found at www.iniwic.net.

1212. BIOMETRICS. Biometrics is a force multiplier that enables the Commander/installation to effectively identify and categorize individuals as friend or adversary. Biometric systems gather data through incorporation of iris scan, fingerprints, photo, and contextual data. The biometrics system matches previously enrolled individuals to historical data and actions in order to confirm and ascertain a person's identity, credentials, and past behavior. By linking an individual to a history, a Commander has facts on which to base a decision. Biometric signatures cannot easily be faked, and therefore, have the capability of identifying an individual with a degree of certainty of over 99%. By utilizing the biometrics verification system, the Commander can more effectively focus his forces on missions rather than determining the authenticity of credentials.

APPENDIX A

SAMPLE INSTALLATION AT PLAN

OVERVIEW

The format outlined below is offered as one means of developing an Antiterrorism (AT) Plan. It is designed for a base or installation, but can be adapted for other facilities and deployed units. It is meant to help the ATO structure the AT plan in a comprehensive and organized manner. The format is patterned after the standard five-paragraph military operations order (Situation, Mission, Execution, Administration and Logistics, and Command and Signal). Another available option is to use the Joint Antiterrorism Program Manager's Guide resident within ATEP in AKO.

This format enables the synchronization of existing programs such as Law Enforcement, Physical Security, AT, Operations Security (OPSEC), INFOSEC, High-Risk Personnel protection, and other installation efforts. AT Plans should be integrated into all plans and separate annexes. Staff interaction and coordination is a crucial element of developing a realistic, executable plan.

Although this sample is patterned after the military operations order, it is applicable to Commanders/Directors of DoD Elements as they develop plans to protect personnel, activities, and material under their control.

This sample uses supporting Annexes, Appendices, Tabs, and Enclosures to provide amplifying instructions as required. This method shortens the length of the basic plan (which should be read by all personnel outlined in the plan), and provides organization, structure, and scalability.

SAMPLE AT PLAN (U)

Task Organization: [Include all agencies/personnel (base and civilian) responsible for implementing the plan. Include as a separate Annex. See Annex A (Task Organization).]

Maps/Charts: [List all applicable maps or charts. Include enough data to ensure personnel are using the correct year/edition/version of the subject material.]

Time Zone: [Enter the time zone of the installation. Indicate the number of hours to calculate (plus/minus) ZULU time.]

Ref: [Enter the compilation of pertinent publications, references, MOU/MOA/MAA. This list may be included in a separate Annex. See Annex Q (References).]

1. SITUATION.

a. General. [This plan applies to all personnel assigned or attached to the installation. [Describe the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT operations.]

b. Enemy. [The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. [ENTER the general threat of terrorism to this installation, including the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces. Include the general threat of terrorist use of WMD against this installation. This information should remain unclassified when possible. See paragraph 1f, Intelligence, on identifying specific threats.] This information may be included as a separate Annex. See Annex B (Intelligence).]

c. Friendly. [ENTER the forces available (both military and civilian) to respond to a terrorist WMD 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 local, State, or Federal LE agencies and military police forces, fire and emergency services, medical, Federal/State/local agencies, special operations forces, engineers, detection (radiological, nuclear, biological, and chemical) decontamination or smoke units, and explosive ordnance disposal (EOD). Include Memorandums of Agreement (MOAs)/Memorandums of Understanding (MOUs) and any other special arrangements that will improve forces available to support the plan. If in the U.S. and its territories, the Department of Justice, Federal Bureau of Investigation (FBI) is responsible for coordinating all Federal agencies and DoD forces assisting in the resolution of a terrorist incident. If outside the U.S. and its territories, the Department of State (DoS) is the lead agency. This information can be included in a separate

Annex(s). See Annex A (Task Organization) and Annex J (Command Relationships).]

d. Attachments/Detachments. [ENTER installation/civilian agencies NOT normally assigned to the installation that are needed to support this plan. Explain interagency relationships and interoperability issues. This can be listed in other Annexes. See Annex A (Task Organization) and Annex J (Command Relationships).]

e. Assumptions. (List planning/execution assumptions) [ENTER all critical assumptions used as a basis for this plan. Assumptions are those factors unlikely to change during the implementation of the AT plan and that must addressed in order to continue to plan. They can range from the installation's troop strength to addressing the local political/social environment. Examples follow:

(1) The installation is vulnerable to theft, pilferage, sabotage, and other threats. The installation is also vulnerable to a WMD attack.

(2) An act of terrorism involving WMD can produce major consequences that will overwhelm almost immediately the capabilities of the installation.

(3) 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.

(4) No single unit on the installation possesses the expertise to act unilaterally in response to WMD attacks.

(5) If protective equipment is not available, responders will not put their own lives at risk.

(6) Local, non-military response forces will arrive within [time] of notification.

(7) Units specializing in WMD response will arrive onsite within [number of hours based on installation location] of notification.

(8) The HN is supportive of U.S. policies, and will fulfill surge requirements needed to respond to a WMD incident IAW MOAs/MOUs.]

f. Intelligence. [ENTER the person, staff, or unit responsible for intelligence/counterintelligence collection and dissemination. The installation Commander must have a system in place to access current intelligence. This can be included in

Annex B (Intelligence).] [National-level agencies, Combatant Commanders, intelligence, and CI systems provide theater or country threat levels and threat assessments. In the U.S. and its territories, local installations must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other Federal agencies.] 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 means of dissemination of the installation's tailored AT product. Note: Commanders cannot change the threat level, which is developed at the national level, although they can declare higher FPCONS than the baseline.

2. MISSION. [ENTER a clear, concise statement of the command's mission and the AT purpose or goal statement supporting the mission. The primary purpose of the AT plan is to safeguard personnel, property, and resources during normal operations. It is also designed to deter a terrorist threat, enhance security and AT awareness, and assign AT responsibilities for installation personnel.]

3. EXECUTION.

a. Commander's Intent. (Commander's vision on how he/she sees the execution of the unit's AT Program. Refer to Service planning doctrine for assistance.)

b. Concept of Operations. [ENTER how the overall AT operation should progress. This plan stresses deterrence of terrorist incidents through preventive and response measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT planning and passive, defensive operations. This paragraph should provide subordinates with sufficient guidance to act if contact or communications with the installation chain of command is lost or disrupted.

(1) The installation's AT Concept of Operations should be phased in relation to pre-incident actions and post-incident actions. AT 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. The AT mission and the unpredictability of its execution requires very specific "how to" implementation instructions on DoD FPCON measures and how these actions must be coordinated. This "how to" element is not normally included in the Concept of Operations paragraph; however, the necessity to provide "how to" guidance in the AT plan requires a different manner of data presentation to ensure brevity and clarity. The implementation instructions are put into the form of action sets and can be displayed in the form of an execution matrix (Pre-Incident Action Set Matrix).

(2) In Post-Incident planning, the installation should focus on its response and reconstitution responsibilities upon notification of a terrorist incident and the procedures for obtaining technical assistance/augmentation if the incident exceeds the installation's organic capabilities. 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. Therefore, each installation must plan for the worst-case scenario by planning its response based on its organic resources and available local support through MOA/MOUs.

(3) The situation may dictate that the installation will conduct not only the initial response but also sustained response operations. Many installations do not have onboard WMD officers or response elements. This paragraph will include specific implementation instructions for all functional areas of responsibility and the manner in which these actions must be coordinated. The implementation instructions can be put in the form of action sets and displayed in the form of a synchronization matrix (Post-Incident Action Set Synchronization Matrix). The synchronization matrix format clearly describes relationships among activities, units, supporting functions, and key events that must be carefully synchronized to minimize loss of life and contain the effects of a terrorist incident.]

c. Tasks. [ENTER the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT- 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 planning and response element will be delineated in the Pre- 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) First Subordinate Unit/Element/Tenant.

(a) Task listing.

d. Coordinating Instructions. [This paragraph should include AT-specific coordinating instructions and subparagraphs, as the Commander deems appropriate. In addition, this section of the AT plan outlines aspects of the installation's AT posture that require particular attention to guarantee the most effective and efficient implementation of the AT plan. For the purposes of this plan, there are five basic coordinating instructions: 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.

(1) AT Planning and Response. For instructional purposes, this template outlines AT planning and response elements on the installation required to respond to a terrorist/WMD incident. Initial and sustained response to an attack must be a coordinated effort among the many AT 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 (U.S. and its territories) or HN (outside the U.S. and its territories). For the purposes of this plan, an installation's capability is divided into AT planning and response elements. These tailored, installation-level elements parallel the national-level FEMA Emergency Support Functions (ESFs) and the MCMAAP evaluation criteria to the greatest degree possible.

AT Planning & Response Elements

Information & Planning *
Communications * +
HazMat *
Security * +
Explosive Ordnance Disposal (EOD) +
Firefighting * +
Health & Medical Services * +
Resource Support *
Mass Care *
Public Works *
Intelligence Process +
Installation AT Plans/Programs +
Installation Perimeter Access +
Security System technology +
Executive Protection +
Response & Recovery +
Mail Handling +

* Derived from FEMA ESFs

+ Derived from MCMAAP assessment criteria

(2) Procedural.

(a) Alert Notification Procedures. See Appendix 14 to Annex C (Operations).

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

(c) Installation Training & Exercises. See Annex N (AT Program Review, Training, & Exercises).

(d) Incident Response. See Appendix 1 to Annex C (Operations).

(e) Consequence Management. See Appendix 1 to Annex C (Operations).

(f) High-Risk Personnel Protection Procedures. See Appendix 9 to Annex C (Operations).

(g) AT Program Review (See Annex N (AT Program Review, Training, & Exercises)).

(h) Higher Headquarters Vulnerability Assessments. See Annex N (AT Program Review, Training, & Exercises).

(3) Security Posture Responsibilities.

(a) Law Enforcement. See Appendix 7 to Annex C (Operations).

(b) Physical Security to include Lighting, Barriers, Access Control. See Appendix 6 to Annex C Operations).

- (c) Other On-Site Security Elements. See Appendix 8 to Annex C (Operations).
- (d) Operations Security. See Appendix 10 to Annex C (Operations).
- (e) Technology. See Appendix 15 to Annex C (Operations).
- (f) Emergency Operations Center (EOC) Operations. See Appendix 12 to Annex C (Operations).
- (g) Critical Systems Continuity of Operations (optional). See Appendix 13 to Annex C (Operations).
- (h) Other.

(4) Threat-Specific Responsibilities.

- (a) Antiterrorism. See Appendix 2 to Annex C (Operations).
- (b) Weapons of Mass Destruction. See Appendix 5 to Annex C (Operations).
- (c) Special Threat Situations. See Appendix 3 to Annex C (Operations).
- (d) Information Security. See Appendix 11 to Annex C (Operations).
- (e) Natural/Man-made Hazards (Optional). See Appendix 17 to Annex C (Operations).
- (f) Other.

(5) Special Security Areas.

- (a) Airfield Security. See Appendix 4 to Annex C (Operations).
- (b) Port Security. See Appendix 4 to Annex C (Operations).
- (c) Embarkation/Arrival Areas. See Appendix 4 to Annex C (Operations).
- (d) Buildings. See Appendix 4 to Annex C (Operations).
- (e) Other.

4. ADMINISTRATION AND LOGISTICS. [ENTER the administrative and logistics requirements to support the AT plan, which should include enough information to make clear the basic concept for planned logistics support. Ensure the staff conducts logistical planning for both pre- 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 chemical defense equipment "push" packages. 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 operations.

- a. Administration. See Annex O (Personnel Services).
- b. Logistics. See Annexes D (Logistics) and E (Fiscal).

5. COMMAND AND SIGNAL. [ENTER instructions for command and operation of communications-electronics equipment. Identify the primary and alternate locations of the command post and EOC. Enter the installation's chain of command. Highlight any deviation from that chain of command that must 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 any technical support elements that could be called upon in the event of a terrorist WMD incident and the means to contact each. Recommend the installation coordinate with higher headquarters to establish procedures to allow for parallel coordination 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. Command. See Annex A (Task Organization) and Annex J (Command Relationships).

b. Signal. See Annex K (Communications).

c. Command Post Locations.

- (1) Primary: [ENTER location]
- (2) Alternate: [ENTER Location]

d. Succession of Command.

- (1) First alternate: [ENTER POSITION/TITLE]
- (2) Second alternate: [ENTER POSITION/TITLE]

//SIGNATURE// Commanding General/Officer Signature Block

ANNEXES: (Should provide amplifying instructions on specific aspects of the plan. Each ANNEX can be subdivided into Appendices, Tabs, and Enclosures as required to provide amplifying instructions. Further, some of these supporting documents may be established in other unit operating orders/procedures, and referenced as required.)

ANNEX A - Task Organization. [ENTER key AT organization composition, e.g., AT Working Group, Crisis Management Team, Emergency Operations Center, First Response Elements, etc.]

Appendix 1 - Table of Organization

Appendix 2 - Post Prioritization Chart

ANNEX B - Intelligence. [ENTER the agency(ies) responsible for intelligence and specific instructions. In the U.S. and its territories, commanders must obtain the local terrorist threat information by querying the FBI through the installation's law enforcement liaison, local law enforcement, or other Federal agencies.]

Appendix 1 - Local Threat Assessment

Appendix 2 - Local WMD Assessment

Appendix 3 - Counterintelligence

Tab A - Counterintelligence Target List

Tab B - Multidiscipline Counterintelligence Threat Report

Tab C - Designation of Theater CI Executive Agency (Draft Message)

Tab D - Umbrella CI Force Protection Source Operation Proposal

Appendix 4 - Risk Assessment

Appendix 5 - Pre-deployment AT Vulnerability Assessment

ANNEX C - Operations. [This is the most important part of the plan.] Annex C and supporting Appendices will provide specific instructions for all of the various AT operations. All other Annexes/Appendices support the implementation of Annex C.

Appendix 1 - Incident Planning and Response. [ENTER how the various agencies (military/civilian) and resources will be integrated to respond to the operations outlined below. These instructions should be generic enough to apply across the operational spectrum. Specific instructions for each operation will be detailed in the appropriate Annex/Appendix/Enclosure.]

Tab A - Incident Command and Control Procedures

Tab B - Incident Response Procedures

Tab C - Incident Management Procedures

Appendix 2 - Antiterrorism

Tab A - Critical Asset List

Tab B - Potential Terrorist Targets

Tab C - FPCON

Enclosure 1 - FPCON Action Sets

[Who/What/When/Where/How]

Tab D - Random Antiterrorism Measures (RAM) Procedures

Appendix 3 - Special Threat Situations

Tab A - Bomb Threats

Enclosure 1 - Bomb Threat Mitigation

Enclosure 2 - Evacuation Procedures

Enclosure 3 - Search Procedures

Tab B - Hostage Barricaded Suspect

Tab C - Mail-Handling Procedures

Appendix 4 - Special Security Areas

Tab A - Airfield Security

Tab B - Port Security

Tab C - Embarkation/Arrival Areas

Tab D - Buildings

Appendix 5 - Weapons of Mass Destruction (CBRNE) & HazMat. [ENTER the specific procedures, planning, training, and response to WMD (CBRNE) incidents. Care should be taken to integrate existing plans for response to HazMat incidents to avoid duplication. Include "baseline" preparedness.]

Tab A - WMD Action Set Synchronization Matrix

[Who/What/Where/When/How]

Tab B - CBRNE Emergency Responder Procedures

Appendix 6 - Physical Security

Tab A - Installation Barrier Plan. [ENTER procedures and pictorial representation of barrier plan.]

Tab B - Installation Curtailment Plan

- Tab C - Construction Considerations
- Tab D - Facility and Site Evaluation and/or Selection
- Tab E - AT Guidance for Off-Installation Housing

Appendix 7 - Law Enforcement

- Tab A - Organization, Training, Equipping of Augmentation Security Forces
- Tab B - Alternate Dispatch Location
- Tab C - Alternate Arming Point

Appendix 8 - Other On-Site Security Forces

Appendix 9 - High-Risk Personnel

- Tab A - List of High-Risk Billets

Appendix 10 - Operations Security

Appendix 11 - Information Security

Appendix 12 - Emergency Operations Center (EOC) Operations.
[ENTER procedure for the activation & operations of the EOC.]

- Tab A - EOC Staffing (Partial/Full)
- Tab B - EOC Layout
- Tab C - EOC Messages & Message Flow
- Tab D - EOC Briefing Procedures
- Tab E - EOC Situation Boards
- Tab F - EOC Security and Access Procedures

Appendix 13 - Critical Systems Continuity of Operations Plans (Optional). [ENTER those systems that are essential to mission execution and infrastructure support of the installation, e.g., utilities systems, computer networks, etc. This document outlines how the installation will continue to operate if one or more critical systems are disrupted or fail, and how the systems will be restored.]

- Tab A - List of installation critical systems
- Tab B - Execution checklist for each critical system

Appendix 14 - Emergency Mass Notification Procedures.
[ENTER the specific means and procedures for conducting a mass notification. Also covered should be the procedures/means for contacting key personnel and agencies.]

Tab A - Situation-Based Notification

Tab B - Matrix List of Phone Numbers/E-mail Accounts

Appendix 15 - Exploit Technology Advances. [ENTER the process and procedures for developing and employing new technology. Identify who is responsible and what should be accomplished.]

Appendix 16 - Higher Headquarters Vulnerability Assessments. [ENTER procedures for conducting higher headquarters vulnerability assessments.]

Appendix 17 - Natural/Man-made Hazards (Optional)
[Hurricanes, Flooding, Chemical Plants, etc.]

Tab A - Locality-specific natural and man-made hazards)

ANNEX D - Logistics (Specific logistics instructions on how to support AT operations.)

Appendix 1 - Priority of Work. [ENTER the priority regarding employing scarce logistical resource.]

Appendix 2 - Emergency Supply Services

Appendix 3 - Weapons and Ammunition Supply Services

Appendix 4 - Emergency Equipment Services

Appendix 5 - Evacuation Shelters

Appendix 6 - Generator Refueling Matrix

ANNEX E - Fiscal (Specific fiscal instructions on how to support AT operations from pre-incident through post-incident.)

Appendix 1 - AT Program Objective Memorandum/Budget Estimate Submission Instruction

Appendix 2 - Combating Terrorism Readiness Submission Instructions

Appendix 3 - Fiscal Management during Exigent Operations

ANNEX F - Tenant Commanders (Specific instructions on how tenant commands/agencies support AT operations.)

Appendix 1 - Areas of Responsibility (Pictorial)

ANNEX G - Air Operations (Specific air instructions on how to support AT operations.)

Appendix 1 - List of Landing Zones (Used for emergency medical evacuations or equipment/personnel staging areas)

ANNEX H - Legal. [ENTER the jurisdictional limits of the installation's commander and key staff. Although the Department of Justice, Federal Bureau of Investigation (FBI) has primary law enforcement responsibility for terrorist incidents in the United States, the installation Commander is responsible for maintaining law and order on the installation. Once a task force or other than installation support arrives on the installation, the agencies fall under the direct supervision of the local Incident Commander. In all cases, command of military elements remains within military channels. The installation should establish agreements to address the use of other military personnel, and local resources that clearly delineate jurisdictional limits. The agreements will likely evolve into the installation having responsibility "inside the wire or installation perimeter" and the local authorities having responsibility "outside the wire or installation perimeter." There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms that may require the installation to be responsible for certain areas outside of the installation perimeter.]

Appendix 1 - Jurisdictional Issues

Appendix 2 - Use of Force and/or Rules of Engagement Instructions

Appendix 3 - Pictorial Representation of Installation Jurisdiction

ANNEX I - Public Affairs (Specific Public Affairs Office [PAO] instructions on how to support AT operations.)

Appendix 1 - Command Information Bureau Organization & Operation

Appendix 2 - Local/Regional Media Contact Information

ANNEX J - Command Relationships (Provides specific guidance on command relationships and military/civilian interoperability issues during incident command and control.)

Appendix 1 - AT Organizational Charts [Crisis Management Team, AT Working Group, First Responder Elements, Incident Command Organization (include civilian and other external agencies)]

ANNEX K - Communications (Specific communications instructions on how to support AT operations. Include systems/procedures for SECURE and NON-SECURE communications means.)

Appendix 1 - Installation AT Communication Architecture

Appendix 2 - Incident Command Communication Architecture

Appendix 3 - EOC Communication Architecture

Appendix 4 - Security Force Communication Architecture

Appendix 5 - Fire Department Communication Architecture

Appendix 6 - Medical Communication Architecture

Appendix 7 - Other Agencies

ANNEX L - Health Services (Specific medical instructions on how to support AT operations.)

Appendix 1 - Mass Casualty Plan

Appendix 2 - Procedures for Operating with Civilian
Emergency Medical Service and Hospitals

ANNEX M - Safety (Specific safety instructions on how to support AT operations.)

ANNEX N - AT Program Review, Training, & Exercises

Appendix 1 - AT Program Review

Tab A - Local Assessments

Tab B - Higher Headquarters Assessments

Appendix 2 - AT Required Training

Appendix 3 - Exercises

ANNEX O - Personnel Services. [ENTER administrative and personnel procedures required to support the plan, e.g., civilian overtime, post-traumatic stress syndrome counseling.]

Appendix 1 - Operating Emergency Evacuation Shelters

ANNEX P - Reports. [ENTER all the procedures for report submissions and report format.]

Appendix 1 - Reporting Matrix

ANNEX Q - References. [ENTER all supporting reference materials, publications, regulations etc.]

ANNEX R - Distribution. [ENTER the list of agencies to receive this plan. Cover plan classification, handling and declassification procedures.]

APPENDIX B

SAMPLE EXPEDITIONARY AT PLAN

ANTITERRORISM PLAN FOR SURGICAL COMPANY (-)
INDONESIAN DR/HA

REFERENCES:

- a. DoD Directive (DoDD) 2000.12-H, Protection of DoD Personnel Against Terrorist Acts, 15 Sept 96
- b. DoD Instruction (DoDI) 2000.16, DoD Combating Terrorism Program Standards, 14 Jun 01
- c. Joint Pub 3-07-2, Joint Tactics, Techniques, and Procedures for Antiterrorism, 25 Jun 93
- d. Joint Pub 3-10.1, Joint Tactics, Techniques, and Procedures for Base Defense, 15 Mar 93
- e. MCO P5530.14, Marine Corps Physical Security Program Manual
- f. USPACOMINST 3850.2K, "Antiterrorism/Force Protection" (AT/FP)
- g. MCO 5500.6F, Arming of Security Personnel and the Use of Force
- h. Group Order 3302.1A, Antiterrorism/Force Protection Program

1. SITUATION. In an effort to mitigate the devastating effects of the recent earthquake in Bantul, Indonesia, III MEF forces will conduct Disaster Relief/Humanitarian Assistance operations in The Republic of Indonesia. III MEF Marines, Sailors, facilities, and infrastructure are symbols of the United States, the Marine Corps, and our way of life. As such, they are all potential targets of terrorism. The cornerstone of this AT/FP Plan is an alert, educated, combat-ready Marine and Sailor.

a. Threat

(21 November 2005): This Travel Warning updates information on the security threat to Westerners in Indonesia. The Department of State continues to warn U.S. citizens to defer non-essential travel to Indonesia. The American Embassy (AmEmbassy) reminds Americans in Indonesia of the continued serious security threat to Americans and other Westerners in Indonesia. The information obtained in the 9 November raid in which Indonesian police killed Jemaah Islamiyah (JI) terrorist Azahari bin Husin shows that JI-affiliated terrorists were in

the advanced stages of planning additional attacks against Westerners in Indonesia. Specifically, the police discovered in the raid 35 bombs prepared and ready to use in attacks. Police also found a videotaped threat from a hooded terrorist who threatened specific attacks against Americans, Australians, British, and Italians. The AmEmbassy and the Indonesian government take these threats very seriously.

The AmEmbassy further informs Americans that a recently discovered Internet Website provides detailed instructions on how terrorists can attack and kill individual Westerners on the streets of Jakarta. The Website, written in Indonesian, specifically mentions locations in the Kuningan area known to be frequented by many Western pedestrians, including hotels, office buildings with international tenants, and pedestrian overpasses. The Website also mentions recreation and entertainment sites frequented by Westerners and refers in general to hotels, sports centers, and exhibition halls. Roads leading to and from such locations, toll booths, and parking lot entrances and exits could also be targeted. The bombs and other materials in the Azahari safe house and the information on the Website make it clear that terrorists in Indonesia are likely changing their tactics to include targeting of individual Western citizens. In addition to past information that indicated that terrorists would target specific businesses or buildings, the new information shows that terrorists are likely now planning to attack Westerners riding in cars or walking on streets, sidewalks, or pedestrian overpasses in Jakarta. The AmEmbassy considers that the information on the Website was developed by persons with serious terrorist intent.

The AmEmbassy reminds Americans that in recent years, terrorist attacks have occurred in Indonesia during the Christmas and New Year's holiday season. The possibility of terrorist attacks appears even higher this year in view of the new threat information detailed above. Due to these serious security concerns, the Department of State warns U.S. citizens to defer non-essential travel to Indonesia. Terrorist attacks could occur at any time and could be directed against any location, including those frequented by foreigners and identifiably American or other Western facilities or businesses in Indonesia. Such targets could include but are not limited to places where Americans and other Westerners live, congregate, shop, or visit, including hotels, clubs, restaurants, shopping centers, identifiably Western businesses, housing compounds, transportation systems, places of worship, schools, or public

recreation events. Reports suggest attacks could include targeting individual American citizens.

The AmEmbassy urges Americans in Indonesia to evaluate very carefully the security implications of all their daily activities in light of the above information. Americans should maintain a vigilant security posture at all times, be aware of their surroundings, and vary the routes and times of their daily activities. The most recent terrorist attack was the 1 October 2005 bombings in Bali that killed 20 people. A terrorist bombing outside the Australian Embassy in Jakarta on 9 September 2004 killed 11 and injured more than 180 people. An August 2003 terrorist bombing at a major international hotel in Jakarta killed 12 persons and injured scores, including several American citizens. A terrorist attack in Bali in October 2002 killed 202 people, including seven Americans. Suicide bombers wearing explosives in vests or backpacks carried out the 1 October 2005 bombings in Bali. Prior terrorist attacks involved the use of vehicle-borne explosives. In addition, sectarian, ethnic, communal, and separatist violence continue to threaten personal safety and security in several areas.

Over the past three years, domestically targeted bombings have struck religious, political, and business targets. In 2003, the Jakarta International Airport, an open-air concert in Aceh, and other Indonesian Government facilities were bombed. Americans should avoid travel to Aceh. Northern parts of the island of Sumatra, and particularly the province of Aceh, suffered severe damage following an earthquake and a series of tsunami waves on 26 December 2004. Although reconstruction efforts are underway, communications infrastructure, roads, medical care, and tourist facilities on the western and northern coasts of Sumatra and on coastal islands off Sumatra were seriously damaged and have not yet been fully restored. Infrastructure on the island of Nias was seriously damaged in an earthquake on 28 March 2005.

Adequate lodging facilities are difficult to find in Aceh and Nias. Americans should not travel to Aceh to participate in humanitarian relief efforts except under the auspices of a recognized assistance organization that has permission to operate in Indonesia. The Government of Indonesia and the free Aceh movement (GAM) signed a peace accord on 15 August 2005, officially ending armed hostilities. However, the overall security situation in Aceh remains unsettled. Humanitarian workers should be cautious of their security when traveling in

Aceh due to the continuing potential for separatist and terrorist violence, which could be directed against American or other Western humanitarian assistance workers. Americans participating in relief efforts should make sure that their organization has facilities in place to accommodate and feed staff and a security plan coordinated with Indonesian authorities. Travel by road after dark is particularly dangerous. All travelers to Aceh should follow health precautions (from the U.S. Centers for Disease Control and Prevention [CDC] at <http://www.cdc.gov/travel>) for travelers to the tsunami area.

Americans considering travel to the province of Papua should exercise extreme caution because of sectarian, ethnic, communal, and separatist strife. Papua's ongoing separatist conflict has the potential to become violent. In August 2002, two Americans were killed in Papua under as yet unresolved circumstances. Americans should avoid travel to Maluku, in particular the capital city of Ambon. Since 25 April 2004, sectarian violence has killed at least 40 and injured more than 220 people. Americans should avoid travel to central, south, and southeast Sulawesi; those considering travel to north Sulawesi should exercise extreme caution. Sporadic violence occurred in Poso and in neighboring areas of central Sulawesi in 2003 and 2004, resulting in several fatalities. Central Sulawesi's general security situation remains unstable; bombings and killings occurred in late 2004 and 2005 in Poso and Palu. A terrorist explosion at Tentana market in Poso, central Sulawesi, on 28 May 2005 killed 22 people. The Philippine-based terrorist Abu Sayyaf group poses an ongoing kidnapping threat in areas near Malaysia and the Philippines. The U.S. Mission in Indonesia restricts U.S. Government employees' travel to certain areas of the country.

For the latest security information, contact a U.S. Mission consular office. The U.S. Mission can occasionally suspend service to the public or close because of security concerns; in these situations, it will continue to provide emergency services to American citizens. Americans who travel to Indonesia despite this Travel Warning should obtain up-to-date health information before departing the U.S. The Websites of CDC at <http://www.cdc.gov/travel> and the World Health Organization at <http://www.who.int> have up-to-date information on outbreaks of contagious and tropical diseases. Americans considering travel to Indonesia should read the Department of State's Fact Sheet on Avian Influenza, dated 3 August 2005, and should consult with

their personal physicians concerning avian flu. Americans living and traveling in Indonesia are urged to register and update their contact information with AmEmbassy Jakarta, AmConsulate General Surabaya, or the U.S. Consular Agent in Bali. Registration facilitates the U.S. Mission's contact with Americans in emergency situations, and may be done online and before travel. Information on registering can be found at the Department of State's consular affairs Website: <https://travelregistration.state.gov>. Registration information and recent warden messages are also available on the AmEmbassy Jakarta website at <http://jakarta.usembassy.gov>. Americans can obtain information on travel and security in Indonesia from the Department of State by calling 1-888-407-4747 within the United States or 1-202-501-4444 from outside the United States and Canada. Americans also can call the AmEmbassy in Jakarta at (62) (21) 3435-9000, the AmConsulate General in Surabaya at (62) (31) 295-6400, and the Consular Agent in Bali at (62) (361) 233-605. American citizens should read the Department of State's Consular Information Sheet for Indonesia and latest Worldwide Caution Public Announcement, both available at <http://travel.state.gov>.

(2) Terrorist/Criminal Threat Level(s). The present Terrorist Threat is **high** and criminal threat is **high** for Indonesia.

(3) Vulnerability Assessment. U.S. personnel are vulnerable to various medical conditions, criminal activity, and injuries incurred as a result of traffic mishaps while transiting to and from the billeting site. The APOE will have host nation security. The off-loaded equipment at the APOE will be secured by interior Guard Force. Personnel and vehicles in transit are vulnerable to attacks from displaced persons attempting to get food and water. Current environment has potential for looters to attempt to gain access into billeting, staging, and port areas.

(4) Risk Assessment. The risk of vulnerabilities being exploited is considered **high** based on mitigating factors that have been implemented through awareness briefings, defense in depth by having personnel billeted and working in secure areas, and the use and cooperation of host-nation civil and military authorities.

(5) Criticality Assessment. TBD

(6) Force Protection Condition. The present force protection condition for Indonesia is **Charlie With Additional Measures**.

(7) Medical Threat. Medical facilities in Indonesia are limited because of the current situation. Surgical Company Bravo (-) will possess an organic medical capability. Infectious diseases, such as malaria, including the severe P. falciparum form, which is resistant to the anti-malaria drug Chloroquine, poses a serious health risk in rural areas throughout the country, in Irian Jaya (the western half of New Guinea), and at the temple complex of Borobudur. There is no malaria risk in the cities on Java and Sumatra and in the main resorts on Bali. The CDC recommends the use of malaria prophylaxis and protective measures to avoid mosquito bites, such as clothing that covers most of the body, insect repellents, and mosquito nets. Refer to the medical plan for specific prevention measures.

(8) Criminal Threat. The current criminal threat for Indonesia is **high**.

b. Friendly

(1) Own Forces Locations. The DAC-PAC will be located in Buntal, Indonesia. Once located, a vulnerability assessment will need to be conducted.

(2) Type and Number of Security Personnel and Equipment. Surgical Company Bravo (-) will possess an organic security element that will provide interior guard over fixed locations and assets. METT-T will be used to determine the required number of personnel. This security element will provide Entry Control Point (ECP), perimeter, area security, and Quick Reaction Force (QRF). In addition, the security element will have Military Police attached to provide Maneuver Mobility Support Operations (MMSO), along with subject-matter expertise in the training and employment of Non-Lethal Weapons (NLW) to deal with potentially hostile displaced persons and refugees. Their primary mission is to protect personnel and equipment in support of the disaster relief and humanitarian assistance mission to Indonesia.

(3) Host nation security capability. Will be established at the APOE.

2. FORCE PROTECTION MISSION. Surgical Company Bravo (-) Commander shall immediately take this plan to develop, implement, and maintain an effective AT/FP posture in order to deter, detect, delay and defend against terrorist attacks; mitigate the effects of an attack, and safeguard personnel, property, and resources to preserve and reconstitute support capabilities following an attack.

3. EXECUTION OF FORCE PROTECTION.

a. Commander's Intent (Force Protection). It is 3D MLG policy to protect military personnel, government facilities, and material resources from acts of terrorism and destructive or potentially destructive events. Surgical Company Bravo (-) will exercise proper caution and sound judgment in reducing individual vulnerability. Awareness of the terrorist threat on the part of the individual is central to every effort to deal effectively with the threat of terrorism.

b. Key Tasks and Responsibilities. Surgical Company Bravo (-)'s Commander is responsible overall for the force protection of the personnel and equipment assigned. The Force Protection Officer is responsible for the implementation of this plan. All personnel are required to complete Level I AT/FP training within the previous 12 months and an AOR threat brief prior to deploying in accordance with reference (f). A pre-deployment brief will be conducted for operation participants at the A/SPOD and will satisfy the above requirements.

c. Concept of Force Protection. The cornerstone of the AT/FP Plan is an alert, educated, combat-ready Marine and Sailor. During day-to-day operations, all personnel will stress continuous AT/FP planning and passive, defensive techniques to deter and prevent terrorist incidents. All personnel have been briefed on immediate action to be taken, location of safe havens, and communication procedures in the event of a terrorist attack.

(1) Intelligence/Counter-Surveillance/Counterintelligence. Counterintelligence agents will support the operation. The FPD Maj Shelton, U.S. Army, is available for local threat information. The Embassy FPD, DAC-PAK FPO, Antiterrorism Officer, and an Intel Marine will form the nucleus of the Threat Working Group (TWG), and will meet periodically to assess the local threat. Any significant changes to the threat

will be immediately briefed to the Commander for appropriate action.

(2) Deployment/travel security measures.

Currently, all area personnel will be traveling through or working in area at deployed unit FPCON Charlie. Measures from increased FPCONS will be selected and implemented as part of the operation's Random Antiterrorism Measure (RAM) Program. RAMs provide a different look at security procedures in effect to deny the terrorist surveillance team the opportunity to accurately predict security actions. Refer to Tab C for operation RAMs. The Commander will approve these RAMs to be implemented based on the TWG recommendations. All personnel will maintain in their possession a list of emergency contact numbers and communication procedures.

(3) Access control/entry control procedures.

(a) Personnel access procedures. The Security Element will establish a duty at the billeting site to control access and evacuate the building if necessary. Any guests and visitors will be escorted at all times, and will not be allowed to be unaccompanied at any time in billeting or work areas.

(b) Material access. The Security Element will control material access into the camp. The billeting duty will screen all packages and contact the person it is addressed to (to personally sign for it). If the addressee is not available, the delivery person will take the package and attempt to deliver at it a later time. At no time will unknown packages be allowed in the billeting or work areas. Personnel will not accept any unsolicited packages.

(c) Vehicle access/search area procedures. Security Element Marines will control vehicle access into the camp entry control points (ECP). The Security Element Marines will conduct a thorough search of all vehicles for improvised explosive devices (IEDs) and other tampering that could cause harm to occupants. All vehicles will be parked in well-lit screened areas and safe distances away from billeting sites as much as possible. At no time should any vehicle be allowed to park within 25 meters of billeting area. UFC 4-010-01 sets standards for parking standoff distances within a controlled perimeter and outside a controlled perimeter. Within a controlled perimeter, the minimum standoff distance for billeting and high occupancy family housing and primary

gathering buildings is 25 meters, whereas the standoff distance is 10 meters for inhabited buildings. Outside a controlled perimeter, the minimum standoff distance for all buildings is 10 meters. Refer to Tab E, Bomb Threat Procedures, for further details on searching for and identifying IEDs.

(4) Physical Security. The physical security plan, Tab M, includes measures to detect, deter, and delay terrorism by conducting ongoing assessments of the situation and procedures for immediate notification of an incident to higher headquarters. The following paragraphs describe the physical security measures for Surgical Company Bravo (-).

(a) The camp assessment is currently being conducted and will provide a terrain analysis that will assist the security force in providing an effective force protection posture with limited resources. Refer to Tab K for port assessment.

(b) Critical facilities and infrastructure. Refer to Tab D for the Surgical Team Bravo criticality assessment.

(c) Off-installation residential locations. TBD.

(5) Subsistence protection. (Food and water protection). The following paragraphs address the procedures required to prevent terrorists from contaminating food and water sources, and response measures if sources are contaminated. Efforts must be made to ensure that AT considerations are part of all contracting operations. Refer to reference (f), paragraph 13-5, logistics and contracting AT concerns.

(a) Food. Meals Ready to Eat (MREs) are part of the subsistence plan. The Camp dining facilities will be inspected for sanitation prior to any U.S. personnel being authorized to subsist from them. Health Service Support Element (HSSE) will provide food sanitation awareness training during the pre-deployment brief.

(b) Water. Operation participants will consume contracted bottled water. Adequate security measures will be in place to prevent unauthorized tampering of the water source. Consumption of local water should be avoided unless first tested by medical personnel for proper sanitation.

(6) Off-installation travel/convoy security. Traveling off the installation in uniform will be minimized as much as possible. At no time will anyone travel off the installation alone. Minimum two-man rule will be in effect. Off-base personnel will maintain some form of communication with the CP in the form of cell phones or radios. Off installation, the host-nation authorities will provide security and the Security Element. Convoys will move using the traveling technique by maintaining visual contact with each other. Vehicle operators will maintain dispersion between vehicles to avoid getting "boxed" in. All convoys will maintain communication with the CP, and internally to the convoy. Host-nation vehicles and operators will be used to transport Surgical Company Bravo (-)'s personnel to and from billeting sites. Refer to Tab J, MSR Assessment.

(7) Plan for arming personnel. Surgical Company Bravo (-)'s Security Element who has qualified with the M9 will carry the weapon concealed and be armed with a combat load. All interior guard members will be qualified with the weapon they will carry. Guard Force training will include, at a minimum, use of force, Rules of Engagement, weapons handling, and immediate action drills in accordance with reference (g). U.S. personnel bearing weapons will be in accordance with the U.S./Host Nation Agreement and reference (g).

(8) Rules of Engagement (ROE). ROE training has been provided pre-deployment by the SJA, Capt J.D. Rosen. The Force Protection Element has received two additional training sessions.

(9) Use of deadly force training for security and law enforcement personnel. The interior guard will receive a class on deadly force and sign a deadly force acknowledgment form prior to assuming any security duties. U.S. military authorities' rights to exercise criminal and disciplinary jurisdiction over military personnel will be in accordance with the UCMJ and the U.S./Host Nation Agreement.

(10) Terrorist incident response measures. If Surgical Company Bravo (-)'s personnel should come under a terrorist attack, they will immediately take cover and communicate the situation to organic and host-nation authorities for security, fire, and medical response. Surgical Company Bravo (-)'s personnel will mitigate the attack by maintaining accountability

of personnel and rendering medical aid to the wounded/injured. Refer to Tab L for emergency evacuation plan.

(a) Medical. Emergency medical response capability will be provided by Surgical Company Bravo (-). While away from the billeting/work areas, refer to Tab F for emergency contact information.

(b) Firefighting. Refer to Tab F.

(c) Explosive Ordnance Disposal (EOD). Host-nation EOD capability in Indonesia is undetermined at this time. Refer to Tab E for Bomb threat procedures.

(11) AT/FP Training. The following paragraphs include the Surgical Team Bravo site-specific training requirements.

(a) Formal training. The Commander conducted a mandatory pre-deployment brief for all personnel prior to embarkation at the A/SPODs. The briefing included Level I training, AOR threat brief, cultural awareness training, medical/health concerns, and other information to fully implement this plan. Individuals can also complete Level I training at www.at-awareness.org; password is AWARE.

(b) Initial training. Once in theater, all personnel will become situationally aware of the operational area and facilities through the Company leadership. All personnel will know locations of safe havens, local security forces, and emergency phone numbers.

(c) AT/FP Exercise. During the initial phases of the deployment, the TWG will de-conflict this plan with the NCIS, CI, and host-nation authorities. At a minimum they will test communication capability among the training areas, NCIS, and emergency services.

(12) Weapons of Mass Destruction (WMD) measures. On a continuing basis and in conjunction with host-nation support, personnel will be prepared to respond to a WMD incident by conducting pre-incident planning and mitigation measures and performing crisis response/consequence management operations aimed at lessening the effects of a WMD incident once they occur. Based on the limited capabilities of the unit, situational awareness of the exercise participant is critical. Our best defense against a WMD attack is by preventing an attack

or limiting its effects through vigilance. Everyone is tasked to immediately report any suspicious activity to authorities, and sound the "alarm" to evacuate personnel to a safe area. The TWG needs to coordinate with host-nation authorities through NCIS for host-nation WMD capabilities. Refer to Tab N, WMD Plan for further details.

(13) Conduct While on Liberty. Personnel will adhere to the III MEF Liberty Campaign Order 1020.2a. The operational commander will establish specific liberty guidelines. All personnel are required to have a liberty buddy. At no time will anyone under 21 years of age consume alcoholic beverages. Personnel authorized to consume alcohol will do so in moderation. Exercise caution and good judgment while on liberty. Avoid poorly lit areas and "seedy night clubs/bars." Stay clear of any public demonstrations and respect local customs. Maintain a low profile and avoid any activity that draws attention to yourself. If any suspicious activity is observed, immediately report it to the chain of command.

4. ADMINISTRATION AND LOGISTICS

a. Administration. Each person will maintain a list of emergency contact numbers while in Indonesia. Refer to Tab F for complete list.

b. Logistics. The following paragraphs detail the specialized or unique equipment and materials required for the AT Mission directed by the plan.

(1) Transportation of Weapons. Weapons will be maintained in the Surgical Company Bravo (-) Armory and transported from the airfield to the operation area via contracted host-nation vehicles.

(2) Maintenance/Storage of Force Protection-Related Arms and Equipment. Interior Guard weapons and ammo will be stored in accordance with regulations. Surgical Company Bravo (-) is assigned an MOS 2111 Armorer. Weapons and ammo will be secured by an armed guard or an Intrusion Detection System with a 15-minute armed response capability in accordance with reference (e).

(3) AT measures in the contracting process. All deployment contracts will be completed in accordance with paragraph 13-5 of reference (f).

5. COMMAND AND SIGNAL

a. Command

(1) C2 for Force Protection. The Commander is responsible overall for the execution of the force protection mission. The Interior Guard Force day-to-day activities will be controlled by the guard officer who will report to the commander. Surgical Company Bravo (-) has established a TWG consisting of a Force Protection Officer, Force Protection Chief, and Intel Marine. The TWG will maintain contact with the U.S. Embassy Force Protection Diplomat and host-nation authorities to ensure smooth lines of communication and current local threat info. The TWG will ensure this information is passed to the Surgical Company Bravo (-)'s personnel to increase situational awareness and vigilance on the part of the individual. Each individual will incorporate this information into their daily routine.

(2) Component/Supporting Agency chain of command and responsibilities. N/A

(3) AT Cell composition.

- (a) Commander. (Name)
- (b) Surgical Co. FPO. (Name)
- (c) Surgical Co. FP Chief. (Name)
- (d) Intel. (Name)
- (e) FPD US Embassy Indonesia. (Name)

b. Signal. The following paragraphs contain the equipment requirements and the measures taken to ensure communications to support the AT mission.

(1) Internal Force Protection Notification System. Cell phones, international phones, PRC 119s, PRC 148s.

(2) Mass notification system. Refer to Tab L emergency evacuation plan.

(3) External communication capabilities. TBD. Landline Phone, Cell Phone, SAT Phone, SIPRnet/NIPRnet.

(4) Suspicious Incident Report. Refer to Tab G for sample report.

(5) Blue Dart. Procedures for passing time-critical threat warning information from the information collector to the threatened U.S. units or personnel. Refer to Tab H for blue dart procedures.

TABS:

- A - NCIS Threat Assessment for Indonesia
- B - Force Protection Conditions
- C - MAGTF RAMs
- D - MAGTF Criticality Assessment
- E - Bomb Threat Procedures
- F - Emergency Contact Numbers
- G - Suspicious Incident Report
- H - Blue Dart Procedures
- I - Billeting Assessment
- J - MSR Assessment
- K - Port Assessment
- L - Emergency Evacuation Plan
- M - Physical Security Plan
- N - WMD Plan

Reviewed and approved by:

APPENDIX C

SAMPLE RESERVE AT PLAN

UNITED STATES MARINE CORPS
UNIT NAME
UNIT ADDRESS

From: Inspector-Instructor/Commanding Officer
To: Distribution List

Subj: Installation/Unit/Facilities (NAME) ANTITERRORISM PLAN
(Date)

Ref: (a) DoD Directive (DoDD) 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(b) DoD I (DoDI) 2000.16, "DoD Antiterrorism Standards," October 2, 2006
(c) DoDI 2000.18, "DoD Installation Chemical Biological Radiological Nuclear and High Yield Explosive Emergency Response Guidelines," December 4, 2002
(d) Marine Forces North Anti-Terrorism OPOD 06-01
(e) MCO 3302.1D, "The Marine Corps Antiterrorism/Force Protection (AT/FP) Program," July 18, 2002
(f) MCO 5530.14, "The Marine Corps Physical Security Program Manual," December 21, 2000
(g) Force Order 3300.1, "Marine Forces Reserve Antiterrorism/Force Protection (AT/FP) program," July 20, 2000
(h) BN or DIV Order
(i) Installation/Facility Antiterrorism Order (if applicable TENANT COMMANDS)

Encl: (1) Task Organization (Annex A)
Appendix 1: Command Relationships
Appendix 2: Working Groups

(2) Intelligence (Annex B)
Appendix 1: Travel Security
Appendix 2: Threat Assessment
Appendix 3: NCIS

(3) Operations (Annex C)
Appendix 1: Daily Procedures
Appendix 2: FPCON Matrix
Tab A: FPCON Implementations
Exhibit 1: RAMS Matrix

Appendix 3: Operational Security
Appendix 4: Information Awareness
Appendix 5: Incident Response
 Tab A: Security Forces/Reaction Forces
Appendix 6: Public Affairs
Appendix 7: Antiterrorism Training and Exercises
Appendix 8: Communication
Appendix 9: Safety
Appendix 10: COOP Plan
 Tab A: Bomb Threat
 Exhibit 1: Bomb Threat Procedures
 Tab A: Destructive Weather
 Tab B: Terrorist Incident
Appendix 11: CBRNE Plan
 Tab A: HazMat
Appendix 12: Reports
 Tab A: Monthly
 Tab B: Annual
Appendix 13: Mail-Handling Procedures

- (4) Physical Security (Annex D)
 - Appendix 1: Physical Security Survey
 - Appendix 2: Barrier Plan
- (5) Logistics (Annex E)
- (6) Fiscal (Annex E)

1. Situation

a. General. To establish policy, responsibilities, procedures and standards for the (Unit Name) Anti-Terrorism (AT) Program to include facilities and personnel in accordance with references (a) through (i). Commander, (Unit Name) views Force Protection as an overarching concept that includes those procedural and leadership principles necessary to ensure the safety and well-being of Marines, their dependents, other service members, Department of Defense (DoD) personnel and civilian employees.

b. Terrorism. Terrorism, as defined in references (a) through (i), is the calculated use of violence or threat of violence to instill fear. Its purpose is to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Terrorism has

shifted from the traditional cell organization to a highly skilled mobile attack force.

c. Enemy Forces. The enemy is any adversary, foreign or domestic, capable of threatening the Marine Corps' personnel, facilities, and equipment and/or interfering with the execution of the mission. Potential enemy forces may include:

- a. International Terrorist Groups
- b. Domestic Terrorist Groups
- c. Criminal Activity
- d. Destructive Weather

d. Friendly. (Unit Name) is committed to protecting their resources while providing for the Nation's defense. Recognition of the dangerous and enduring nature of the terrorist threat drives the unit/facilities to establish and implement a comprehensive and well-defined AT program. Need to include POC for local police, FBI, NCIS, FEMA, local hospitals

e. Assumptions. For the purpose of this plan, a threat is defined as any condition or event that occurs within the (Unit Name) AOR that may have an adverse impact on human life, resources, or mission accomplishment that requires (Unit Name) personnel to institute appropriate measures to address, respond, deter, and/or mitigate that condition. To assist in the planning, the following incidents constitute a threat:

- a. Hazardous Material Spills
- b. Weapons of Mass Destruction
- c. Mass Casualty Incidents
- d. Increasing Force Protection Conditions Based on Intelligence on Criminal or Terrorist
- e. Bomb Threats
- f. Any one or Combination of Incidents at a Training Center

(1) (Unit Name) as a whole or part is vulnerable to criminal/terrorist incidents because of the geographical location of the facility, diverse missions of assigned units, and overall accessibility.

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

(3) Sound security measures, randomly implemented, are viable and visible deterrents to criminals and terrorists.

2. Mission. The goal of the (Unit Name) AT program is to educate and train Marines, Sailors, civilian employees, and family members to protect themselves at home and abroad from acts of terrorism. MARFORRES will detect and deter acts of terrorism by a collective effort that synchronizes Force Protection (FP) elements in order to reduce the likelihood that MARFORRES personnel, their families, facilities, and materiel will be subjected to a terrorist attack. FP is a Commander's responsibility. However, it is also an individual's responsibility to be vigilant and proactive in daily practice.

a. Commanders at all levels are required to integrate the standards of reference (a) through (i) into their AT programs.

b. Deter Terrorist Incidents: (Unit Name) will deter terrorists from targeting, planning against, or attacking the installation/facility personnel and assets by communicating a firm intent and resolve to defeat terrorism.

c. Employ Countermeasures: (Unit Name) will employ the appropriate mix of countermeasures, both active and passive, to prevent terrorists from attacking personnel and assets.

d. Mitigate the Effects of a Terrorist Incident: (Unit Name) will employ the full range of active and passive measures to lessen the impact of potential terrorist events.

e. Recover from a Terrorist Incident: (Unit Name) will design plans to quickly recover from the effects of a terrorist incident in an effort to rapidly resume the unit's mission.

3. Execution

a. Commander's Intent

(1) Purpose. (Unit Name) will remain the most effective force possible against a rapidly changing threat environment, accented by asymmetrical warfare and the continuing Global War on Terrorism (GWOT), by ensuring that AT is embedded into (Unit Name) planning, operations, and culture.

a. All Marines, civilians, and family members will be prepared in the event of an "ALL-HAZARDS INCIDENT."

b. (Unit Name) will ensure that the AT plans are fully coordinated and synchronized throughout the chain of command.

(2) Concept of Operations. (Unit Name) AT operations will consist of three phases: pre-incident, incident, and post-incident. During these three phases, actions will range from baseline antiterrorism physical security measures through progressively increasing actions, from FPCON ALPHA to FPCON DELTA, through consequence management measures.

a. In accordance with references (a) through (i), (Unit Name) will implement AT operations through the following elements:

1. Threat Assessment: effective inter-agency intelligence and counterintelligence analysis is essential to identify the terrorist threat and to provide warning about potential terrorist attacks.

2. Identification of Critical Assets: the identification of likely threat(s) assists in determining critical personnel, facilities, and equipment.

3. Vulnerability Assessments: threat likelihood coupled with identified critical assets assists in determination of vulnerabilities; areas that require mitigation or enhancements of procedural and programmatic requirements.

4. Incident Response Capability Assessments: an effective incident response strategy and capability can contribute to deterring terrorist attacks if adversaries recognize our ability to limit the effects of their attacks.

5. Risk Assessments: after weighing threats to assets, critical assets, vulnerabilities, and incident response capability, risk levels are established and prioritized and a strategy is developed to guide all members of the Antiterrorism Working Group (ATWG) toward strengthening our posture.

6. Planning: a comprehensive AT plan provides maximum protection to personnel and other assets, and includes specific FPCONs, physical security measures, and AT courses of action clearly tailored to address possible threats and vulnerabilities, as well as specific terrorist consequence management and response procedures. These measures shall include procedures for determining the nature and scope of incident response; procedures for coordinating security, fire, and

medical first responders; and steps to reconstitute the unit's ability to conduct its mission and perform AT measures.

7. Training and Exercises: training increases the awareness level of personnel and fosters a mindset focused on prevention of terrorist acts; exercises provide an opportunity to test AT plans, the ability to transition between FPCONs, and the opportunity to practice the skills taught in terrorism awareness training.

8. AT Resource Requirement Documentation and Submission: the efficient management of scarce resources is key to the success of the AT Program. The identification of AT resource requirements should be related to an assessed vulnerability or risk; documentation and submission of these requirements should be accomplished in an accurate and timely fashion via the chain of command.

The focal point for development, implementation, and assessment of the installation/facility AT program is the ATWG.

The AT plan establishes a baseline AT posture that is to be maintained while conducting normal operations and, when required, serves as the foundation for developing and executing increased appropriate reactive measures, as defined in this AT plan.

(3) End State. This order is to ensure effective command, control, and coordination by using common terminology, methodology, and reporting procedures.

4. Task Organizations

a. Antiterrorism Working Group (ATWG). The ATWG will meet semi-annually or as required to review and discuss the terrorist threat and assess vulnerabilities, all-hazards and AT plans, funding, and construction projects. The ATWG is designed to provide the Site Commanding Officer with advice and recommendations on combating terrorism for personnel, assets, and facilities. At a minimum, the ATWG will consist of the following members: Site Commanding Officer, Site Executive Officer, AT Officer, Fiscal/Supply, S-2, S-4, Medical, Legal, PAO, other tenant commands and, if possible, local law enforcement officials.

b. Site Commander. Will stay consistent with ref (a) through (i) and assumes overall responsibilities for planning, programming, training, exercising, and executing AT measures and courses of action under this plan.

1. Provide AT developmental and managerial guidance.

2. Maintain control and jurisdiction over all incidents until management responsibilities have been assumed by another agency that has been designated as having primary jurisdiction for such incidents.

3. Declare site FPCON levels based on intelligence or the authority of higher headquarters.

4. Serve as Crisis Management Team (CMT) Commander.

c. Executive Officer. Maintain primary staff cognizance for the preparation, implementation, and revision of this plan and its supporting elements.

1. Maintain the primary responsibility for the development of AT operations.

2. Maintain the primary responsibility for the development of Critical Infrastructure Protection.

3. Serve as the Chairperson for the site ATWG.

4. Serve as the Deputy Commander of the CMT.

5. Develop and maintain the capability to staff and operate a primary and alternate Emergency Operations Center (EOC).

6. Ensure an officer is appointed, trained, and provided with the appropriate staff support to function as the site AT Officer.

7. Ensure the site's threat assessment is current.

8. Coordinate AT training program and plan, develop, and conduct AT exercises and evaluations at least annually.

9. Conduct other tasks as directed in support of this plan.

d. Antiterrorism Officer. Will develop a comprehensive site AT plan.

1. Serve as Deputy Chairperson and coordinator for the ATWG.

2. Compile a prioritized list of mission essential assets.

3. Identify all critical assets.

4. Identify all vulnerabilities.

5. Assess site incident response capabilities.

6. Establish risk priorities.

7. Develop site-specific FPCON measures, random antiterrorism measures (RAM), and AT courses of action.

8. Ensure AT plan complies with DoD, CJCS, Service requirements, and host command if applicable.

9. Ensure AT plan is coordinated with local, state, and Federal agencies, as appropriate.

10. Coordinate and submit the identification, compilation, and submission of AT resource requirement projects and unfunded requirements.

11. Coordinate individual and organizational AT training requirements and annual site AT exercises.

12. Conduct other tasks as directed in support of this plan.

e. Fiscal/Supply. Assumes the primary responsibilities for developing AT program resource management detailing the concept of fiscal support to the AT program and complies with associated tasks and responsibilities.

1. Ensure AT funding requirements are included in the site's programming and budgeting process.

2. Provide quarterly AT funding status to the ATWG.

3. Identify, compile, and report, in coordination with the ATWG, AT unfunded requirements.

4. Develop and implement procedures capturing AT-related expenses during all phases of the AT plan.

5. Establish and implement procedures for emergency purchasing.

6. Provide representative(s) for the CMT, ATWG, and EOC.

7. Conduct other tasks as directed in support of this plan.

f. Intelligence Office. Assumes the primary responsibility for the development of intelligence procedures detailing the concept of intelligence support to AT operations and complies with associated tasks and responsibilities.

1. Develop and maintain a terrorist threat intelligence collection and analysis program in support of this plan. In support of this effort, establish a Threat Information Fusion Cell.

2. Develop and update an annual site-specific threat assessment.

3. Develop and maintain liaison with Federal, State, and local agencies to ensure the unilateral exchange of international and domestic threat information.

4. As required, support security details.

5. Provide representative(s) to the CMT, ATWG, and EOC.

6. Be prepared to support the site AT training program, as required. Conduct country-specific Level I briefs.

7. Conduct OCONUS briefs and request forms and associated paperwork for members of the command seeking to go OCONUS for any reason.

8. Conduct other tasks as directed in support of this plan.

g. Logistics. Assumes the primary responsibility for developing logistical procedures detailing the concept of logistical support to AT operations and complies with associated tasks and responsibilities.

1. Coordinate with necessary external sources for emergency logistical support.

2. Ensure all logistical support and emergency support contracts include AT considerations when formulating contracting requirements, award, execution, and evaluation process.

3. Provide representative(s) to the CMT, ATWG, and EOC.

4. Be prepared to support the site AT training program, as required.

5. Conduct other tasks as directed in support of this plan.

h. Medical. Assumes the primary responsibilities for development of Medical Services and Health protection procedures, detailing the concept of medical as it pertains to AT operations, and complies with associated tasks and responsibilities.

1. Establish and maintain the capability to execute emergency medical services, to include basic lifesaving measures and procedures to treat Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE)-contaminated victims.

2. Maintain adequate medical supplies for medical emergencies.

3. Be prepared to establish emergency morgue services.

4. Provide representative(s) to the CMT, ATWG, and EOC.

5. Conduct other tasks as directed in support of this plan.

i. Facilities Officer. Assumes the primary responsibility for the development of AT Construction Standards and Procedures, detailing the concept of fiscal support to AT operations, and complies with associated tasks and responsibilities.

1. Review and approve construction and renovation designs and plans for all inhabited structures to ensure compliance with AT construction standards. Ensure standards are met in the design, construction, modification, and acceptance phases.

2. Ensure all public works support and emergency support contracts include AT considerations during contracting requirements, award, execution, and evaluation process.

3. Compile and report damage assessment information.

4. Provide representative(s) to the CMT, ATWG, and EOC.

5. Develop a tracking system to monitor and report AT projects.

6. Conduct other tasks as directed in support of this plan.

j. Public Affairs Officer. Assumes the primary responsibility for the development of Public Affairs procedures that detail the concept of public affairs support to AT operations, and complies with associated tasks and responsibilities.

1. Operate as the spokesperson for the (Unit Name) site commander.

2. Initiate liaison with local media as appropriate.

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

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

5. Establish a command Information Bureau, as required, to address media queries and news releases.

6. Provide representative(s) to the CMT, ATWG, and EOC.

7. Conduct other tasks as directed in support of this plan.

5. Coordinating Instructions. It is imperative that all AT matters are well coordinated among all personnel. The conduit for all such coordination will be the AT Officer and the ATWG. This does not preclude direct liaison between sections, but the resident experts in the ATWG will facilitate the resolution of most AT issues. Issues not resolved in this manner shall be forwarded to the site Commander via the AT Officer for resolution.

1. Be prepared to implement portions of this plan for prolonged periods of time.
2. Ensure applicable training requirements are fulfilled.
3. Capture costs associated with implementation of this plan and provide appropriate reports and unfunded requirements to the Fiscal Officer.
4. Prepare and submit reports and lessons learned as they occur.

APPENDIX D

SAMPLE MEMORANDUM OF AGREEMENT (MOA)

INSTALLATION
1000
O&T AT/FP
XX Apr 08

MEF
1000
COPS AT/FP
XX Apr 08

MEMORANDUM OF AGREEMENT (MOA)
BETWEEN
COMMANDING GENERAL, MARINE EXPEDITIONARY FORCE (MEF)
AND
COMMANDING GENERAL, MARINE CORPS INSTALLATIONS

Subj: MOA FOR EMERGENCY NOTIFICATION,
INFORMATION SHARING, SECURITY AUGMENTATION, AND MEF
SUPPORT TO
MARINE CORPS INSTALLATION BASES AND STATIONS DURING A
CRISIS EVENT

Ref: (a) Marine Corps Base, Force Protection Plan 04
(b) Marine Corps Air Station, Anti-Terrorism Plan 06
(c) Marine Corps Air Ground Combat Center, Anti-
Terrorism Force Protection Standard Operating Procedures
(d) Marine Corps Air Station, Anti-Terrorism/Force
Protection (AT/FP) Plan
(e) Marine Corps Air Station, Anti-Terrorism (AT) Program
(f) MCO 3302.1D The Marine Corps Anti-Terrorism/Force
Protection (AT/FP) Program

Encl: (1) Threat Information Management

1. Purpose. To provide policy guidance from Marine Corps Installation and MEF to all personnel involved in Physical Security, Anti-Terrorism (AT), and Force Protection (FP) operations aboard installations. This MOA will establish a joint partnership between the Marine Corps Installation and MEF to ensure an effective and efficient AT posture and crisis response. This document is a formal agreement between the two commands and identifies roles, relationships, and responsibilities.

2. Background. Installation Commanding Officers are responsible for the protection of all personnel and property aboard their installations. FP is an inherent command responsibility. It is