



**UNITED STATES MARINE CORPS**

MARINE CORPS AIR STATION YUMA  
BOX 99100  
YUMA, ARIZONA 85369-9100

StaO 3302.1B

AT  
MAR 27 2007

STATION ORDER 3302.1B

From: Commanding Officer, Marine Corps Air Station, Yuma AZ  
To: Distribution List

Subj: MCAS YUMA ANTITERRORISM (AT) PROGRAM

Ref: (a) StaO 3006.1  
(b) StaO 5510.30  
(c) StaO 5530.14  
(d) DODI 2000.16  
(e) UFC 4-010-01  
(f) UFC 4-010-02  
(g) DODD 2000.12  
(h) MCO 5239.2  
(i) CJCSI 5261.01

Encl: (1) Locator Sheet

1. Purpose. To establish policies and procedures for planning and executing the MCAS Yuma Antiterrorism (AT) program. The AT program seeks to reduce the likelihood that personnel, facilities, and material will be exposed to an attack and to mitigate the effects of such an attack should it occur. Antiterrorism is an all hands responsibility.

2. Cancellation. StaO 3302.1A

3. Background

a. This directive supplements the references. In particular, it compliments reference (a), the MCAS Yuma Emergency Management Program. This directive cannot be applied without understanding the provisions of reference (a). Individuals are encouraged to become familiar with reference (a) prior to reading this order.

b. This order serves as policy except where it contradicts any regulation issued by a higher headquarters in which case the higher headquarters directive shall prevail in determining actions. This directive is applicable to all military,

FOR OFFICIAL USE ONLY

StaO 3302.1B

civilian, and contractor personnel assigned to MCAS Yuma, to include tenant organizations.

4. Action. Commanding Officers, Officers in Charge, and department heads are responsible for the full implementation of this order as it pertains to their organization.



B. D. HANCOCK

Distribution: A



ANTITERRORISM (AT) PROGRAM

RECORD OF CHANGES

Log completed change action as indicated:

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

FOR OFFICIAL USE ONLY

ANTITERRORISM (AT) PROGRAM

CONTENTS

CHAPTER

1	INTRODUCTION
2	GENERAL RESPONSIBILITIES
3	INTELLIGENCE/INFORMATION FUSION
4	ANTITERRORISM OPERATIONS
5	ANTITERRORISM PHYSICAL SECURITY MEASURES
6	ANTITERRORISM CONSTRUCTION STANDARDS
7	SPECIAL EVENTS
8	HIGH RISK PERSONNEL (HRP)
9	COUNTER MANPAD WEAPONS OPERATIONS
10	LOGISTICS
11	TRAINING AND EDUCATION
12	AT EXERCISES
13	PERSONAL AWARENESS CONSIDERATIONS
14	COMMUNICATIONS AND COMPUTER SYSTEMS
15	ANTITERRORISM RESOURCE MANAGEMENT
16	ANTITERRORISM PROGRAM REVIEW

FOR OFFICIAL USE ONLY

ANTITERRORISM (AT) PROGRAM

CHAPTER 1

INTRODUCTION

	<u>PARAGRAPH</u>	<u>PAGE</u>
BASIC POLICY. . . . .	1000	1-2
OBJECTIVES. . . . .	1001	1-2
ASSUMPTIONS . . . . .	1002	1-2
CONCEPT OF OPERATIONS . . . . .	1003	1-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 1

### INTRODUCTION

1000. BASIC POLICY. MCAS Yuma continuously executes a comprehensive AT program that deters, defeats, or mitigates the effects of a terrorist attack and provides protection for DoD personnel, family members, critical assets, and materiel resources.

1001. OBJECTIVES. The installation shall meet the following objectives:

1. The desired end state is an AT program that effectively saves lives and prevents human injury, minimizes mission degradation, and protects government property, in this order.
2. Deter terrorist attacks. MCAS Yuma will dissuade terrorists from targeting, planning against, or attacking the installation's personnel and assets.
3. Employ preventative measures. MCAS Yuma will employ the appropriate mix of preventative measures, both active and passive, to prevent attacks from occurring.
4. Mitigate the effects of an attack. MCAS Yuma will employ the full range of active and passive measures to lessen the impact of an attack.
5. Recover from an attack. MCAS Yuma will design plans to recover from the effects of an attack.

1002. ASSUMPTIONS

1. MCAS Yuma is a potential target for terrorism.
2. Absolute protection is not possible.
3. Attacks may occur with little or no warning.
4. First responders, both military and civilian, may be insufficient to provide total protection for all installation resources; therefore, appropriate AT measures must be developed that ensure unit awareness and provide safeguards for personnel, resources, and facilities.

## ANTITERRORISM (AT) PROGRAM

5. Federal, state, local, and non-military forces will be available to assist in the response and recovery efforts. However, this assistance may not be available for the first twenty four to seventy two hours after a major event has occurred.

### 1003. CONCEPT OF OPERATIONS

1. Reference (a) contains a detailed discussion of Emergency Management (EM) concepts of operation, the majority of which apply to the AT program. Additional, AT-specific concepts include:

a. Information fusion/intelligence will drive the AT program.

b. AT Resource Requirement Documentation and Submission. A key to the success of the AT program is the efficient management of scarce resources; the identification of AT resource requirements must be related to an assessed vulnerability or risk.

c. AT Program Review. MCAS Yuma will conduct an AT Program Review annually that addresses the five elements of an AT program.

ANTITERRORISM (AT) PROGRAM

CHAPTER 2

GENERAL RESPONSIBILITIES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	2000	2-2
RESPONSIBILITIES . . . . .	2001	2-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 2

### GENERAL RESPONSIBILITIES

2000. GENERAL. Antiterrorism is an all hands affair. All personnel, whether military, civilian, or family member, have a role to play.

#### 2001. RESPONSIBILITIES

##### 1. Commanding Officer, MCAS Yuma

a. Retain jurisdiction over all incidents until management responsibilities have been assumed by another agency designated as having primary jurisdiction for such incidents.

b. Set installation Force Protection Condition (FPCON) levels based on intelligence estimates.

##### 2. Director, Installation Security

a. Retain the primary staff cognizance for the Air Station AT program.

b. Retain primary staff cognizance for the preparation, implementation, and revision of this order and supporting plans.

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

d. In conjunction with the Provost Marshal, develop and maintain the installation Barrier Plan.

e. Ensure this order is coordinated with local, state, and federal agencies, as appropriate.

f. Identify unfunded AT requirements.

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

ANTITERRORISM (AT) PROGRAM

4. Supervisory Special Agent, Naval Criminal Investigative Services (NCIS)

- a. Conduct country-specific Area of Responsibility (AOR) briefings as required.
- b. Develop and maintain a counter-intelligence and counter-surveillance program in support of the AT program.
- c. Be prepared to support high-risk personnel security details in accordance with Appendix 4 to Annex C.

5. Provost Marshal

- a. In conjunction with the Director, Installation Security, develop and maintain the installation Barrier Plan.
- b. Establish and maintain an installation-wide mass notification system.
- c. Be prepared to conduct high-risk personnel security operations.

ANTITERRORISM (AT) PROGRAM

CHAPTER 3

INTELLIGENCE/INFORMATION FUSION

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	3000	3-2
OBJECTIVES. . . . .	3001	3-2
ASSUMPTIONS . . . . .	3002	3-2
CONCEPT OF OPERATIONS . . . . .	3003	3-2
RESPONSIBILITIES. . . . .	3004	3-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 3

### INTELLIGENCE/INFORMATION FUSION

3000. GENERAL. This chapter details the concepts and requirements for an intelligence and information collection program that supports MCAS Yuma AT operations.

3001. OBJECTIVES. On a continuous basis, MCAS Yuma will collect all available information, and process, analyze, disseminate and blend sources of threat information in order to enhance the installation's ability to prevent, survive, and prepare to respond to a terrorist attack.

3002. ASSUMPTIONS. Terrorist organizations, whose operational traditions may be either national (to include domestic organizations), transnational, or international may target MCAS Yuma. These groups may be either non-state supported, state supported, or state directed. Such organizations can be expected to operate in a determined fashion to achieve their political goals and are prepared to kill innocent bystanders in the process.

#### 3003. CONCEPT OF OPERATIONS

1. The Threat Working Group (TWG) will be the primary means for the overall analysis and dissemination of threat information. See reference (a).
2. Threat information collection as a result of law enforcement operations will be handled as an operational function. All personnel, documents, and material will be handled through law enforcement channels in accordance with appropriate law enforcement guidance.
3. MCAS Yuma NCIS will manage the collection and analysis of threat information.
4. At least annually, NCIS will prepare an installation-specific threat assessment. The threat assessment shall identify the full range of known or estimated terrorist capabilities. Adequate threat analysis is essential for critical asset identification, vulnerability and risk analysis, the development of FP physical security measures, courses of action, and for FP planning and programming.

## ANTITERRORISM (AT) PROGRAM

5. The Station Commanding Officer will be immediately informed of changes in the threat and will be the only approval authority for changes to the installation threat posture.

6. Patterns of terrorist surveillance, targeting and planning are best recognized through the sharing of information. Therefore, all Commanding Officers on MCAS Yuma will ensure communication channels remain open both up and down the chain of command and with outside agencies.

7. An essential aspect of an effective AT program is trained and alert personnel. In this regard, MCAS Yuma will implement a threat awareness program with the objective of MCAS Yuma personnel remaining vigilant and reporting suspicious persons or activities.

### 3004. RESPONSIBILITIES

#### 1. Director, Installation Security

a. Exercise primary staff cognizance over the development of Commander's Critical Information Requirements (CCIRs) and Priority Intelligence Requirements (PIRs).

b. Develop a Threat Awareness Program and ensure that the program is implemented for all MCAS Yuma personnel.

c. Provide security and classification guidance for the installation in accordance with reference (b). Threat information will be maintained at the lowest prudent security classification to ensure maximum information sharing between DoD and other law enforcement and intelligence agencies.

d. Provide intelligence assistance to NCIS as required.

#### 2. Supervisory Special Agent, Naval Criminal Investigative Services (NCIS)

a. Manage and maintain a terrorist threat intelligence and information collection and analysis program. Develop a Threat Information Collection and Fusion Plan. When local information indicates gaps, forward timely requests for information via appropriate intelligence/information collection and production channels.

b. Coordinate with local, state and Federal law enforcement and intelligence agencies in the collection and dissemination of

ANTITERRORISM (AT) PROGRAM

threat information and security issues.

c. Develop and update an annual installation-specific threat assessment.

d. Provide intelligence updates and threat summaries as required.

e. Conduct country-specific Level I and Area of Responsibility (AOR) briefings as required.

f. Develop and maintain a counterintelligence and counter-surveillance program.

3. Provost Marshal. Ensure security and law enforcement personnel are trained to report suspicious information on individuals, events, or situations that could pose a threat to the security of MCAS Yuma.

4. Commanding Officers/Officers in Charge, Tenant Units

a. Forward up and down the chain of command all information pertaining to suspected terrorist threats or acts of terrorism.

b. Implement a unit Threat Awareness Programs.

c. Ensure personnel are trained to report suspicious information on individuals, events, or situations that could pose a threat to the security of MCAS Yuma.

ANTITERRORISM (AT) PROGRAM

CHAPTER 4

ANTITERRORISM OPERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	4000	4-2
CONCEPT OF OPERATIONS. . . . .	4001	4-2
RESPONSIBILITIES. . . . .	4002	4-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 4

### ANTITERRORISM OPERATIONS

4000. GENERAL. This chapter details the concepts and requirements for MCAS Yuma AT operations.

4001. CONCEPT OF OPERATIONS. AT Operations are divided into three phases - pre-incident, incident, and post incident. See reference (a) for a general discussion of these phases. The following is a discussion of AT-specific phases.

1. Pre-Incident. MCAS Yuma executes its baseline force protection measures. Emphasis during this phase is on physical security and law enforcement, training and exercising installation plans, establishment of memoranda of agreements (MOAs), development of plans to protect high risk personnel (HRP), intelligence gathering and analysis, and execution of security measures. Planning efforts center on the Threat Working Group and the Emergency Management Working Group.

a. Planning tasks to be accomplished during this phase include the following:

- (1) Annual installation-specific threat assessment and periodic update.
- (2) Identification of critical assets. See reference (a).
- (3) Vulnerability analysis. See reference (a).
- (4) Risk analysis. See reference (a).
- (5) Development of courses of action and AT physical security measures.
- (6) AT plan development and annual review; including the development of supporting plans.
- (7) Associated AT resource requirement identification, documentation and submission.
- (8) Annual training and exercises.

b. Operational tasks to be accomplished during this phase include the execution of FPCON measures and AT courses of action

## ANTITERRORISM (AT) PROGRAM

and the implementation of random antiterrorism measures.

2. Incident. A distinct difference between response to a terrorist attack and response to other incidents lies in the nature of the origin of the incident. It is imperative that an incident be identified as terrorist-related as soon as possible. Terrorist-specific considerations include the potential of multiple attacks, including the targeting of first responders by a follow-on attack. Also, the Federal Bureau of Investigation (FBI) must be notified as soon as possible. During this phase, the Station Commanding Officer will determine the modification of FPCONS.

3. Post-Incident. The FBI will most likely be the lead agency during the initial portion of the post-incident phase. Remediation and restoration concerns must be balanced with investigative efforts.

4002. RESPONSIBILITIES. See reference (a) for a general discussion of responsibilities. The following specific AT responsibilities apply:

1. Director, Installation Security. Coordinate the execution of baseline AT measures as well as FPCON measures/courses of action and random antiterrorism measures.
2. Provost Marshal. Execute AT courses of action, AT physical security measures and random AT measures as directed.
3. Tenant Commanders. Be prepared to implement baseline AT security measures, FPCON measures for Alpha through Delta and random AT measures. Coordinate with the Installation Security Department.

ANTITERRORISM (AT) PROGRAM

CHAPTER 5

ANTITERRORISM PHYSICAL SECURITY MEASURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	5000	5-2
CONCEPT OF OPERATIONS. . . . .	5001	5-2
RESPONSIBILITIES . . . . .	5002	5-5

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 5

### ANTITERRORISM PHYSICAL SECURITY MEASURES

5000. GENERAL. AT physical security measures implemented on MCAS Yuma form the backbone of the Stations AT efforts and comprise the first line of defense against a terrorist attack. The MCAS Yuma AT physical security system is based on identified threats, critical assets, and vulnerability and risk analyses. The AT physical security system reflects an integrated approach that employs a layered defense concept. This chapter outlines the layers of defense needed to protect MCAS Yuma facilities and personnel from terrorist attack: baseline (Station-wide) measures, asset-specific measures, Station FPCON measures, tenant unit FPCON Action Sets, and random antiterrorism measures (RAMs).

5001. CONCEPT OF OPERATIONS. The MCAS Yuma AT physical security system is comprised of integrated layers of defense. These layers are designed to progressively enhance and increase the Station's security posture. MCAS Yuma's layers of defense include the following AT physical security measures:

1. Baseline (Station-Wide) Measures. Baseline (Station-wide) physical security measures can be found in reference (c). Tenant unit physical security plans will be incorporated and integrated into the station physical security plan.
2. Asset-Specific Measures. Tenants will implement asset specific levels of protection based on Station FPCON posture, specified threats and the value of the asset. MCAS Yuma-specific MEVAs and HRTs will be published annually in the form of a Station Bulletin.
3. MCAS Yuma-Specific FPCON Measures. The DoD FPCON system as contained in reference (d) is a progressive level of protective measures implemented in response to terrorist threats. Each set of FPCON measures is the minimum that must be implemented when a particular FPCON is declared. Accordingly, MCAS Yuma will develop and implement Station-specific FPCON measures that take into consideration the threat, criticality, vulnerability and risk of the assets requiring protection. Integrated into these measures will be the baseline and asset-specific AT physical security measures previously discussed. Copies of MCAS Yuma-specific FPCON measures can be obtained from the Installation Security Department.

## ANTITERRORISM (AT) PROGRAM

4. Tenant Unit/Department Specific FPCON Action Sets. Tenant Unit Commanding Officers/Department Heads will develop and implement unit/department specific FPCON Action Sets in support of Station-specific FPCON measures. Copies will be provided to the Installation Security Department.

5. Random Antiterrorism Measures (RAMs). RAMs present the image of a hard target to terrorists by conveying an impression of increased vigilance and awareness to terrorists conducting surveillance operations external to MCAS Yuma. RAMs are implemented based upon the current threat and Station security posture. The impact of RAMs on terrorists is difficult to measure, but such programs introduce uncertainty and unpredictability to planners and organizers of terrorist attacks. RAMs alter the external appearance of the Station thus creating unpredictable patterns of security. RAMs also serve to enhance FPCON measures.

a. RAMs provide several advantages, including:

(1) Increased AT awareness for DoD personnel, their family members, and visitors.

(2) Increased alertness among law enforcement and security personnel.

(3) A tool to test which measures have higher costs in terms of productivity than others. RAMs can help identify those measures that security personnel and the installation infrastructure are more capable of sustaining and those that will be unduly stressful on human and materiel resources, to include measures from higher FPCONs.

(4) Training and simulation for security forces. By keeping the security force interested and alert, RAMs increase security, even if they do so only by making the security forces more attentive to their regular assignments.

b. The priority for implementing RAMs is outside-in. The station perimeter and access control points are the primary focus of the RAM program.

c. When the threat or FPCON warrant, tenants will complement installation RAMs by implementing integrated and supportive RAMs within their areas of responsibility. Tenants will notify the PMO, ISD or the EOC, if activated, of all implemented RAMs. The MCAS Yuma Commanding Officer has authority to disapprove the

## ANTITERRORISM (AT) PROGRAM

implementation of tenant RAMs.

d. The implementation of RAMs is not without cost; RAMs will consume time, energy, efforts, and resources. As with changes in the operational tempo of any organization, there may be a slight increase in accidents, minor mishaps, and wear and tear on materials and equipment.

e. RAMs offer an excellent alternative to full implementation of all FPCON measures when terrorist threat estimates suggest that a specific FPCON may not, for the moment, be adequate protection in view of the risk, vulnerability, and criticality of station assets. Selected RAMs extracted from higher FPCONs can supplement a lower FPCON posture and may prove to be a more economical, sustainable response to a terrorist threat.

6. Barrier Plan. MCAS Yuma will execute a Barrier Plan that includes facility standoff, pedestrian, vehicle and visual barriers to control, deny, impede, delay and discourage access to restricted and non-restricted areas by unauthorized persons.

a. Barriers are an integral part of the Station physical security plan. They are used on the perimeter of MCAS Yuma to perform several functions such as establishing boundaries and deterring and intimidating individuals from attempting unlawful or unauthorized entry. Barriers are also used on the perimeter to facilitate pedestrian and vehicle ingress and egress control. Barrier use channels traffic through designated access control points, where pedestrians, vessels, and vehicles can be monitored and searched for contraband, explosives, or other threats as circumstances warrant. Barriers are used outside of and within individual buildings on MCAS Yuma for similar purposes.

b. The Station barrier plan will:

(1) Define the perimeter of restricted areas and establish facility standoff.

(2) Establish a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.

(3) Optimize use of security forces.

(4) Enhance detection and apprehension opportunities by authorized personnel in restricted and non-restricted areas.

## ANTITERRORISM (AT) PROGRAM

(5) Channel the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

### 5002. RESPONSIBILITIES

1. Emergency Management Working Group. Serve as the executive body for the physical security program.
2. Director, Installation Security
  - a. Ensure the AT physical security system is comprehensive, integrated and applicable through all phases (pre-incident, incident, and post-incident) of AT operations.
  - b. Develop baseline (station-wide) physical security measures.
  - c. Develop MCAS Yuma-specific FPCON measures.
  - d. Assist in the development of Tenant Unit/Department specific FPCON Action Sets and barrier plans.
  - e. Review Station FPCONs at least quarterly.
  - f. Recommend to the Station Commanding Officer the implementation of higher FPCON measures as required.
  - g. Develop RAMs.
  - h. Review installation RAMs at least quarterly.
  - i. Coordinate the implementation of RAMs and any higher FPCON measures.
  - j. Document and track through to completion all AT construction projects.
  - k. Supervise the development and implementation of tenant-specific AT physical security measures. Ensuring tenant-specific measures complement and support the Station-wide measures.
  - l. Supervise development and implementation of security engineering and AT construction practices throughout MCAS Yuma.

## ANTITERRORISM (AT) PROGRAM

m. Collaborate with the Provost Marshal on the development of the station barrier plan. Ensure the plan addresses personnel and vehicle ingress and egress.

n. Conduct an annual review of station barrier plan.

### 3. Provost Marshal

a. Coordinate the development of baseline (Station-wide) physical security measures and document in the MCAS Yuma Physical Security Plan. Incorporate tenant unit/organization physical security plans into the Station plan. Ensure the Physical Security Plan includes both physical protective measures and procedural security measures.

b. Collaborate with the Director, Installation Security on the development of the station barrier plan. Ensure the plan addresses personnel and vehicle ingress and egress.

c. Incorporate the implementation of RAMs into routine operations.

d. Assess the effectiveness of RAMs and recommend changes as required.

e. Develop detailed security procedures for the Crisis Management Force.

f. Assist the Directors, Installation Security and I&L in identifying and validating requirements and security lighting systems, electronic security systems, and access control systems. Assist in the development of a long-range plan for these systems.

g. Assist commanding officers and event sponsors in the development and implementation of special event security and physical security measures.

g. Conduct an annual review of station barrier plan.

### 4. Director, Installation & Logistics

a. Procure, resource, and store barrier materials and assist in the execution of the barrier plan as required. Ensure equipment and operators are available to emplace barrier materials.

## ANTITERRORISM (AT) PROGRAM

b. Coordinate the development and implementation of security engineering and AT construction practices throughout MCAS Yuma.

c. Provide management and oversight of all AT construction projects.

### 5. Department Heads/Tenants

a. Develop and document specific AT physical security measures and FPCON Action Sets. As required, supervise the implementation of measures in areas under your cognizance.

b. Ensure facility/building managers prepare site-specific AT physical security procedures, access control procedures and train their personnel to accomplish these procedures/measures.

c. As directed, implement baseline AT physical security measures, FPCON measures and random AT measures. Ensure personnel are trained to implement AT physical security measures.

d. Participate in station AT training and exercises.

e. As required, provide personnel to the Provost Marshal to serve as members of the Crisis Management Force (CMF).

f. As directed, develop and independently implement RAMs within area of operation.

g. Select RAMs that complement and are integrated into the overall installation RAM program.

h. Provide oversight for selection and implementation of facility/building level RAMs under your cognizance. As a general rule, when installation RAM measures do not list specific sites, implement RAM measures at all designated MEVAs, HRTs, and primary gathering buildings (buildings routinely occupied by 50 or more personnel) under your control.

i. Vary times, dates, locations, and time periods of RAMs.

j. Assess the effectiveness of RAMs and recommend changes as required.

k. Provide oversight and execution of RAMs as required.

ANTITERRORISM (AT) PROGRAM

1. Ensure facility/building security managers implement facility/building level RAMs as directed by the Director Installation Security.

ANTITERRORISM (AT) PROGRAM

CHAPTER 6

ANTITERRORISM CONSTRUCTION STANDARDS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL . . . . .	6000	6-2
NEW CONSTRUCTION . . . . .	6001	6-2
EXISTING STRUCTURES . . . . .	6002	6-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 6

### ANTITERRORISM CONSTRUCTION STANDARDS

6000. GENERAL. This chapter prescribes the minimum AT construction design standards that must be incorporated into all MCAS Yuma inhabited structures. Depending on the assessed threat to MCAS Yuma and the level of protection desired for particular high-risk assets, more stringent design standards may be needed. The intent is for the structure to survive well enough to allow people inside the building to safely evacuate in the event of an attack, to provide sufficient protection for personnel survivability, and to mitigate collateral damage, without a bunker mentality.

#### 6001. NEW CONSTRUCTION

1. For new construction and major renovation, the standards identified in references (e) and (f) will be incorporated into the planning, programming, budgeting, and execution of construction activities.

2. The Installation Security Department will be involved in all major military construction (MILCON) planning meeting in order to ensure AT considerations are being considered from design to inception. The ISD will also indicate on all DD-1391 forms (Military Project Construction Data) that the project meets current AT requirements.

6002. EXISTING STRUCTURES. While existing inhabited structures are not mandated to meet the minimum AT construction standards, unless undergoing major renovation or window replacement, mission essential vulnerable assets (MEVAs) and high risk targets (HRTs) will be assessed by the EMWG in accordance with reference (a) for compliance with the standards in references (e) and (f) and to determine structure-specific vulnerabilities, if they do not meet the standards. The EMWG will use this data to prioritize and recommend needed improvements as part of routine facilities upgrades and to support requests for additional funding.

ANTITERRORISM (AT) PROGRAM

CHAPTER. 7

SPECIAL EVENTS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	7000	7-2
CONCEPT OF OPERATIONS. . . . .	7001	7-2
RESPONSIBILITIES . . . . .	7002	7-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 7

### SPECIAL EVENTS

7000. GENERAL. This chapter discusses special events, conducted both on and off the installation. Each event is unique and not all of the considerations listed will apply. Pre-incident measures should be the focus of special events planning. Planning is essential in order to deter, detect, delay, defend, and to mitigate the effects of a terrorist incident.

7001. CONCEPT OF OPERATIONS. Associated with any event there is an inherent degree of risk. Depending on the threat level, appropriate action plans or measures will be implemented to mitigate or deter potential threats.

1. For the purpose of special event planning there are two general categories of events:

a. On-Station Event. These events are the least complex. They are sponsored by an on-Station staff section or organization. An example is the annual Air Show. Depending on the event, it is normally sufficient to coordinate with PMO for event security. For planning purposes, the most current MCAS Yuma Threat Assessment will be utilized. Other departments should be included in the planning as appropriate.

b. Off-Station Event. These events require considerably more coordination, to include coordination with non-DoD entities. Examples include the Marine Corps Birthday Ball, or military parades and ceremonies. Depending on the size of the event, planning requires coordination with the civilian host, i.e. hotel, convention center staff, city planners, etc. In addition, the sponsor may need to contact NCIS, PMO and the Installation Security Department for the current local threat assessment.

2. Mitigation planning must recognize that off-station resources will be the first response, and that civilian medical, fire, and law enforcement points of contact and coordination will need to be in place. Security should be arranged and coordinated through PMO and NCIS. If the sponsor determines the need to provide its own security then that security effort should be coordinated with PMO and NCIS, to include any civilian law enforcement agency.

## ANTITERRORISM (AT) PROGRAM

3. Upon determining the threat level, a special event Force Protection plan may be required. The plan should include a pre-incident phase, an incident response phase, and a post-incident phase.

### 7002. RESPONSIBILITIES

1. The event sponsor or the unit commander is responsible for all Force Protection considerations. The point of contact with local, state, and federal law enforcement agencies is NCIS.

2. Units or activities will use existing Department of Homeland Security Advisory System and FPCONS to keep members informed of the current situation.

ANTITERRORISM (AT) PROGRAM

CHAPTER 8

HIGH RISK PERSONNEL (HRP)

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	8000	8-2
ASSUMPTIONS. . . . .	8001	8-2
CONCEPT OF OPERATIONS. . . . .	8002	8-2
RESPONSIBILITIES . . . . .	8003	8-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 8

### HIGH RISK PERSONNEL (HRP)

8000. GENERAL. Select individuals by the nature of their rank, position, political importance, symbolic value, location or a specific vulnerability or threat may be at greater risk than the general population. Potential targets may include General Officers and civilian equivalents, senior military and civilian leaders and their families. It is imperative that those persons designated as HRP receive the protection commensurate with their position and the existing threat level. As required, MCAS Yuma will take measures necessary to provide appropriate protective services for individuals, assigned to or visiting the installation, that are in high-risk billets or are designated high-risk personnel.

8001. ASSUMPTIONS. Visiting HRP will travel with a security element that provides close-in personal protection.

#### 8002. CONCEPT OF OPERATIONS

1. While there are currently no designated HRP permanently assigned to MCAS Yuma, this is subject to change based on threat intelligence.
2. HRP threat assessments and vulnerability assessments will be conducted to determine the need for supplemental security measures to protect HRP. Supplemental security measures will vary based on threat and available resources. A detailed list of HRP supplemental security measures can be found in ref (g).
3. Individuals receiving supplemental security measures will complete required AT training and will be briefed on the duties of protective service personnel.
4. Visiting HRP protective details are usually short in duration and can be supported with assets organic to NCIS and PMO.

#### 8003. RESPONSIBILITIES

1. Supervisory Special Agent, Naval Criminal Investigative Services (NCIS)
  - a. Develop HRP policy and procedures.

ANTITERRORISM (AT) PROGRAM

b. As required, ensure HRP threat assessments and vulnerability assessments are conducted in order to determine if an HRP warrants supplemental security measures.

c. Ensure HRP security issues are addressed in all operational planning involving HRP.

d. Act as the overall coordinator for HRP visits.

e. Conduct necessary liaison with local, state, federal, and higher headquarters agencies to coordinate issues for HRP visits.

f. Coordinate necessary administrative and logistical requirements to support HRP protection.

g. Ensure personnel assigned to perform personal security detail duties are properly trained and certified.

h. As required, conduct HRP threat assessments.

2. Provost Marshal

a. Ensure personnel assigned to perform personal security detail duties are properly trained and certified.

b. Maintain an explosive detection working dog capability.

3. Public Affairs Officer. Screen news releases as appropriate.

ANTITERRORISM (AT) PROGRAM

CHAPTER 9

COUNTER MANPAD WEAPONS OPERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	9000	9-2
CONCEPT OF OPERATIONS. . . . .	9001	9-2
RESPONSIBILITIES . . . . .	9002	9-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 9

### COUNTER MAN-PORTABLE AIR DEFENSE (MANPAD) WEAPONS OPERATIONS

9000. GENERAL. The terrorist use of MANPADs against military and commercial aircraft operating out of MCAS Yuma cannot be discounted. A particular concern for MCAS Yuma is its geographical location in relation to the U.S./Mexican border. This chapter discusses general plans and procedures to address the MANPAD threat.

#### 9001. CONCEPT OF OPERATIONS

1. Airfield security and local area assessments will be conducted to identify the areas of vulnerability to a MANPAD threat (in terms of possible launch sites) to include the airfield arrival and departure corridors. This assessment will include security force, intelligence, counterintelligence, and operational considerations and will include local authorities.
2. Several organizations, including tenant organizations, can be used to assist in counter-MANPADs planning. These include:
  - a. The Defense Intelligence Agency (DIA). The DIA maintains flight path threat analysis simulation (FPTAS) software that allows the user to quantify the areas of greatest MANPAD threat. FPTAS uses aircraft performance, flight path data, missile characteristics, and digital terrain elevation data to generate maps depicting areas from which MANPADs can engage aircraft.
  - b. The Air Mobility Command (AMC). The AMC maintains a database in with current intelligence and operations information that can assist users in making prudent decisions pertaining to a MANPAD threat.
  - c. The Transportation Security Agency (TSA). The TSA conducts periodic counter-MANPADs assessments of civilian airports. Since MCAS Yuma is a joint use airfield with the Yuma International Airport, these assessments will be used as part of the Air Station's counter-MANPADs program.
  - d. Marine Aviation Weapons and Tactics Squadron-1 (MAWTS-1). MAWTS-1 maintains expertise in Anti-Air Warfare (AAW), including the employment of MANPADs. MAWTS-1 AAW personnel should be

ANTITERRORISM (AT) PROGRAM

consulted as part of the Air Station's counter-MANPADs program.

3. Counter-MANPADs planning considerations should include:

a. Routine flight paths used by aircraft departing and arriving MCAS Yuma. Planning will include visual flight rules and instrument flight rules patterns.

b. Cover and concealment - the ability of an object to provide protection for the terrorist from return fire and prevent detection by security force personnel.

c. Line of sight providing unobstructed view of the target.

d. Exposure time - the amount of time the intended target is vulnerable from an operational attack.

e. Distances to target and target recognition for the terrorist to positively identify the intended target.

f. Accessibility of the location for ease of ingress/egress, set up time required for a terrorist fire team to get into position to attack, and the time to discovery in terms of the amount of time it takes to detect a fire team once their weapons are exposed.

4. Mitigation. If the Air Station receives reports of a MANPADs threat in the local area, the following actions will be taken:

a. Increased physical presence at prime launch sites. PMO will coordinate with local, state, and other federal law enforcement agencies.

b. Consideration will be given to limiting or halting aviation operations.

c. Consideration will be given to the use of tactical countermeasures by military aircraft.

d. Departure and arrival flight patterns will be modified accordingly.

ANTITERRORISM (AT) PROGRAM

9002. RESPONSIBILITIES

1. Director, Installation Security

- a. Maintain current counter-MANPADs studies.
- b. Ensure counter-MANPADs considerations are included in the installation's FPCON Action Set.
- c. Coordinate with the TSA on counter-MANPADs issues.
- d. Provide MANPAD awareness training for PMO and local law enforcement. Training will include weapon and weapon component recognition.

2. Provost Marshal. Be prepared to increase patrolling in areas likely to be used for MANPADs employment against aircraft departing and arriving MCAS Yuma.

3. Operations Officer. Be prepared to modify arrival and departure routes to support counter-MANPADs operations.

ANTITERRORISM (AT) PROGRAM

CHAPTER 10

LOGISTICS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	10000	10-2
ASSUMPTIONS. . . . .	10001	10-2
CONCEPT OF OPERATIONS. . . . .	10002	10-2
RESPONSIBILITIES . . . . .	10003	10-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 10

### LOGISTICS

10000. GENERAL. This chapter discusses the importance and role of the logistics support process in enhancing the AT program. This chapter identifies specific AT considerations and responsibilities that should be integrated for logistics and resource planning, policies and procedures.

#### 10001. ASSUMPTIONS

1. Logistics support requirements will increase following a terrorist act.
2. Some support requirements will increase beyond MCAS Yuma's capabilities.

10002. CONCEPT OF OPERATIONS. Logistics processes, including contracting, will be fully integrated with the AT program.

#### 10003. RESPONSIBILITIES

##### 1. Director, Installation Security

a. Incorporate AT considerations for logistics support into the MCAS Yuma AT program and AT operational planning.

b. Ensure the EMWG periodically addresses AT considerations for logistics and contracting support.

(1) Ensure contracting, engineer, and project leads are present when the EMWG addresses these issues.

(2) Details such as timing of work, the potential types of contractors to be used, and whether a contractor's services are even necessary should be discussed.

(3) Review existing installation-specific AT and risk analysis data to ensure proper coordination and synchronization of potential contract issues.

(4) Careful attention must be paid to establishing a reasonable balance between effective security measures and cost benefit.

## ANTITERRORISM (AT) PROGRAM

c. Periodically review contract compliance with security requirements.

d. Consider contract impact as the threat and FPCON changes.

### 2. Director, Installation and Logistics

a. Incorporate AT considerations for logistics and contracting support into the contracting process and ensure AT guidance is applied to all contracts.

b. Implement a review process to ensure that all contracted support, from construction and facility maintenance to advisory and assistance services, is awarded only after a systematic and disciplined review of security matters and AT requirements.

c. Ensure contract language specifies the contractor's security requirements.

### 3. Comptroller

a. Capture associated costs related to logistics support of AT operations.

b. Assist in the identification and programming of logistics related AT resource requirements.

4. Provost Marshal. Ensure contractors and subcontractors are suitably screened prior to being granted access to the installation.

5. Tenant Units. Provide for the individual equipment needs of assigned personnel, to include CBRN protective equipment, ammunition and weapons.

ANTITERRORISM (AT) PROGRAM

CHAPTER 11

TRAINING AND EDUCATION

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	11000	11-2
ASSUMPTIONS. . . . .	11001	11-2
CONCEPT OF OPERATIONS. . . . .	11002	11-2
INDIVIDUAL TRAINING. . . . .	11003	11-2
RESPONSIBILITIES . . . . .	11004	11-8

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 11

### TRAINING AND EDUCATION

11000. GENERAL. Training and education are essential factors in reducing a terrorist's opportunity to target our forces. Training and education increases the awareness level of personnel and instills a mindset focused on prevention of a terrorist attack rather than post-incident response. In essence, training and education are the cornerstones to making AT an essential part of the way the Air Station operates on a daily basis. MCAS Yuma will provide AT awareness training and education programs in order to prepare individuals, units, and departments to detect, deter, defend and respond to possible terrorist threats. By doing so, MCAS Yuma becomes a significantly less vulnerable target.

#### 11001. ASSUMPTIONS

1. Funds for training are limited.
2. The use of local resources will be maximized.

#### 11002. CONCEPT OF OPERATIONS

1. A properly trained individual is the Air Station's best defense against terrorism.
2. Training will include individual training as well as integrated Air Station exercises such as tabletop exercises, functional exercises, and full scale exercises.

11003. INDIVIDUAL TRAINING. Individual training consists of specific, mandated awareness training and more general awareness training.

#### 1. Mandated Awareness Training

a. Reference (d) mandates specific initial and recurring AT training for all DoD civilian employees and military personnel. Additionally, it requires all DoD contracting agencies to offer AT Awareness Training to DoD contractor employees.

b. Reference (d) details four levels of AT training. Levels three and four are training requirements that are beyond the scope of this order. This order pertains only to Level One

## ANTITERRORISM (AT) PROGRAM

(awareness) and Level Two (ATO) training.

### c. Level One Initial Training.

(1) Uniformed Military Personnel. Not applicable to MCAS Yuma. Initial Level One training is conducted during recruit and initial officer training.

(2) Appropriated Fund Employees. Initial Level One training will be incorporated into the New Employee Orientation program conducted by the Human Resources Office (HRO).

(3) Non Appropriated Fund Employees. Initial Level One training will be incorporated into the New Hire Orientation program conducted by Marine Corps Community Services (MCCS).

(4) DoD Contractor Employees. Not applicable. Contractor employees will only be offered sustainment training.

### d. Level One Sustainment Training

(1) All DoD personnel (uniformed military, APF, and non APF) assigned to MCAS Yuma are required to complete Level One sustainment training on an annual basis. The basis for the completion of this training is the calendar year. The primary method for completing this training is via a web based tutorial program.

(2) This order will be provided to contractor personnel via appropriate Contracting Officer's Representatives. Contractors are encouraged to contact the Installation Security Department for Level One training.

(3) Personnel completing Level One initial training will not be required to complete sustainment training until the following calendar year.

### e. Level Two Training

(1) The installation ATO will complete a Marine Corps recognized Level Two training syllabus.

(2) Only individuals completing a Marine Corps recognized Level Two training syllabus may conduct Level One training.

## ANTITERRORISM (AT) PROGRAM

f. Overseas Travel. Station personnel traveling overseas will receive an AOR-specific AT awareness brief from ISD.

2. General Awareness Training. There are a number of systems designed to make individuals aware of the general threat of terrorism. These systems should be understood by all personnel assigned to MCAS Yuma. The following paragraphs discuss the more common systems.

a. Department of Defense Force Protection Condition Levels (FPCONs). The FPCON is the principal means the Commanding Officer has to apply an operational decision on how to guard against a threat. The Commanding Officer selects FPCONs by assessing the terrorist threat, the capability to penetrate existing physical security systems at the Air Station, the risk of terrorist attack against MCAS Yuma, the ability of the installation to carry on with missions even if attacked, and the criticality to DoD missions of assets to be protected. The Commanding Officer can establish FPCONs. He may establish a higher FPCON than higher headquarters if deemed appropriate. However, he cannot, without permission, lower an FPCON established by a higher commander. FPCON measures are mandatory when declared and can be supplemented by additional measures. The below contains general information about FPCONs; specific FPCON measures are discussed in chapter 5.

(1) There are five FPCONs in current use:

(a) FPCON Normal. This applies when a general global threat of possible terrorist activity exists and warrants a routine security posture designed to defeat the routine criminal threat.

(b) FPCON Alpha. This applies when a general threat of possible terrorist activity exists against personnel and facilities.

(c) FPCON Bravo. This applies when an increased and more predictable threat of terrorist activity exists.

(d) FPCON Charlie. This applies when intelligence is received indicating some form of terrorist action against personnel and facilities is likely.

(e) FPCON Delta. This applies in the immediate areas where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location

## ANTITERRORISM (AT) PROGRAM

or person is imminent.

(2) Ultimately the Commanding Officer must weigh information and balance increased security measures with the loss of effectiveness during prolonged operations and the accompanying impact on quality-of-life.

(3) Once a FPCON is declared, all listed security measures are implemented immediately unless waived by the Commanding Officer.

(4) Units and activities must provide information to their members on the current FPCON, required actions, and points of contact, on a regular basis.

b. The Department of Homeland Security Advisory System (DHSAS). DHSAS, while not specifically tied to DoD threat levels, complements other terrorist threat systems that are in general use. The system is easily recognized by a series of colors, corresponding to a threat level. The following threat conditions each represent an increasing risk of terrorist attacks. Each threat condition lists some suggested protective measures. It is important to note that MCAS Yuma will not take any specific actions based on the DHSAS. Specific MCAS Yuma actions will be taken only based on FPCONs. However, the DHSAS is a good tool for building general individual situational awareness.

(1) Low Condition (Green). This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:

(a) Refining and exercising as appropriate preplanned protective measures.

(b) Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures.

(c) Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

## ANTITERRORISM (AT) PROGRAM

(2) Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. In addition to the protective measures taken in the previous threat condition, federal departments and agencies should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

(a) Checking communications with designated emergency response or command locations.

(b) Reviewing and updating emergency response procedures.

(c) Providing the public with any information that would strengthen its ability to act appropriately.

(3) Elevated Condition (Yellow). This condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous threat conditions, federal departments and agencies should consider the following general measures in addition to the protective measures that they will develop and implement:

(a) Increasing surveillance of critical locations.

(b) Coordinating emergency plans as appropriate with nearby jurisdictions.

(c) Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures.

(d) Implementing, as appropriate, contingency and emergency response plans.

(4) High Condition (Orange). This condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken in the previous threat conditions, federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:

(a) Coordinating necessary security efforts with Federal, State, and local law enforcement agencies.

ANTITERRORISM (AT) PROGRAM

(b) Taking additional precautions at public events and possibly considering alternative venues or cancellation.

(c) Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce.

(d) Restricting threatened facility access to essential personnel only.

(5) Severe Condition (Red). This condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for this condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous threat conditions, federal departments and agencies also should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:

(a) Increasing or redirecting personnel to address critical emergency needs.

(b) Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources.

(c) Monitoring, redirecting, or constraining transportation systems.

(6) Closing public and government facilities.

c. Reporting Points of Contact

(1) Unit/Department AT officer, security manager, and supervisor.

(2) Installation Security Department (928-269-6223/6250).

(3) Installation Naval Criminal Investigative Services (NCIS) (928-269-2305).

(4) Provost Marshal Office (928-269-2361).

(5) Emergency responders, including those not related to terrorism (911).

ANTITERRORISM (AT) PROGRAM

11004. RESPONSIBILITIES

1. Director, Installation Security

- a. Conduct initial Level One training for APF and non APF employees.
- b. Track completion of sustainment and initial (APF and non APF only) training for station personnel.
- c. Ensure the ATO has completed a Marine Corps recognized Level Two course of instruction.
- d. As required, conduct AOR-specific AT awareness briefs for individuals traveling overseas.

2. Director, Human Resources Office. Schedule newly hired employees for initial Level One training. Coordinate with the Director, Installation Security.

3. Director, Marine Corps Community Services. Schedule newly hired employees for initial Level One training. Coordinate with the Director, Installation Security.

4. Contracting Officer Representatives. Provide a copy of this order to contractor personnel. Emphasize that Level One training information is available to contractors via the Installation Security Department.

ANTITERRORISM (AT) PROGRAM

CHAPTER. 12

ANTITERRORISM EXERCISES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	12000	12-2
CONCEPT OF OPERATIONS. . . . .	12001	12-2
RESPONSIBILITIES . . . . .	12002	12-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 12

### AT EXERCISES

12000. GENERAL. This chapter discusses AT exercises. Exercises should be designed to test procedures to react and recover from terrorist incidents that threaten MCAS Yuma's ability to conduct its mission. Reference (a) discusses the Air Station's exercise policies.

#### 12001. CONCEPT OF OPERATIONS

1. AT exercises will encompass all aspects of AT and physical security plans. Additionally, the current baseline FPCON through FPCON Charlie measures will be exercised.
2. AT exercises will use a building block approach, culminating with a full scale exercise.
3. Elements of the AT program may be combined with elements of other program requirements in the same exercise.

#### 12002. RESPONSIBILITIES

1. Director, Installation Security.
  - a. Ensure a comprehensive AT exercise program is developed and implemented.
  - b. Coordinate all AT related exercise activities on MCAS Yuma.

ANTITERRORISM (AT) PROGRAM

CHAPTER 13

PERSONAL AWARENESS CONSIDERATIONS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL . . . . .	13000	13-2
INDIVIDUAL REPORTING REQUIREMENTS . . . . .	13001	13-2
PERSONAL VULNERABILITY . . . . .	13002	13-3
PREDICTABILITY . . . . .	13003	13-4
OFFICE BUILDING SECURITY . . . . .	13004	13-4
SECURITY ENROUTE . . . . .	13005	13-6
SECURITY AT HOME . . . . .	13006	13-8
ACTIONS IF INVOLVED IN A KIDNAPPING . . . . .	13007	13-9
HOSTAGE TAKING . . . . .	13008	13-10

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 13

### PERSONAL AWARENESS CONSIDERATIONS

13000. GENERAL. This chapter discusses general awareness issues for personnel assigned to MCAS Yuma. Force protection anomaly reporting is critical to defeat future terrorist attacks. After action reviews of terrorist attacks typically indicated observations of, but not reporting of, suspicious behavior. Single incidents are reportable as they may coincide with other reporting requirements. Reference (a) details first responder actions for many of the below scenarios. This chapter discusses considerations for individuals. It is a good refresher; however, it is not designed to replace Level One training as discussed in chapter 11. Additionally, the measure described below should not be construed as directive in nature. They are merely things to be considered - common sense should prevail.

13001. INDIVIDUAL REPORTING REQUIREMENTS. There are six categories of information that may indicate pre-operational terrorist activity. Individuals must know to observe and report the following:

1. Specific Threats. Report any threats received by any means that contain a specific time, location, or area for an attack against US forces. This may include any event or incident that indicates a potential threat to US forces, facilities or mission.
2. Surveillance. Report any attempt to record information or use unusual means to monitor activities. Examples of surveillance include use of cameras (still or video), note taking, annotated maps or drawings, or use of binoculars.
3. Elicitation. Report any attempt to obtain security related information by personnel not having an appropriate clearance or need to know. Queries can be in many forms, including by mail, fax, telephone, or in person. Documents that are "For Official Use Only" such as recall or alert rosters fall into this category. Do not divulge this information to personnel except on a need to know basis.
4. Tests of Security. Report any attempt to measure security reaction times. Examples of security tests include penetration of physical security barriers, testing of base-entry procedures,

ANTITERRORISM (AT) PROGRAM

and attempting to acquire duplicate uniforms, badges, or passes.

5. Repetitive Activities. Report any activity observed or repeated two or more times within a one-month period. Examples include activities by the same person or same vehicle, or multiple requests for the same information (classified or unclassified).

6. Suspicious Activities or Interests. Report any incident that does not fall in a specific category but is suspicious in nature. Examples include thefts of material that could be used to manufacture false identification cards or badges, missing documents, or evidence of tampering.

13002. PERSONAL VULNERABILITY. To begin a general terrorist threat assessment of your personal vulnerability, address the following questions:

1. Are you a publicly recognizable member of your organization's management or technical team with an assigned parking space?
2. Do you normally drive or ride in a "prestige" automobile or display a special license plate?
3. Do you drive the same route between home and work each day? Arrive at the same time each day? Buy your gasoline at the same station?
4. In the past 18 months, has your name or photograph appeared in any newspaper, magazine, trade journal or organizational publication?
5. Do you, or members of your family, engage in a regularly scheduled recreation or fitness program -- jogging, swimming, golf, tennis, or handball -- which is usually conducted weekly at the same location?
6. If you answered "yes" to two or more of these questions, it is a pretty good indication that a terrorist would have little trouble identifying you, following you home, or keeping you under surveillance. You are not a "low profile" person. It might be prudent for you to take increased notice of your surroundings and people as you move through your day. Consider these observations:

## ANTITERRORISM (AT) PROGRAM

- a. Is someone watching your home?
- b. Is your car being followed?
- c. Has your office received recent inquiries about your plans?
- d. Have you noticed anyone taking photographs near your home, car, or office?
- e. Have you seen strangers in the parking lot?
- f. Has a meter reader, building inspector, or repairman visited you recently?
- g. Any of these observations could be indications of possible terrorist targeting. As preventative measures, try to be more conscientious about what is going on around you -- your curiosity about activities around you is an excellent self-protective action. Try to develop a new habit - self-protective curiosity. Don't be predictable in your daily activities.

### 13003. PREDICTABILITY

1. First, and most important of all, honestly examine the existing patterns associated with your day-to-day life. Do you leave home for the office at the same time every morning? Do you drive the same route each day? Do you park in the same space, use the same door, or eat in the same restaurant?
2. Routine habits can be deadly. Repetitious day-to-day routines can do more to make you a terrorist target than any other activity. Terrorists rarely attack people who do not have rigid daily habits, simply because they cannot accurately prepare their trap. Remember:

SAME TIME + SAME ROUTE + SAME PLACE = TEMPTING TERRORIST TARGET

### 13004. OFFICE BUILDING SECURITY

1. Many security precautions are simply the application of common sense and are not costly. Be alert to anyone loitering near your office building. Avoid working late on a routine basis. Avoid routinely going into the office on weekends when nobody else is there.

## ANTITERRORISM (AT) PROGRAM

2. Do not clutter building lobbies with plants, displays or art objects that could conceal the presence of a suspicious package or object. Do not place pictures of personnel in the lobby or put their names on the building directory. Avoid listing personnel by name/rank/title in telephone books or rosters.
3. Limit public access to your building. Ground floor offices are especially vulnerable. Do not place desks near the windows. Keep the window blinds closed to prevent observation from outside. Do not place name signs outside offices. Restrooms should be locked as should all maintenance closets, electrical and telephone rooms. Keys should be inventoried and issued on a very restricted and controlled basis. Parking spaces should be marked with numbers rather than nameplates or titles and they should be scattered throughout your parking lot, not concentrated in a row close to the building.
4. Instruct office assistants not to provide any information on travel plans, dates of departure, airlines, hotels, and so forth to any caller. Do not convey over the phone the absence of personnel in the office.
5. Impress upon all employees that they should be alert to unfamiliar personnel or deliveries. Particular attention should be directed at packages left behind, boxes or briefcases in lobbies, restrooms, stairwells, and coffee shops.
6. Develop, implement, and practice regularly scheduled drills to cope with fire, bomb threats, and intrusion. Establish notification instructions for emergencies such as accidents, kidnappings/hostage taking, or violent intrusions.
7. Limit normal visitor entry and exit of the building to one or two well marked, clean, lighted doorways. Encourage employees to escort their visitors when they are inside the building and to stop and offer escort assistance to anyone who is not an organization employee.
8. Instruct janitors, maintenance personnel, and loading dock personnel to keep their area doors closed and locked except when in use.
9. Good housekeeping practices applied to your building, its entrances, grounds, and parking lot act as a deterrent to attack. A clean, neat, uncluttered, businesslike appearance sends the terrorist a "message" that the people inside are not negligent, careless or sloppy. Your office or home environment

## ANTITERRORISM (AT) PROGRAM

tells the terrorist that you have a security program. Terrorists prefer to attack unprotected and unconcerned targets.

### 13005. SECURITY ENROUTE

1. Many attacks directed against personnel occur when they are transiting between their homes and their offices. Specifically these attacks occur while:
  - a. Walking to an automobile.
  - b. Traveling in an automobile.
  - c. Walking from an automobile.
2. The key to minimizing personal vulnerability to kidnap, hostage-taking, assassination or other forms of attack is simple -- avoid repetition and habit patterns during these high threat movement periods. Vary time of departure and arrival from day to day. Do not transport personnel in attention attracting "prestige" vehicles. When traveling in an automobile keep the windows closed and the doors locked. Park vehicles off the street and under cover at night. Lock cars no matter how short a time they may be unattended.
3. Install an alarm system on the automobile and test it daily. Before entering the vehicle look underneath and all around it to be sure that no suspicious objects, strings, wires, or devices have been attached. If you find anything suspicious, immediately notify authorities; take no actions other than moving to a safe location away from the vehicle.
4. Remember that terrorists usually watch potential targets for days before they attempt an attack. Before leaving your home or office, spend a few minutes looking around the street. Are there any cars, trucks, vans, or motorcycles that look out of place or that seem to be "waiting" at the curb, particularly near your home. As you drive, watch your rear view mirrors and take note of any vehicle that may be following you. If you think you are being followed make two right turns and go back where you came from or pull into a safe haven.
5. Safe Haven. A Safe Haven can be defined several ways:
  - a. It can be any place along your route of travel where you could go and where terrorists probably would not follow, such as a police department, firehouse, military base, factory gate,

## ANTITERRORISM (AT) PROGRAM

etc.

b. At home or in the office, a Safe Haven is normally a strong, secure room or closet containing essentials to sustain life for a limited time plus communications to call for assistance.

c. When driving, use main roads and thoroughfares and avoid secondary roads as much as possible. Drive your vehicle in the lane closest to the centerline. This makes it more difficult for attackers to force you to a stop or force you off the road.

d. Keep at least one-half car length of empty space in front of your vehicle when stopped at traffic signals and stop signs. This gives you room to maneuver your car if you need to escape a kill zone or kidnap attempt.

e. Keep your car in gear ready to move and keep your hand on the horn. Watch what is going on around you, particularly to your rear. If individuals on foot move toward your vehicle, rev your engine and rock or jerk your car forward and backwards in the space you have available. Blow the horn to attract attention. Notify the authorities immediately.

f. Select three to five different travel routes from home to office and use a different route each time you travel. Be careful not to use the same routes on particular days. Watch that you do not fall into the habit of using a "favorite" route more than others. Avoid all detours and do not stop for people in distress - both are commonly employed traps.

g. Do not gas up at the neighborhood service station. Stop at different well-lighted stations along your various travel routes. Keep your fuel tank at least half full.

h. Remember, when you are walking to your vehicle, and walking away from your vehicle, especially between your residence and your vehicle, you are at the greatest period of vulnerability and risk in your entire day. Be observant, alert, and aware of your surroundings. Develop these skills into new personal protection habits.

## ANTITERRORISM (AT) PROGRAM

### 13006. SECURITY AT HOME

1. Both criminals and terrorists consider the home a tempting target. Some common sense precautions will help to deter both.
2. Do not advertise where you live. Take your name off the mailbox and the front door. Do not have department stores, dry cleaners, or grocery firms deliver to your home.
3. Do not pose for newspaper photographs at social, business or sports events. Keep a very low public profile.
4. Park your car inside a garage, not on the street. Keep the garage locked at all times.
5. Install a peephole device on all entrance/exit doors so that visitors may be observed. It is also a good idea to install a two-way communication system at the doors. All outside doors should be solid wood or metal with no glass. Deadbolt locks should be installed on exterior doors. Doorways should be well lighted by at least two separate fixtures. Sliding glass doors and French doors should be secured with anti-entry bars and locks.
6. Ground floor windows and upper story windows accessible from balconies, trees, or low roofs should be fitted with iron grills. Keep all window curtains and blinds tightly closed after sundown. It is also a good idea to coat all ground floor windows with mirrored plastic film which makes the glass much more difficult to break or cut and limits daytime viewing into the house. Mylar shatter-resistant window film is one of several choices.
7. Install a quality burglar alarm system that has an exterior horn or siren and ask your neighbors to call the police if it should sound. Consider running a buried private telephone or intercom line to a neighbor's house so that you can call for assistance even if the terrorist cuts your phone lines.
8. Home security should be discussed with all family members. Do not frighten them, but honestly discuss their safety and security and at least establish procedures for how the door is to be answered and what is discussed over the telephone. You should assume that someone is listening to all your telephone conversations and you should never discuss family travel plan, pickup points, or appointments on the telephone.

## ANTITERRORISM (AT) PROGRAM

9. Do not let anyone into your home to make an "emergency" phone call. Keep them outside and make the call for them.

10. If you have children, they should be escorted to and from school and school authorities should never release children to any person who is not a family member. All family members should be careful not to establish fixed recreation or fitness habits such as tennis every Tuesday and Saturday, or jogging every day at 0600, etc.

11. Request or develop mutual assistance security programs with your neighbors. Plan and regularly hold family drills for emergency situations such as fire, the burglar alarm sounding, or forced entry. Designate a room - usually an upstairs bedroom - as a home "SAFE HAVEN". Reinforce the door, door hinges, and doorframes. Install an intercom to a source of assistance and stock the room with emergency supplies. If the room has a window, install interior shutters with a lock or bar. Explore the possibility of constructing a hidden emergency escape route from the room to the roof - these are best constructed inside a closet or bathroom.

12. While these security suggestions may sound frightening and restrictive, the lifestyle changes and discomfort associated with their employment is far less than that associated with the victimization, kidnap, injury, or death of a family member. The person most interested in your continuing safety should be you.

13007. ACTIONS IF INVOLVED IN A KIDNAPPING. Consider the following:

1. As you step out of your car, you are suddenly confronted by three armed men in ski masks. What should you do? Don't struggle or attempt to run! Physical resistance, verbal banter, or sarcastic remarks at this point may lead to physical abuse or death. Remember that the attackers are also scared and "uptight" and may react violently and irrationally to any provocation. Many "Plan B's" to an unsuccessful kidnapping translates to an assassination. Listen to their instructions and quietly do what you are told.

2. After the first few moments or while you are being driven away from the scene quietly let your attackers know of any medical problems you may have. It is important that you let the terrorist know immediately if you have a heart condition, diabetes, or allergies - they may intend to drug you or give you

## ANTITERRORISM (AT) PROGRAM

an injection to keep your quiet.

3. Force yourself to be calm and keep your brain alert. Make mental notes about your captors, their speech patterns, mannerisms, physical characteristics, who is in charge, the type of vehicle, where you are going, landmarks, time, speed, and distance. Try to draw a mental map. Note any distinctive sounds such as trains, airplanes, heavy traffic, horns, bells, construction, and any special odors you may encounter. Use your eyes, ears, nose and brain.

4. Later on, try to establish some measure of rapport with your captors at the same time maintaining your dignity, poise, and honor. Listen to the questions they ask and think very carefully before you answer. Do not lie, but do not volunteer any information, and do not discuss the probable reactions of your organization, family, friends, or the authorities. Do not discuss your organization's security arrangements, emergency plans, ransom payments, or your financial wealth. Do not discuss politics, race, religion, or ideologies.

5. Later still, try a few legitimate complaints on your captors and note their reactions. Complaints relating to the quality of the food, lack of physical cleanliness, need for medication, exercise, or reading material are "legitimate." Keep your mind constantly occupied; establish daily routines so that you always have something to look forward to. Exercise daily and closely monitor your own physical and mental health.

6. Kidnap or hostage victims rarely have the opportunity to overpower their guards or to escape. No attempt to escape should be made unless it has been carefully planned in conjunction with a real (not imagined) opportunity. Escape should be attempted only by a person who has the physical skills and mental discipline necessary to ensure the best possible odds of success. Remember that the majority of kidnap or hostage victims are eventually released unharmed and resume normal lives. While being held captive, remember that there are many talented and courageous people working to obtain your release - be patient and have faith.

### 13008. HOSTAGE TAKING

1. If you are involved in a hostage taking incident at your work place, after you attempt to notify authorities, look around your workspace and see if you can find a more protected area. If there is an adjacent restroom, storage or work area that does

## ANTITERRORISM (AT) PROGRAM

not have a hall door, consider hiding in that room and locking the door. If possible, take the telephone with you. Stay on the floor behind heavy objects such as filing cabinets or bookshelves and mentally take stock of the situation and your position. Hide your wallet and identification.

2. If you are detected and are ordered to come out of hiding, do so. Stay calm, keep quiet, and do exactly what you are told to do. This is not the time for bravado or bluster. Carefully observe, make mental notes, identify the terrorist leaders, and be patient. Time is on your side. Remember that in most terrorist hostage situations, the hostages are eventually released unharmed.

3. While you are waiting to be released, a good mental exercise might be to plan how you will improve security and individual preparedness so that this type of threat situation cannot happen again.

4. If there is an attempted rescue, get down on the floor immediately and stay there no matter what happens. Do not yell or attempt to run. Wait to be told what to do. You will most likely be considered as a threat by law enforcement officers until they can ascertain your status. Therefore, expect to be treated as such (ie, handcuffed, searched, etc.).

ANTITERRORISM (AT) PROGRAM

CHAPTER. 14

COMMUNICATIONS AND COMPUTER SYSTEMS

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	14000	14-2
ASSUMPTIONS. . . . .	14001	14-2
RESPONSIBILITIES . . . . .	14002	14-2

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 14

### COMMUNICATIONS AND COMPUTER SYSTEMS

14000. GENERAL. Users of Information Technology (IT) are increasingly dependent on network IT-based Command & Control systems (C2S) to process and transfer daily administrative and operational information. Consequently, external and internal threats to these systems increase the likelihood that a successful attack may degrade or wholly disrupt daily administrative and operational tasks. Reference (h) promulgates Marine Corps policy on Information Assurance (IA). This chapter establishes policy as it pertains to AT operations.

#### 14001. ASSUMPTIONS

1. During attack preparation and planning, terrorist groups' efforts may include, but will not be limited to: monitoring of unencrypted communications, disruption of computer network operations, and attempts to gain unauthorized access to computer systems containing sensitive Antiterrorism (AT) information.
2. Communications and computer systems may be the primary targets of terrorist attacks.

#### 14002. RESPONSIBILITIES

1. Director, Communication Data and Electronics
  - a. Provide IA awareness indoctrination and annual IA refresher training in accordance with reference MCO (h).
  - b. Ensure current IA standard operating procedures are available, used, and updated regularly for each information technology resource.
  - c. Ensure computer intrusion incidents, or suspicion of any, are reported to the Intrusion, Detection, and Analysis Section of the Marine Corps Information Technology and Network Operations Center.
  - d. Establish Information Operations Conditions (INFOCON) as required to support AT operations. The decision to change INFOCON levels will be based on assessed threat, vulnerabilities, extant situation, and the effect the action would have on all MCAS Yuma operations.

ANTITERRORISM (AT) PROGRAM

CHAPTER 15

ANTITERRORISM RESOURCE MANAGEMENT

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL. . . . .	15000	15-2
CONCEPT OF OPERATIONS. . . . .	15001	15-2
LOCAL AND MARINE CORPS PROVIDED FUNDING. . . . .	15002	15-2
UNFUNDED REQUIREMENTS. . . . .	15003	15-3
COMBATING TERRORISM READINESS INITIATIVES FUNDS. . . . .	15004	15-3
RESPONSIBILITIES . . . . .	15005	15-3

# ANTITERRORISM (AT) PROGRAM

## CHAPTER 15

### ANTITERRORISM RESOURCE MANAGEMENT

15000. GENERAL. The dynamics of the terrorist threat and the evolving AT mission require AT resources to ensure the safety and security of MCAS Yuma and personnel. The resources may be needed to meet emergency or emerging threats in the short term (weeks or months) or longer-term threats (years). To obtain resources to implement antiterrorism activities, requirements must be identified, justified, prioritized, documented, submitted, obtained, and tracked through various processes. This chapter provides instructions and guidance for those tasks regarding AT resource management.

#### 15001. CONCEPT OF OPERATIONS

1. AT resource requirements will be identified through the Risk Management process. See reference (a).
2. There are three basic sources of funding:
  - a. Local and Marine Corps provided funding.
  - b. Unfunded Requirements (UFRs) through the Planning, Programming, Budgeting, and Execution (PPBE) process.
  - c. Combating Terrorism-Readiness Initiatives Funds (CbTRIF).
3. The Comptroller will guide the use of local and Marine Corps provided funding.
4. UFRs and CbTRIF processes will be under the cognizance of the Installation Security Department and will be effected via the Core Vulnerability Assessment Management Program (CVAMP).

15002. LOCAL AND MARINE CORPS PROVIDED FUNDING. If local and Marine Corps-directed funds are available, the Installation Security Department will implement approved courses of action to mitigate risk. If current allocations of funds are not available, the Installation Security Department will work with the Comptroller's Department to develop a recommendation for internal reallocation of resources. The Installation Security Department will present the reallocation recommendations with justifications through the Resources Allocation Committee to the Station Commanding Officer for a decision and implementation as

## ANTITERRORISM (AT) PROGRAM

directed. If funds are not available, the Installation Security Department will pursue resources as described in paragraphs 15003 and 15004, below.

15003. UNFUNDED REQUIREMENTS. If resources are not available through current allocations or from local and Marine Corps-directed and controlled resources, the resource requirement will be considered an Unfunded Requirement (UFR). Requirements must compete with other higher headquarters responsibilities and priorities. CVAMP will be used to submit AT-related data to local and higher headquarters as required.

15004. COMBATING TERRORISM READINESS INITIATIVES FUNDS. The Installation Security Department can request funding through a Combating Terrorism Readiness Initiatives Fund (CbTRIF) submission. The fund allows combatant commanders to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of risk assessments and exercising AT plans. CbTRIF is not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities that are normally a Service responsibility. Hence, articulating and justifying resource requirements is crucial. Reference (i) contains amplifying guidance.

### 15005. RESPONSIBILITIES

#### 1. Director, Installation Security

a. Supervise the development of AT resource requirements to ensure thorough documentation, prioritization, and justification.

b. Develop a realistic and affordable fiscal year budget and procurement strategy for AT resource requirements.

c. Supervise the review process involving EMWG members, Comptroller, and Staff Judge Advocate that provides cost, scheduling, status, documentation, justification, prioritization, and other AT-related data regarding resources as needed.

d. Develop life-cycle costs (e.g. manpower needs, logistics, maintenance, etc.) for resource requirements when considering funding requirements.

## ANTITERRORISM (AT) PROGRAM

- e. Utilize the Core Vulnerability Assessment Management Program (CVAMP) tool as appropriate to submit AT funding requirements and requests.
- f. Track funds obtained through the CbTRIF process to ensure they are obligated within the constraints contained in reference (i).
- g. Assess the importance of AT resource requirements as determined through the risk management process to determine if an internal reallocation of funding is appropriate and feasible.
- h. Provide AT funding and project status reports as required.

### 2. Comptroller

a. Provide fiscal guidance and oversight for the MCAS Yuma AT Resource Management program and ensure compliance with fiscal regulations.

b. Allocate funds for supplies, service, or equipment for AT-related activities.

c. Review CbTRIF submissions.

d. Submit UFRs to higher headquarters as required.

3. Staff Judge Advocate (SJA). Review CbTRIF submissions.

4. Emergency Management Working Group (EMWG). Develop recommendations for the use of funds for AT course of action implementation.

ANTITERRORISM (AT) PROGRAM

CHAPTER 16

ANTITERRORISM PROGRAM REVIEW

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL . . . . .	16000	16-2
CONCEPT OF OPERATIONS . . . . .	16001	16-2
RESPONSIBILITIES . . . . .	16002	16-3

ANTITERRORISM (AT) PROGRAM

CHAPTER.16

ANTITERRORISM PROGRAM REVIEW

16000. GENERAL. This chapter establishes policies, procedures and responsibilities for the development and implementation of the MCAS Yuma AT Program Review.

16001. CONCEPT OF OPERATIONS

1. MCAS Yuma will conduct an AT Program Review annually that addresses the following five elements of an AT program:

- a. Risk management.
- b. Planning.
- c. Training and exercises.
- d. Resource generation.
- e. Program review.

2. The annual program review will evaluate each of the five elements as follows:

a. Risk Management Process

- (1) AT Threat Assessment.
- (2) Criticality Assessment.
- (3) Vulnerability Assessment.
- (4) Risk Assessment.

b. Planning

- (1) Station FPCON Action Sets.
- (2) Threat Assessment and Response.
- (3) AT Program Review.
- (4) Physical Security Measures.

ANTITERRORISM (AT) PROGRAM

- (5) Incident Response.
- (6) Consequence Management.

c. Training and Exercises

- (1) Level One Training.
- (2) Level Two ATO Training.
- (3) High Risk Personnel and High Risk Billets.
- (4) Annual AT Exercise.

d. Resource Generation

- (1) Generating requirements.
- (2) Prioritizing resource requirements.
- (3) Funding sources.
- (4) Unfunded requirement submissions.

e. Program Review

- (1) AT Plans and Programs.
- (2) Counter intelligence, law enforcement liaison, and intelligence support.
- (3) AT physical security measures.
- (4) Vulnerability to a threat and incident response measures.
- (5) Terrorist use of WMD.
- (6) Local community and tenant support.

16002. RESPONSIBILITIES

1. Director, Installation Security

- a. Develop and implement annual AT program review utilizing EMWG.

ANTITERRORISM (AT) PROGRAM

b. Annually brief the station Commanding Officer on the status of the AT program.

c. Maintain copies of the annual AT program review.

2. Department Heads/Tenant Units. Support the annual program review process via the EMWG.

3. Emergency Management Working Group. Support the Director, Installation Security in the annual program review process.