



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
3000 MARINE CORPS PENTAGON  
WASHINGTON, DC 20350-3000

NAVMC 3500.103  
PS  
27 Oct 2010

NAVMC 3500.103

From: Commandant of the Marine Corps  
To: Distribution List

Subj: MARINE CORPS ANTITERRORISM (AT) MANUAL

Ref: (a) DOD Instruction 2000.16 of December 8, 2006

1. Situation. Reference (a) outlines the overarching framework for the Marine Corps AT program by imparting specific AT tasks that must be completed at all Marine Corps levels and locations. The AT Manual establishes training and program design recommendations, examples, and standards required to accomplish the specified tasks.

2. Mission. In response to the ever-changing terrorism threat, the Marine Corps employs a combination of Antiterrorism (AT) and Counterterrorism (CT) efforts. AT is an integral component of Combating Terrorism (CbT), and consequently of Force Protection (FP) and Mission Assurance (MA). AT involves planning and the implementing of defensive measures to mitigate or reduce the vulnerability of individuals, forces, and property to terrorist attacks. The AT Manual presents a combination of best practices and tactics, techniques and procedures (TTP's) for how an Antiterrorism Officer (ATO) can design an AT program that best reduces the opportunity for terrorists to target Marine Corps personnel and disrupt the USMC mission. A sound AT program helps to minimize the overall risk of an attack and its negative impact on mission sustainability.

3. Execution

a. Commander's Intent and Concept of Operations.

(1) Commander's Intent.

(a) In an operating environment of constrained resources, and constant and complex threats, the Marine Corps will remain the most effective fighting force possible by ensuring that AT is embedded throughout Marine Corps planning, operations, and daily activities. Multi-faceted, comprehensive AT programs must nest within the overarching USMC Mission Assurance construct, take an "all-hazards" threat approach to planning, be proactive in nature, and be coordinated and synchronized throughout appropriate commands.

(2) Concept of Operations

(a) This Publication is distributed to ensure effective command, control, and coordination by utilizing common terminology, methodology, and reporting procedures.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

NAVMC 3500.103

(b) AT has five essential program elements: Risk Management, Planning, Training and Exercises, Resource Application, and Comprehensive Program Review. Commanders at all levels are required to develop prescriptive and comprehensive AT plans that include these five essential AT program elements.

5. Administration and Logistics. Recommendations concerning changes to this publication may be forwarded to CMC (PS) via the appropriate chain of command.

6. Command and Signal

a. Command. This Publication is applicable to the Marine Corps Total Force.

b. Signal. This Publication is effective on the date signed.



R.F. GEOFFROY  
Assistant Deputy Commandant  
(Security)

DISTRIBUTION: PCN 10031982300

NAVMC 3500.103

TABLE OF CONTENTS

CHAPTER

INTRODUCTION . . . . . 1

ANTITERRORISM PLAN DEVELOPMENT. . . . . 2

RISK MANAGEMENT FUNDAMENTALS. . . . . 3

INFORMATION FUSION . . . . . 4

INCIDENT/EVENT RESPONSE AND MANAGEMENT  
CAPABILITIES. . . . . 5

REPORTING . . . . . 6

ANTITERRORISM TRAINING . . . . . 7

EXERCISES . . . . . 8

RESOURCE APPLICATION AND FUNDING . . . . . 9

PROGRAM REVIEW . . . . . 10

PHYSICAL SECURITY. . . . . 11

ANTITERRORISM-RELATED CONSIDERATIONS . . . . . 12

APPENDICES

- APPENDIX A - Sample Installation AT Plan
- APPENDIX B - Sample Expeditionary AT Plan
- APPENDIX C - Sample Reserve AT Plan
- APPENDIX D - Sample Memorandum of Agreement (MOA)
- APPENDIX E - Sample FPCON Action Sets
- APPENDIX F - Sample FPCON Change Report
- APPENDIX G - Sample RAM Program
- APPENDIX H - Sample Separate AT Plan
- APPENDIX I - Individual AT Plan Checklist
- APPENDIX J - Sample Individual AT Plan
- APPENDIX K - Installation Emergency Response Priority  
Planning Template
- APPENDIX L - Sample Design Basis Threat
- APPENDIX M - Risk Management Worksheet
- APPENDIX N - Sample Local Vulnerability Assessment
- APPENDIX O - ASSESSMENT Mitigation Plan / GO/FO Letter
- APPENDIX P - Sample Vulnerability Mitigation Report
- APPENDIX Q - Exercise Timelines
- APPENDIX R - Sample Expeditionary AT Plan for Initial Site  
Survey/ Initial Planning Conference (ISS/IPC)

APPENDIX S - References and Resources

APPENDIX T - Web Sites

APPENDIX U - Source Spreadsheet

CHAPTER 1  
INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	1000	1-1
PURPOSE.....	1001	1-2
OBJECTIVES.....	1002	1-2
METHOD.....	1003	1-2

## CHAPTER 1

### INTRODUCTION

1000. GENERAL. Terrorism continues to require the utmost attention at Marine Corps facilities worldwide. In response to this asymmetrical and amorphous threat, the Marine Corps combats terrorism through antiterrorism (AT) and counterterrorism (CT) efforts. This AT Manual focuses on AT, an integral component of combating terrorism, and consequently of force protection and mission assurance (MA). AT involves defensive measures to reduce the vulnerability of individuals, forces, and property to terrorist attacks. In particular, this AT Manual explains how an Antiterrorism Officer (ATO) can design an AT program that best reduces the opportunity for terrorists to target Marine Corps personnel and derail their mission. A sound AT program helps to minimize the overall risk of an attack and its negative impact on mission sustainability.

1. Mission Assurance (MA). MA is an all-hazards process that synergizes security program activities and protection functions, such as force protection; AT; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) defense; readiness; and installation preparedness. The MA process is designed to foster a more robust protection posture by integrating protection policies, guidance, and operations; facilitating coordination and collaboration across all functional protection areas; and reducing the duplication of efforts. This synergistic process aids the Marine Corps in mobilizing, deploying, supporting, and sustaining military operations throughout the continuum of operations.

The end state of mission assurance is protection. Protection, as defined in JP 1-02 Department of Defense (DoD) Dictionary of Military and Associated Terms, is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. A robust protection posture requires a holistic, synchronized construct, which mission assurance provides. While this manual will help ATOs create an effective AT program, it is important for ATOs to recognize that coordinating and collaborating with other protection programs significantly increases the effectiveness of

an AT program and will better achieve the ultimate goal of protection.

1001. PURPOSE. Marine Corps Order (MCO) 3302.1E drives this AT Manual and outlines the overarching framework for the Marine Corps AT program by imparting specific AT tasks that must be completed at all Marine Corps levels and locations. This AT Manual is intended to explain the processes required to accomplish the specified tasks. In general terms, this AT Manual is the "how-to" AT handbook for the Marine Corps. It should offer a clearer picture of how AT is to be addressed within the Marine Corps.

This AT Manual differs from Department of Defense Instruction (DoDI) 2000.16 and Department of Defense (DoD) O-2000.12-H. DoDI 2000.16 provides general AT standards to which all services must adhere. DoD O-2000.12-H recommends universal AT procedures based on the standards in DoDI 2000.16. The AT Manual takes AT within the Marine Corps another step further. It supplements DoDI 2000.16 and DoD O-2000.12-H by providing the Marine Corps with a clear, efficient, and effective method to achieve a robust AT program. This step is important in successfully protecting the Marine Corps mission, its personnel, and its assets from the threat of terrorism.

1002. OBJECTIVES. The purpose of the AT Manual is achieved through the following objectives:

- Provide a clear, user-friendly handbook that gives ATOs a body of information needed to create an effective AT program.
- Address AT from all viewpoints: operating forces, expeditionary forces, bases, stations, and facilities.
- Address AT from the ATOs' perspective.
- Provide Commanders and ATOs with a resource on AT best practices so they have the knowledge, tools, and insight to create the most comprehensive and effective AT program, and so they will be best prepared to successfully respond to an incident.

1003. METHOD. To meet the purpose and objectives of this AT Manual, there are several overarching principles that should be employed throughout the AT process.

1. Commander's Role. AT is the Commanders' responsibility. Commanders must execute an AT program that complies with DoD and Headquarters Marine Corps (HQMC) policy within their geographic Combatant Command (COCOM). Although ATOs typically conduct the day-to-day AT duties, it is the ultimate responsibility of the Commander to develop, implement, and sustain an effective AT program that will deter, detect, delay, and defend against an attack; to mitigate the effects of an attack; and to preserve and reconstitute Marine Corps combat power following an attack.

The Commander holds the most important role in AT planning and program execution, and should assume an active role in the AT program by offering guidance and oversight that drives the entire AT process. Before AT planning begins, the Commander must define the mission and explain key AT objectives so an ATO can develop a program tailored toward preserving the mission and attaining the Commander's objectives. The Commander's role does not end at the planning process. Continued guidance must be provided, prudent risk decisions must be made, and AT funding must be pursued. It is critical that the Commander remain involved throughout the entire AT process. Failure to remain involved can result in severe lapses in communication, leading to programmatic gaps. These gaps can cripple the effectiveness of an AT program.

2. All-Hazards Approach. The threat of diverse hazards—terrorist attacks, natural hazards, disease epidemics, criminal offenses, and accidents—requires the Commander to develop a multifaceted and comprehensive Mission Assurance program. This AT Manual is designed to provide ATOs with the guidance and tools needed to properly assess and mitigate the risks of all hazards—not only those associated with terrorism. An all-hazards approach does not reduce the need to focus on AT-related issues; it simply incorporates all-hazards risk analysis into the overall process so the Marine Corps will be more resilient and prepared for any potential threat.

Planning for all hazards does not imply that all risks can be eliminated. It ensures that Commanders have an accurate risk picture to determine what risks, both natural and manmade, should be addressed. In knowing what risks to address, the AT program will help the mission assurance program use all of its security capabilities (Critical Infrastructure Protection [CIP], CBRNE, physical security, etc.) to better protect Marine Corps elements and personnel.

3. Scope of AT Manual. The boundless threat of terrorism demands that this AT Manual place equal weight on the development of installation-specific and expeditionary-focused AT protocol. Even though there are differences between the AT-related requirements and operations of installation and expeditionary forces, many similarities exist that can be concurrently addressed. Although expeditionary forces typically face more complex situations, the overall principles in this AT Manual should guide all ATOs, regardless of station.

CHAPTER 2

ANTITERRORISM PLAN DEVELOPMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	2000	2-1
AT PLAN REQUIREMENTS.....	2001	2-1
AT PLAN DEVELOPMENT.....	2002	2-3
WORKING GROUPS.....	2003	2-6
TYPES OF AGREEMENTS.....	2004	2-9
FORCE PROTECTION CONDITIONS (FPCONS).....	2005	2-10
SUPPLEMENTARY AT PLANNING.....	2006	2-14
DESIGN BASIS THREAT (DBT).....	2007	2-16

## CHAPTER 2

### ANTITERRORISM PLAN DEVELOPMENT

2000. GENERAL. AT planning is the mechanism for developing specific guidance and execution-oriented instructions for subordinates. An AT plan contains command-specific guidance for the establishment of an AT program and the implementation of the AT standards outlined in the MCO. AT planning is a continuous process carried out in advance of and concurrent with AT operations. The goal of the AT planning process is to develop an actionable written plan that drives the execution of the five AT program elements: risk management, planning, training and exercises, resource application, and program review. This is accomplished through adhering to established standards, coordinating with internal and external organizations, and implementing Force Protection Condition (FPCON) measures. The AT plan provides the AT framework for Commanders, their subordinate units, and, where applicable, tenant commands during routine operations and extraordinary circumstances. As with any planning process in the Marine Corps, AT planning should incorporate the overarching principles of the Marine Corps planning process.

Upon assignment as an ATO, the ATO, together with the AT Working Group (ATWG), will conduct a mission analysis by reviewing the current AT plan. Courses of action are developed through review of requirements, coordination with internal and external actors, and implementation of a baseline FPCON stance. To evaluate the AT plan, exercises are conducted for testing and validation purposes. As a result of these exercises, additional courses of action can be developed by reviewing the requirements, coordinating with internal and external organizations, and implementing FPCON measures. Finally, once the AT plan and order are developed, they should be dispersed to subordinate units and tenant units for coordination and execution. This chapter describes the components of AT planning and plan development.

2001. AT PLAN REQUIREMENTS. The AT plan should be tailored to the level of command or activity for which it is developed, but, at a minimum, it must follow the AT standards identified in MCO 3302.1E. Additionally, the AT plan must account for all personnel under the command's area of responsibility. It should specify assessment requirements and implementation measures needed to protect the command's mission, its personnel, and its assets during daily operations and in extraordinary

circumstances. The endstate of an AT plan is an operations order that should subsequently be exercised as part of the AT program. The AT plan should be evaluated continuously and updated yearly. Figure 2-1 outlines all of the components an AT plan must contain to be in compliance with Higher Headquarters (HHQ) and Joint Staff Integrated Vulnerability Assessment benchmarks.

- The minimum essential AT program elements and standards prescribed by Department of Defense Instruction (DoDI) 2000.16.
- Specific threat risk mitigation measures to establish a local baseline defensive posture, which will facilitate systematic movement to and from elevated security postures, including the application of Random Antiterrorism Measures (RAMs).
- Physical security measures.
- AT measures for DoD:
  - Off-installation facilities, housing, activities
  - High-risk personnel
  - Construction and building considerations
  - Logistics and other contracting
  - Critical asset security
  - In-transit movements
- Incident response measures.
- Consequence management measures, including CBRNE and weapons of mass destruction mitigation planning.
- FPCON implementation measures, including site-specific AT measures.
- CBRNE defense joint enabling concepts of sense, shape, shield, and sustain.

Figure 2-1. AT Plan Minimum Requirements

This chapter outlines the basic AT planning process; the subsequent chapters explain in detail how to achieve each of the AT plan requirements in Figure 2-1. A Sample Installation AT Plan (Appendix A), Expeditionary AT Plan (Appendix B), and Reserve AT Plan (Appendix C) are all included in the appendix section of this document.

2002. AT PLAN DEVELOPMENT. Although the Commander is ultimately responsible for the AT program, the ATO conducts the daily operations necessary to develop an AT plan. AT plan development should be a comprehensive and continual process that incorporates each of the AT program elements outlined in this AT Manual. The development of an AT plan is a cyclic rather than a sequential process. Thus each step may yield new information that affects the information generated earlier. AT plan development must incorporate specific area of responsibility considerations.

In addition to this AT Manual, the Antiterrorism Enterprise Portal (ATEP) on Army Knowledge Online (AKO) is a resource-rich web site to aid ATOs in developing an AT plan. It provides additional information on planning, doctrine and policy, lessons learned, and community-based forums to share information and best practices. New ATOs must sign up for an AKO account and should use the resources available on ATEP in AKO to augment this AT Manual. The AKO web site is <https://www.us.army.mil/suite/login/welcome.html>

1. Writing the AT Plan. An ATO responsible for writing the plan must select a format that best suits the organization and allows for rapid and decisive execution. Although there is no mandated format, it is recommended that organizations use the standard five-paragraph order format with associated annexes. Sample AT plans can be found in Appendices A through C. Each level of an organization will produce a supporting AT plan consistent with its mission and responsibilities. For example, at the installation level, the AT plan will have a tactical perspective and provide minute details for actions to be taken locally. A Service Component Commander's plan, on the other hand, will be at the operational level and will provide descriptive guidance rather than prescriptive solutions.

a. Integrating the AT Manual and AT Plan. Every AT plan (installation or expeditionary) begins with a description of the situation, mission, execution, administration and logistics, and command and signal. The five-paragraph order is often accompanied by substantive annexes detailing specific AT considerations. Although portions of each chapter in this AT Manual may be present in several different areas of an AT plan, some chapters emphasize a specific section in the AT plan. This section describes where the content from the chapters in this AT Manual are placed in an AT plan.

(1) Chapter 2, "Antiterrorism Plan Development," provides guidance with the overall development of an AT plan and program. It provides guidance for developing Annex A (Task Organization), which describes key AT organization composition, including working groups and other collaborative AT initiatives. This chapter also provides guidance for developing the portions of Annex C (Operations) dealing with mission-essential or vulnerable areas, FPCONS, RAMs, risk assessments, and natural and manmade hazards.

(2) Chapter 3, "Antiterrorism Risk Management Fundamentals," provides guidance for conducting criticality, threat, and vulnerability assessments, which will help to determine the overall risk at a specific location. These assessments will assist the ATO with the development of Annex B (Intelligence) and portions of Annex C (Operations).

(3) Chapter 4, "Information Fusion," provides guidance on the collaboration of information sources and the Marine Corps AT program. Information gathered from these sources will assist with the development of Annex B (Intelligence).

(4) Chapter 5, "Incident/Event Response and Management Capabilities," provides guidance for developing the portions of Annex C dealing with incident planning and response, emergency operations center (EOC) operations, continuity of operations plans, and the integration of military and civilian response capabilities. Chapter 5 also provides guidance for developing the EOC communication architecture portion of Annex K (Communications). If the installation has an all-hazards emergency operations plan (EOP), it would meet most of the requirements for the appendices identified above. Additionally, the EOP would also lay out the structure of the EOC, as well as the training requirements of personnel who will be responsible for operating the EOC. Consideration should be given to working closely with the Installation Emergency Manager for coordination of all Emergency Support Functions.

(5) Chapter 6, "Reporting," provides guidance for developing Annex P (Reports), which outlines report format and submission procedures.

(6) Chapter 7, "Antiterrorism Training," assists with the development of Annex N (AT Program Review, Training, and Exercises).

(7) Chapter 8, "Exercises," provides guidance to assist with the development of Annex N (AT Program Review, Training, and Exercises).

(8) Chapter 9, "Resource Application and Funding," assists the ATO with developing Annex E (Fiscal), which provides specific fiscal instruction on how to support AT operations from pre-incident through post-incident.

(9) Chapter 10, "Program Review," provides guidance for developing the AT Program Review portion of Annex N (AT Program Review, Training, and Exercises).

(10) Chapter 11, "Physical Security," assists with the development of the portion of Annex C (Operations) that addresses physical security.

(11) Chapter 12, "Antiterrorism-Related Considerations," assists with the development of several portions of the AT plan, including the sections of Annex C (Operations), that address law enforcement and high-risk personnel. Chapter 12 also provides guidance for developing Annex I (Public Affairs), which includes specific Public Affairs Office instructions on how to support AT operations.

2. AT Plan Coordination. AT plans must be coordinated with subordinate and tenant commands, off-base authorities, and other stakeholders. An ATO should evaluate the organic response capabilities at their location to help to determine the stakeholders needed for coordination. Organic capabilities may include hazardous materials (HazMat), security, explosive ordnance disposal, firefighting, health and medical services/mass casualty care, logistical support, public works, intelligence, previous AT plans and programs, installation perimeter access, security systems technology, executive protection, Information Assurance (IA) Office, response and recovery, and mail handling. The ATO should coordinate the use and availability of these capabilities throughout the development and execution of an AT plan. Working groups provide a beneficial means of involving these diverse capabilities in the AT planning process. Table 2-1 provides recommendations in determining coordinating elements.

Table 2-1. AT Plan Coordination

AT Requirement	Coordinating Elements
AT Program Elements	Commander, ATWG, TWG, ATEC, CIP, CBRNE, PS
Specific Threat Risk Mitigation Measures	Commander, Tenant Commands, NCIS/LE, Intel, CIP
Off-Installation/FOB Components	Local Law Enforcement, Local Fire Department, Utility Organizations, CIP, and Other Community Entities, Host Nation, Other US Services, and/or Allies
High-Risk Personnel	Commander, HRP Family Members
Construction and Building Considerations	Physical Security, Facility Engineering, Information Management, G6, Host-Nation, CIP
Logistics and Other Contracting	Comptroller, Contracting Officer, SJA, GSA
Critical Asset Security	CIP, Security Management, Communications Officer, DISA, GSA, PMO, IA Office, Physical Security
In-Transit Movements	Service Movement Provider, COCOMs, LE, Comptroller
Incident Response Measures	Commander, Emergency Management, Local Community, Tenant Commands, Fire, Safety, PMO, Medical, Public Works, PAO, or Host Nation Response Capabilities
Consequence Management Measures	Commander, CBRNE, CIP, Engineering, Logistics, Host-Nation, Local Community, PAO, PMO
FPCON Measures	Commander, ATWG, TWG, Operations, Law Enforcement, Tenant Commands, Physical Security
CBRNE Defense	CBRNE, PMO, Fire, Safety, Medical, Tenant Commands, LE, Host-Nation, EOD

2003. WORKING GROUPS. A working group is the interdisciplinary coordination of subject-matter experts designed to assist the ATO with the development of the AT program. The goal of an AT working group is to provide the ATO with the body of knowledge and support needed to create a comprehensive AT program that includes all possible hazards. The ATO is responsible for coordinating and/or participating in various Mission Assurance working groups. Depending on the participants involved, working groups may be internal or external. Meeting minutes for each working group should be developed and maintained in accordance with MCO 3302.1E.

1. Internal. Internal working groups primarily comprise DoD-specific personnel providing a wide range of expertise. Membership may overlap for several of the working groups described below, and many Marine Corps installations possess minimal staff elements. If practical, a single Working Group may be formed that incorporates the functional areas as defined by AT, Physical Security, CIP, CBRNE, and Threat Working Groups. If Working Groups are combined, separate charters and meeting minutes must be delineated for each.

a. AT Working Group. The Commander will establish an Antiterrorism Working Group (ATWG) that meets quarterly. Depending on the level of threat activity the ATWG may meet more frequently. AT plan development typically begins with the ATO collaborating with an ATWG. The ATWG oversees the implementation of the AT program, develops and refines AT plans, and addresses emergent or emergency AT program issues. ATWG membership will include the ATO, the Commander (or a designated representative), key members of the principal staff, subordinate and tenant unit representatives, and other representatives as required to support the AT planning and program implementation. The ATWG must have a charter approved by the Antiterrorism Executive Committee (ATEC) and a plan of action and milestones or similar document that provides direction and measurable end-states. Installations, operating forces, and HHQ should all have an ATWG that is involved in all phases of the AT planning process.

b. Threat Working Group (TWG). The Commander of an installation, operating force, or HHQ will establish a TWG that meets at least quarterly or more frequently, depending on the level of threat activity. The TWG develops and refines terrorism and natural hazards threat assessments and coordinates and disseminates threat warnings, reports, and summaries. TWG

membership will include the ATO; the Commander (or a designated representative); key members of the principal staff; tenant unit representatives; and appropriate representation from direct-hire; contractor; federal, state, local, and host-nation law enforcement agencies; and the intelligence community.

c. AT Executive Committee (ATEC). The Commander of an installation, operating force, or HHQ shall establish an AT executive-level committee or similarly structured corporate body that meets at least semi-annually. The ATEC develops and refines AT program guidance, policy, and standards; acts on recommendations of the ATWG and TWG; and determines resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. An ATEC must receive a charter from the Commander.

d. Critical Infrastructure Program Working Group (CIPWG). The CIPWG provides CIP support and solutions, enabling the ATO to address CIP in the development of the AT Plan.

e. CBRNE Emergency Response Working Group (ERWG). The CBRNE ERWG is responsible for planning, assessing, training, and exercising the installation's emergency response CBRNE program. Membership will include the CBRNE protection officer, ATO, CIP Officer, HazMat representatives, senior emergency responder representatives, installation commander (or designated representative), representatives of the principal staff, tenant unit representatives, and other representatives as required to support CBRNE planning and program implementation. Membership will support CBRNE planning and program implementation. Membership may also include appropriate federal, state, and local emergency responder/emergency management personnel, as necessary.

f. Physical Security Working Group (PSWG). The PSWG develops recommended measures to mitigate installation vulnerabilities and presents these measures to the ATEC for consideration. PSWG membership will include the ATO, CIP Officer, CBRNE preparedness officer, and representatives from installation Physical Security to include PMO, Installations and Environment (I&E)/Facilities, and the Comptroller's office. The I&E/Facilities representative will be responsible for construction projects, installation/maintenance of security-related equipment, and recommending design modifications within the scope of the project to ease future maintenance. The Comptroller will identify possible funding sources and manage funding.

2. External. External working groups are the principal forums for Mission Assurance-related issues. The composition of these groups can include but is not limited to Security Cooperation Forums, host nation security, and other federal, state, and local entities as defined by the commander.

An example of an external working group is the Joint Terrorism Task Force (JTTF). JTTFs are a partnership among the Federal Bureau of Investigation, other federal agencies, state and local law enforcement, and other specialized agencies that investigate terrorism. JTTFs are formed to help maximize interagency cooperation and coordination by creating cohesive units capable of synchronizing terrorism information and investigations in the United States.

2004. TYPES OF AGREEMENTS. During AT planning, an ATO should explore different types of formal agreements with off-installation authorities and others for the purpose of sharing resources and capabilities. ATOs should consult with other base entities (e.g., Fire, Provost Marshal's Office, Hospital) to determine the types of agreements that currently exist and possible gaps in response capabilities. Once gaps are identified, several types of agreements may be pursued. It is vital to integrate the advice of the Staff Judge Advocate (SJA) when drafting and entering into any of these agreements to avoid unauthorized commitments of appropriated funds and violations of federal statutes. All agreements should be validated through an exercise, reviewed annually, and modified as needed. A recommended best practice is for ATO's to keep copies of all relevant agreements with other important AT documents.

1. Interservice or Intraservice Support Agreement (ISSA). Intra-DoD agreements are generally termed ISSAs. Interservice support is provided by one DoD activity to a DoD activity of another Military Service, Defense Agency, Unified Combatant Command, Army Reserve, Naval Reserve, Air Force Reserve, Marine Corps Reserve, Air National Guard, or Field Activity. ISSAs provide recurring support to another DoD or non-DoD federal activity. Support agreements are recorded on a DD Form 1144, *Support Agreement* form, in accordance with DoDI 4000.19. DD Form 1144 is designated for recurring interservice support that requires reimbursement. They define the support to be provided by one supplier to one or more receivers, specify the basis for calculating reimbursement charges (if any) for each service, establish the billing and reimbursement process, and specify other terms and conditions of the agreement. Broad areas of

recurring interservice support and cooperation that do not require reimbursement should be documented with a memorandum of understanding (MOU) or a memorandum of agreement (MOA).

2. Memorandum of Understanding (MOU). A MOU is typically used when different agencies are acting cooperatively and in parallel to accomplish a joint result. A MOU sets forth the basic principles and guidelines under which the parties will work together to accomplish established goals. Memoranda that define general areas of understanding between two or more parties - explains what each party plans to do; however, what each party does is not dependent on what the other party does (e.g., does not require reimbursement or other support from receiver).

3. Memorandum of Agreement (MOA). A MOA is used when one agency specifically supports the activities of another. A MOA defines general areas of conditional agreement between two or more parties - what one party does depends on what the other party does (e.g., one party agrees to provide support if the other party provides the materials). MOAs that establish responsibilities for providing recurring reimbursable support should be supplemented with DD Form 1144. Appendix D provides a Sample MOA.

4. Mutual-Aid Agreement (MAA). MAAs are generally reciprocal agreements in which two or more jurisdictions promise to provide each other assistance in the event of an emergency. An MAA is a written agreement between agencies and/or jurisdictions in which they agree to assist one another on request by furnishing personnel and/or equipment.

5. Cooperative Assistance Agreement (CAA). A CAA is an agreement that involves a commitment for a response when certain agreed-upon conditions exist. It generally involves a government unit that is contracting with a private organization such as a hospital, ambulance service, bus company, or American Red Cross unit to provide specific resources in the event of an emergency. Cost reimbursement may or may not be included.

6. Host Nation Support Agreements. Host Nation Support Agreements are basic agreements normally concluded at government-to-government or government-to-combatant commander level. Host Nation Support Agreements may include Status of Forces Agreements, Visiting Force Agreements, umbrella agreements, and MOUs between the host nation and U.S. Forces.

a. Status of Forces Agreements (SOFA). SOFAs determine the legal status of U.S. armed forces stationed in a foreign nation. They play a vital role in preserving command authority, guaranteeing fair treatment of individual service members, and conserving scarce resources. SOFAs typically address issues that include entry into and exit from the country, tax liabilities, postal services, employment terms for host-country nationals, and civil and criminal jurisdiction. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement (Visiting Force Agreements), or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials.

b. Visiting Force Agreement (VFA). A VFA is similar to Status of Forces Agreements (SOFAs), but typically covers forces visiting temporarily. A SOFA covers forces based in the host nation as well as visiting forces.

2005. FORCE PROTECTION CONDITIONS (FPCONS). Once an AT plan is developed and an AT program becomes operational, FPCONS drive the implementation of AT measures for commands and tenant commands. A complete explanation of the DoD FPCON System can be found in DoD O-2000.12-H, "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence." A well-constructed AT plan will delegate tenant command tasks for each FPCON level and associated measures. The DoD FPCON System is a progressive level of protective measures that can be implemented by all DoD components in response to manmade and natural threats. FPCONS are designed to assist Commanders in reducing the effect of terrorism and other security threats to DoD units and activities by increasing the force protection posture. Operational costs should be a significant factor when selecting and maintaining FPCONS because the implementation of all FPCONS may have adverse effects on daily operations. Elevated FPCON levels for an extended duration can be counterproductive to security effectiveness and overall mission accomplishment. To prevent elevated FPCON levels from being counterproductive, every Commander should establish a review mechanism to lower the FPCON level as soon as the threat environment permits. Evaluate the impact of raising the FPCON prior to implementation for better decision making.

1. FPCON Procedures. Commanders at all levels will set a local FPCON with the help of the ATWG and the TWG. Commanders should also develop a process to raise or lower FPCONs as necessary. The AT plan should promulgate the current FPCON and the conditions needed to change FPCON levels. FPCON transition procedures and measures will be disseminated and implemented by subordinate commanders. Local commanders must then develop measures to support the transition between FPCONs. The AT plan will include a written explanation of the process to raise or lower FPCON levels.

a. Subordinate commanders can establish higher FPCONs as the local situation warrants, but a Commander cannot lower a higher-level commander's FPCON without written concurrence. The declaration, reduction, and cancellation of FPCONs remain the responsibility of the Commander issuing the order.

b. FPCON measures, alert notifications for augmentation forces, and standard operating procedures for responding to developing situations are crucial FPCON procedures that enhance the effectiveness of managing an incident.

2. FPCON Waivers. An FPCON waiver may be requested if it is determined that certain FPCON measures are inappropriate for current operations or for proper threat mitigation. Overseas, the waiver procedure directed by the geographic Combatant Commander applies. In the domestic United States, the first general officer exercising operational control in the chain of command has the authority to waive FPCON measures. The waiver process is not intended to diminish the authority or responsibility of commanders to exercise oversight of FPCON and RAM program execution.

3. Baseline FPCON Levels. The DoD FPCON System comprises five progressive levels of enhanced AT protective measures: NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA.

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

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

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

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

e. FPCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

4. Site-Specific FPCON Measures. Commanders at all levels will develop site-specific FPCON measures that supplement the measures/actions contained in the FPCONs and DoD Handbook 2000.12-H. The development of site-specific FPCON measures should permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement (CJCSI 3121.01A) and Rules for the Use of Deadly Force (DoDD 5210.56). In addition, outside sources of information such as critical infrastructure protection, intelligence, counterintelligence, law enforcement resources, and institutional knowledge of the area should be considered when developing site-specific FPCON measures. Site-specific AT measures and physical security actions linked to an FPCON shall be properly marked "FOR OFFICIAL USE ONLY." Strict distribution policies of the AT measure and physical security actions should be maintained, which include storing in a controlled and lockable room and not posting on public websites.

5. FPCON Action Set. When an FPCON level is established, it should be accompanied by an FPCON action set for each measure. An FPCON action set includes the FPCON, the selected measure under that FPCON, an action set describing the duties and responsibilities of those involved with that measure, and the coordination necessary to execute the action. FPCON action sets clearly define the actions and coordination necessary to execute an effective FPCON measure. Each action should be assigned to a specific unit, and that unit should be fully cognizant of their

FP responsibilities. Appendix E provides Sample FPCON Action Sets.

6. FPCON Change Reports. All Marine Corps supporting commands and their subordinate installation and facility commanders should submit FPCON change reports to HHQ and CC their Geographic Combatant Command Service Component and HQMC when FPCON changes are implemented. Tenant commands of DoD installations/facilities do not have to submit FPCON change reports because their host installation/facility will. However, tenant commands of non-DoD installations/facilities should submit reports to HHQ. FPCON change reports should be sent to HHQ within 2 hours of implementing the change. FPCON change reports should state the new FPCON level, the date-time group effective, why the FPCON change occurred, who directed the change, and any additional details. Appendix F provides a Sample FPCON Change Report.

7. Random Antiterrorism Measures (RAM). The purpose of RAMs is to identify a set of protective measures in addition to those in effect through the current FPCON, and implement those measures in such a way as to prevent patterns of security to be observed by hostile forces. The measures can be obtained from higher FPCONs or developed specifically for a particular RAM program. RAM programs change the security atmosphere surrounding a facility. Such programs, when implemented in a random fashion, alter the external appearance or security "signature" of an installation. Proper execution of a RAM program helps to ensure a robust security posture from which terrorists cannot easily discern patterns or routines that could be easily exploitable during pre-attack planning. An effective RAM program instills uncertainty in terrorist planning by enabling security to appear not only formidable, but also unpredictable and ambiguous. Installation ATOs are responsible for the RAM program in partnership with the Installation PMO. ATOs should coordinate with security forces regarding RAM measures that require security personnel. All assigned and tenant units, agencies, and activities will participate by developing and implementing their own RAMs. Appendix G provides a Sample RAM Program.

8. Mutual-Aid Response Procedures. To ensure Installation Commanders can maintain their ability to support and be supported by outside agencies and first responders, they must identify and establish access/egress procedures for mutual-aid responders. This will ensure that there is no mission degradation while responding to incidents safely and

efficiently. These procedures should be identified within applicable MAAs/MOUs/MOAs/ISSAs with designated state, local, other service, and/or private (or host-nation) responders.

2006. SUPPLEMENTARY AT PLANNING. In addition to installations, separate or leased facilities, operational deployments, large-scale training events, and special events all require the development of a separate, event specific, risk assessment plan. A Sample Plan is provided in Appendix H.

1. Off-Installation Facilities, Housing, and Activities. An AT plan must include specific AT measures for off-installation facilities, housing, transportation services, daycare centers, and other activities used by or involving a mass gathering of DoD personnel and their dependent family members. These risk mitigation measures will include emergency notification and recall procedures; guidance for selection of off-installation housing, temporary billeting, and other facility use (including compliance with Unified Facilities Criteria 04-010-01, DoD Minimum AT Standards for Buildings, for leased, newly constructed, and expeditionary buildings); physical security measures; CBRNE defensive measures; and shelter-in-place, relocation, and evacuation procedures.

At locations where there are multiple DoD components, such as DoD-leased facilities or other facilities where DoD occupies space, the designated senior DoD component will be responsible for integrating and coordinating individual DoD component security plans into a comprehensive installation, facility, or area-wide AT program. MOAs or other similarly structured protocols with the appropriate federal, state, local, and host-nation authorities to coordinate security measures and assistance requirements should also be established to ensure the protection of DoD personnel and their family members at off-installation facilities and activities.

2. Operational Deployments. AT planning and assessments for operational deployments should be conducted in a manner similar to that of installation procedures. However, because of the nature of deployment planning, a few extra components must be added to the planning process. These include developing operational security procedures (OPSEC), acquiring necessary materials, obtaining tailored and focused intelligence, organizing necessary security support augmentation, and conducting required host-nation coordination.

3. Large-Scale Training Events. Every training event at the battalion/squadron level or higher requires a separate AT plan that addresses specific AT issues that may arise during the training event. The large-scale training event plan should follow the same format as the installation AT plan and should be updated for each training event.

4. Special Events. A special event is an activity, often unique or symbolic, characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved. Special events AT Plan requirements may be met by writing a separate annex. AT annexes may accompany a special event operations order or Letter Of Instruction (LOI). A vulnerability assessment is required for any special event or other activity involving a gathering of 300 or more DoD personnel.

a. Supporting Marine Corps commands should generate a report to HHQ on all special events or activities that will gain national attention or significant media coverage, increase vulnerability, or present a large gathering type-target with the potential for mass casualties. The report must list the name/description of event, location, date, and any specifics as to why each event may gain national attention.

5. Individual AT Plans for Travel. Personnel traveling officially or unofficially OCONUS will submit an Individual AT Plan to their chain of command through their ATO. Individuals traveling should compile their own plan with assistance from their ATO. Appendix I provides an Individual AT Plan Checklist detailing all the information an individual AT plan should include: the traveler's data, a summary of the threat, transportation plans, medical care, communication capabilities, U.S. consulate location, and an emergency action plan. AT travel plans should be approved in accordance with appropriate Geographic Combatant Command (GCC) policy. Appendix J provides a Sample Individual AT Plan. The individual should fully understand and comply with the plan throughout his/her travel.

2007. DESIGN BASIS THREAT (DBT). AT planning must include design basis threat analysis so an ATO understands the baseline type and size of threat that buildings or other assets are designed to withstand. The DBT is the threat against which an asset must be protected and on which the protective system's design is based. It provides a basis for confidence that the protection system developed is appropriate and effective against a certain threat. The DBT provides both a basis for system design and a

consistent criterion for assessing the adequacy of a pre-existing physical protection system. A DBT should include the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics. Many natural hazards are addressed by local building codes. Appendix K provides a Generic DBT Matrix; Appendix L provides a Sample DBT.

CHAPTER 3

RISK MANAGEMENT FUNDAMENTALS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	3000	3-1
RISK MANAGEMENT PROCESS OVERVIEW.....	3001	3-3
MISSION ANALYSIS.....	3002	3-3
RISK ANALYSIS.....	3003	3-13
RISK MANAGEMENT PROCESS REVIEW.....	3004	3-19

## CHAPTER 3

### MISSION ASSURANCE RISK MANAGEMENT METHODOLOGY

3000. General. Mission assurance is defined as a *process* linking and integrating various protection-related programs and activities using a risk management-based framework to ensure missions and core functions or capabilities are attained. The goal of Mission Assurance is to integrate numerous risk management programs and other activities and security related functions - such as force protection; continuity of operations; critical infrastructure protection; physical security; information assurance; law enforcement; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; operational security; and installation emergency management to create synergies in implementing a standardized process for managing risk to Marine Forces in the execution of their assigned missions and core functions. Considering the interdependencies of these programs and activities, this chapter promulgates policy and procedures for a uniform risk management process to be conducted across the Marine Corps.

a. Goal. To develop, integrate, and promulgate a uniform process for identifying and managing risk to assets that support the execution of Marine Corps missions and core functions/capabilities across all mission assurance programs and activities. The ultimate goal of the process is accomplishing the mission through the management of risk of loss to mission assets in a wide variety of operating environments worldwide.

b. Definitions.

- 1) **Risk Management**: A process by which decision makers identify and assess risks and subsequently undertake actions to reduce or mitigate risk, or where circumstances warrant acknowledging risk, which is weighed against the benefits provided to assuring mission execution. Risk Management consists of two core activities: Risk Assessment and Risk Response.
- 2) **Risk**: The potential for loss or an unwanted outcome resulting from an imposition of a certain level of threats or hazards as determined by their likelihood and severity of loss or impact on the missions and associated assets and vulnerabilities.

- 3) **Risk Assessment:** A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks.
- 4) **Risk Response:** Actions taken to remediate or mitigate risk, to reconstitute capability in the event of loss or degradation, or to acknowledge risk where warranted."

c. Assessing Risk. Risk assessment involves the collection and evaluation of data in three core areas: 1) Criticality, which is defined as the total impact (failure or severe degradation) on execution of all missions or functions supported by an asset; 2) Identifying all threats and hazards and the likelihood or probability of their occurrence; and 3) identifying vulnerabilities of assets that could be exploited by an identified threat or hazard. Assessing risk is the key foundation for executing an effective risk management program.

d. Managing Risk. The objective is to manage risk to missions and assets, rather than managing to vulnerabilities alone. The goal is to achieve an acceptable level of risk in the execution of missions and functions. The principal methods of managing risk include the following risk response activities:

- (1) Detect, Delay, Deter, Deny the threat or hazard.
- (2) Implementing effective and efficient risk remediation and mitigation countermeasures such as, physical security measures, personal protection measures, cyber security measures, or building redundancy for mission assets.
- (3) Transferring the risk. As examples, risk may be transferred by assigning the mission to another command, or when risk management resources required to reduce risk to an acceptable level are requested of higher headquarters. Although there is no consensus on the definition of transferring risk, at a minimum, risk is shared by the chain of command when a risk-related unfunded resource requirement is submitted via the Planning Programming Budgeting Execution System PPBES.

(4) Acknowledging risk. Commanders may decide to acknowledge a particular risk when the impact of loss or the anticipated reduction in risk is not significant enough to justify the cost or benefit of the proposed risk reduction countermeasure.

3001. Risk Management Process Overview. Risk management is a continuous process and is a task inherent in the goal to achieve mission assurance. The risk management processes identified herein is to be executed by the Marine Corps Mission Assurance - Enterprise (MCMA-E):

a. Marine Corps Installations. The risk management processes and framework identified herein are a fundamental responsibility of the commander and must be continuously executed and applied across the full spectrum of military operations, functions, and capabilities. Marine Corps tenant commanders are responsible for executing risk management processes for their command, and are required to coordinate with, and support the host installation risk management program and activities. Under the Joint Basing concept, other Service/Agency tenants will also coordinate and collaborate with the host installation for execution of the risk management process.

b. Operating Forces. Commanders will execute risk management as part of its mission assurance and force protection requirements. Risk management principles will be integrated into mission planning, preparation, and execution in all Areas of Operation (AOA). Per paragraph 2a, when Operating Force commands are tenants aboard USMC installations, other Service installations or Joint bases, Operating Force commanders will coordinate and support their host installation's risk management program and activities, as required.

3002. Mission Analysis. Risk Assessment Concepts, Components and Tools.

a. Risk Assessment Process - Criticality Assessment Component. The first component of conducting a risk assessment is to conduct a criticality assessment, which is an assessment of command's missions and functions/capabilities, and mission impact or consequence of loss of assets that support execution of command's missions. All command mission assurance program elements (POCs/Program Managers) are required to perform annual risk assessments and will use the following process and

tools to identify missions and functions, associated assets and their criticality and impact score:

(1) Mission-Focused Criticality Assessment. Utilizing command approved Mission Essential Tasks (METs) with their associated conditions and standards and/or core functions, MA personnel will identify assets associated with the execution of the METs. Assets can be people, physical entities, systems or information that provides a service or capability. The analysis will examine those assets whose degradation or destruction impacts the command's ability to complete its assigned mission(s) or functions. DODI 3020.45, Vol 1, describes in detail this Critical Asset Identification Process (CAIP), which is the process that must be used to conduct the criticality assessment process (see also, Joint Pub 3-07.2 - Antiterrorism). There are other assets that may not be critical to the execution of the mission or function that may be identified in this criticality process and included in the overall risk assessment process. These non-critical assets could include assets such as high population facilities, such as theaters, commissaries, base exchanges, etc.

(2) Criticality Score. All identified assets will have their criticality score determined by use of the USMC Asset Priority Methodology (USMC-APM) and tool. Mission and asset data can be entered into a stand-alone USMC-APM tool, or in MC-CAMS Next Generation to obtain a standardized priority or criticality value based on all missions supported by the asset. Note: This asset priority value is also the impact value or score that is utilized in the USMC Risk Assessment (USMC-RA) methodology and tool to support the determination of risk of loss to the critical asset.

b. Risk Assessment Process - All Hazard Threat Assessment Component. Execution of mission assurance goals and risk management processes must be based on an assessment of the threat and hazard environment in which our forces operate and missions are executed. The development of an all hazard threat assessment must accomplish two goals: the identification of a comprehensive list of threats and hazards and the likelihood or probability of occurrence of each threat or hazard. In the context of assessing risk, the higher the probability or likelihood of a threat or hazard occurring, the higher the risk of loss will be to the asset, all things being equal. All command Mission Assurance program elements will perform an all hazard threat assessment annually. Furthermore, all command

Mission Assurance Programs will develop an integrated Threat and Hazard Matrix that reflects the likelihood of assessed threats and hazards. See Figure (1) Threat and Hazard Matrix template.

(1) Threat and Hazard Definitions

a. Threat. Generally refers to intentional conduct by an adversary having the intent, capability, and opportunity to cause loss or damage to assets or personnel.

b. Hazard. Generally refers to unintentional incidents such as accidents, events of nature such as destructive weather, and equipment failure that cause loss or damage to assets or personnel.

(2) Hazard and Threat Baseline Analysis. Analysis must be executed that will identify a baseline of threats and hazards that could adversely impact command assets. See Figure 3-2 Threat and Hazard Matrix template. Note that when discussing execution of vulnerability assessments below, the assessor must align one or more identified threats/hazards to one or more discrete vulnerabilities of assets or the installation that could be exploited by the threat or hazard. The annual threat assessment must be tailored to the local environment and should include all likely or feasible WMD, including CBRNE threats. The ATO / threat working group / fusion cell must fuse all sources of information (strategic, operational, and tactical (local) for use in the annual threat assessment. The annual threat assessment must be integrated into all aspects of the risk management process. Additionally, Toxic Industrial Chemicals (TICs)/Toxic Industrial Materials (TIMs) and locations of activities that produce biohazards (i.e. hospitals and medical research facilities) should be included in the Hazard Assessment.

Threat and Hazard Probability Ratings and Definitions. Once a baseline of threats and hazards has been identified, the assessor must analyze those threats and hazards to determine the likelihood or probability of occurrence of each threat and hazard. Four categories of Threat and Hazard Probability

(1) Ratings and Definitions (Critical, High, Medium, Low) are detailed below and contained in the USMC-RA stand-alone tool and are also embedded in MC-CAMS Next Generation. The use of these ratings and definitions will facilitate the uniform assessment of the likelihood or probability of any individual threat or hazard occurring, which is an essential component of the risk assessment process. Probability is the estimate of the likelihood that a threat shall cause an impact on the mission or a hazard to the installation. See chart below which annotates the NCIS probability ratings, which are cross referenced to those in MC-CAMS.

a. Low - Indicates little or no credible evidence of a threat.

i. For man-made threats, it is based on little or no credible evidence of capability or intent with no history of actual or planned targeting.

ii. For naturally occurring hazards and accidental disruptions, it is based on little or no credible evidence of capability to cause damage, which may affect mission execution and there is no history of occurrence.

b. Medium - Indicates a potential threat.

i. For man-made threat, it is based on the threat's desire to compromise the mission or the facility and the possibility that the threat could obtain the capability through alternate sources where the capability has been demonstrated in related incidents. Also indicates there is a significant capability with low or no current intent, which may change under specified conditions, and low or no demonstrated history.

ii. For naturally occurring hazards/threats and accidental disruptions, it is based on a significant capability to cause damage to a CA with a low or no probability of occurrence which may change under specified conditions and there is low or no history of occurrence.

a. High - Indicates a credible threat. On our knowledge of the capability and/or intent of the hazard/threat

to cause service interruption to the systems; this is based on demonstrated incidents that took place against like systems.

i. For man-made threat, this is based on the knowledge of the threat's capability, their intent to cause disruption to the CA based on related incidents that took place at similar assets or locations, and a demonstrated history of occurrence.

ii. For naturally occurring hazards/threats and accidental disruptions, this hazard/threat is based on a significant capability to cause damage to a CA with a significant probability of occurrence, which may change under specified conditions, and there is an occasional history of occurrence.

b. Critical - Indicates an imminent threat.

i. If referring to a man-made threat (criminal, terrorist, insider, etc) the threat has both the capability and intent to cause a disruption and the facility or similar assets are being targeted on a frequent or recurring basis.

ii. If referring to naturally occurring events (flood, tornado, hurricane, earthquake, etc.), disaster or accidental disruption (construction mishap, accident, design flaw, etc.), the hazard/threat has the capability to cause a disruption and a demonstrated history of occurring on a frequent basis.

A depiction of the probability/likelihood rating is shown in Figure 3-1:

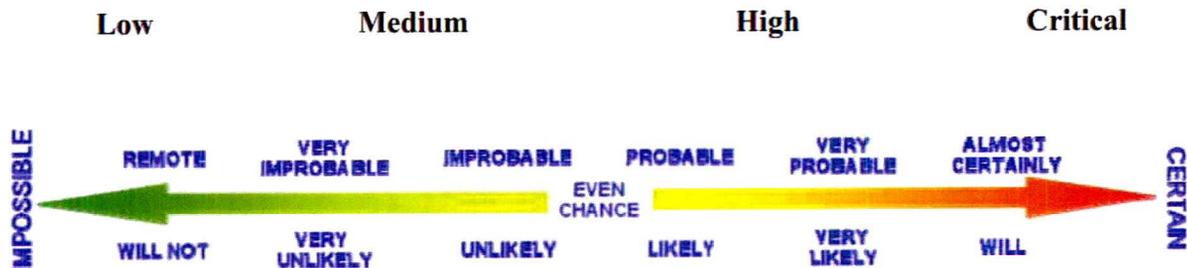


Figure 3-1

(4) Sources of Threat Assessment Data. Each Service maintains its own terrorist threat analysis capability. Although DOD threat levels may only be set by DIA, Service Analysis (OSI, MTAC ...) and or Information Fusion Centers can provide valuable assessments to installation commands and or Operating Forces regarding terrorist threats for specific, localized areas. The following are primary sources of threat assessment data that contributes to indications and warning for US military forces:

(a) Marine Forces (MARFOR) Intelligence Department (G2) or Information Fusion Center (IFC). The G2 and/or IFC is the focal point for all intelligence support for FP related intelligence, information, and counterintelligence (CI) issues for US Marine Corps assets within their respective AOR. IFC will oversee correlation of law enforcement (LE) information in order to provide a domestic summary consistent with other DOD Intelligence Oversight Directives.

(b) Naval Criminal Investigative Service (NCIS) Multiple Terrorist Alert Center (MTAC) Threat Products. Products include: time-sensitive Spot or Suspicious Activity Reports, Warning Reports, CI/Terrorism Supplements, Annual Regional Threat Assessments, Port Threat Assessments, and Baseline Study Reports.

(c) U.S. Army Counterintelligence Center (ACIC) Threat Products. Products include: Monthly International Terrorism Summary (MITS), Multi-disciplined CI Threat Assessments, ACIC Information Papers.

(d) U.S. Air Force Office of Special Investigation (AFOSI) Threat Products. Products include: CI Notes, and AFOSI Blue Line - a daily synopsis of global incidents of interest to Air Force personnel.

(e) Defense Intelligence Agency (DIA)/Joint Intelligence Task Force for Combating Terrorism (JITF-CT). DIA/JITF-CT disseminates intelligence on foreign terrorist threats, including specific warning of threats against DOD personnel, facilities, and other DOD material resources. Additionally, DIA produces a Threat Assessment triennially, or more frequent if required.

(f) Geographic Combatant Command area of responsibility - specific supplement to the DIA-produced global threats report.

(g) Joint Department of Homeland Defense (DHS)/Federal Bureau of Investigation (FBI) Intelligence and Analysis Reports.

(h) DHS Intelligence Reports: DHS Daily Open Source Infrastructure Reports, Homeland Security Digital Library (HSDL) Critical Releases, DHS Homeland Security Advisory System/Threat Levels, DHS Daily Infectious Disease Report, DHS Daily Drug Trafficking and Smuggling Report, DHS Homeland Security Central Digest, DHS Daily Cyber Report.

(5) Sources of Hazard Assessment Data. There are numerous Federal and private agencies performing hazard assessments on a periodic basis that provide indications and warning of natural hazard.

(a) US Army Corps of Engineers (USACE) Commercial Infrastructure Network Disruption Analysis Report. This report identifies potential natural hazards and their probability of occurrence for the various regions of CONUS.

(b) National Oceanic and Atmospheric Administration (NOAA) and the US Geological Survey, Department of Earth and Science. These reports cover the probability of destructive weather and seismic events that could disrupt mission accomplishment.

(c) Department of Energy 5480.7A, Fire Hazards and Probability

(d) Site Specific Mission and Supporting Infrastructure Analysis. These reports provide insight on various hazards such as the site's proximity to chemical and nuclear facilities along with likely commercial infrastructure single points of failure supporting mission execution.

(e) Local Emergency Planning Committees. The committees are made up of county/regional first responder agencies that provide hazard data and reports for planning and action. Much of the data is based on records of historical occurrences of hazards such as destructive weather in a given geographical area.

c. Risk Assessment Process - Vulnerability Assessment Component. A Vulnerability Assessment is a systematic examination of the characteristics of an installation's system, asset, application, or its dependencies to identify

vulnerabilities that could be susceptible to the effects of any number of threats or hazards. Vulnerability assessments must be conducted by team of subject matter experts with backgrounds in different functional areas such as Physical Security, Anti-Terrorism, Infrastructure and Emergency Management and Plans. VAs will be conducted as follows:

(1) Identify and assess all vulnerabilities to the installation or facilities within, to specifically include all identified critical assets. Vulnerabilities are defined as a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard effects. Vulnerabilities to a critical asset can result from a wide variety of factors such as: design and construction flaws, environmental factors, proximity to other structures or systems, factors influencing accessibility, personal behaviors of people working in or around the critical assets, or operational practices associated with the critical assets or the installation. Vulnerabilities of a critical asset can also be determined by vulnerabilities to other assets or areas that are not in close proximity to the critical asset. For instance, vulnerabilities in access or perimeter control of an installation may lead to an adversary gaining access to the installation, and ultimately to the critical asset located somewhere inside the installation.

(2) Identify degrees of vulnerability. When assessing and identifying vulnerabilities the assessor needs to make a judgment as to the significance or degree of an identified vulnerability. For example, lack of standoff around a high population building may be identified as a vulnerability, based on Unified Facility Criteria (UFC) requiring 80 feet of standoff. The actual standoff is 79 feet. The significance or degree of vulnerability would be relatively low, as would the impact of exploiting that vulnerability from a threat such as a 220 lb Vehicle Borne Improvised Explosive Device (VBIED) that the UFC requirement was designed to address. Identifying degrees of vulnerabilities assists in providing a weight to each vulnerability, which in turn supports providing an overall risk assessment rating. Degrees of vulnerability are defined as follows and their definitions found in the USMC RA tool and MC-CAMS Next Generation:

(a) Critical: Indicates minimal effective physical, design, technical, procedural, or behavioral countermeasures in place and many known weaknesses through which adversaries, natural hazards or accidental disruptions would be capable of causing loss of or disruption to critical assets.

(b) High: Indicates some effective countermeasures in place, but still multiple known weaknesses through which adversaries, natural hazards or accidental disruptions would be capable of causing loss of or disruption to asset.

(c) Medium: Indicates multiple effective countermeasures in place; however, at least one known weakness exists through which adversaries, natural hazards or accidental disruption would be capable of causing loss of or disruption to asset.

(d) Low: Indicates multiple effective layers of integrated countermeasures in place and there are no known weaknesses through which adversaries, natural hazards or accidental disruptions would be capable of causing loss of or disruption to asset.

(3) Align specific threats and hazards to asset vulnerabilities. Threat-asset vulnerability pairing is conducted to link likely threats and hazards to specific asset vulnerabilities that may be susceptible to a specific threat or hazard. This process is crucial because individual assets may have a greater degree of vulnerability to different threats or hazards. Pairing a threat or hazard with an asset vulnerability will allow for greater precision and understanding of which assets are susceptible to certain threats. This in turn will support the preparation of effective remediation or mitigation plans designed to lower overall risk by incorporating and addressing both threat/hazard and vulnerability analysis in those plans.

(4) All assessments team will use the most current Marine Corps Mission Assurance Assessment (MCMAA) standards and benchmarks when performing VAs on the installation, facilities and assets. These standards will be used when conducting the Higher Headquarters Assessments and the annual self assessments.

(a) Higher Headquarters Risk Assessments. All Marine Corps installations will be subject to a MCMAA once every three

years. These assessments will not only examine installations, but they will also review installation tenants and their MA programs in coordination with the host installation. Each assessment will evaluate the command's risk management execution and provide advice, guidance, and advocacy for improvement of the commands MA program.

(b) Annual Self-VAs. Local VAs shall be conducted by all installations and Operating Force units (squadron/battalion and above) at least once per year, or more frequently if the terrorist threat or mission requirements dictate. Local VAs will be conducted for any event or activity determined to be a special event or other activities involving a gathering of 300 or more DoD personnel. Again, all discrete assets will receive this local VA. Since DOD facility policy directives also require a detailed VA be performed each year on utility systems, the VA completed in accordance with DOD facility policy can be used to fulfill the MA annual self-VA requirement if utility systems are identified as supporting infrastructure critical assets (SICAs).

d. Risk Assessment Methodology and Supporting Tools. A risk assessment involves the collection and evaluation of data concerning the criticality of the assets based on mission impacts, likely and probable threats and hazards, degrees of vulnerability, and existing countermeasures to determine the overall risk posture of the asset. Essentially, it is a systematic, rational, and defensible process for identifying, quantifying, and prioritizing risks. Based on the values produced from the criticality, all hazard threat assessment, and vulnerability assessments, a risk assessment rating or score is produced. Risk is determined by the following equation: Criticality Rating x Threat/Hazard Rating x Vulnerability Rating = Risk Rating. A risk rating is produced for each specific threat/hazard-vulnerability-asset pairing of data.

See Figure 3-2 below:

USMC Mission Assurance – Threat / Hazard Matrix Template  
(Notional Data)  
Individual Threat / Hazard Analysis Data Matrix

Installation / Site Name	Threat / Hazard Name	T/H Probability Rating Ranges	Probability Rating Source Information	Assessed T/H Probability Rating (Using CARA Tool)	Other Rating Factors - Comments
Camp Zebra	Explosive – 220 lb. VBIED	Critical .76 to 1.00	NCIS Threat Assessment dated x/xx/xx;		Site specific intelligence factors; other relevant analysis such as a DBT; identify a specific period for duration of the threat or hazard;
		HIGH .51 to .75			
		Medium .26 to .50	DIA Threat Assessment dated x/xx;	HIGH .60	
		Low .01 to .25	Local installation threat assessment dated x/xx;		
			past history of similar events occurring, etc.		

Integrated and Prioritized Threat / Hazard Matrix

Installation / Site Name	Threat / Hazard Name	Assessed T/H Probability Rating (Using CARA Tool)
Camp Zebra	Flooding - Hurricane	Critical .80
	Explosive – 220 lb. VBIED	HIGH .60
	Aged Equipment – No Spares	Medium .47
	EMP	Low .05

