



UNITED STATES MARINE CORPS

11TH MARINES

BOX 555503

CAMP PENDLETON, CALIFORNIA 92055-5503

3000
AFP
25 Aug 20

REGIMENTAL ORDER 3302

From: Commanding Officer, 11th Marines

To: Distribution List

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

Ref: (a) DoD Instruction O-2000.16, DoD (Antiterrorism) Standards
(b) DoD Instruction O-2000.16, DoD (Antiterrorism) Force Protection Condition (FPCON)
(c) DoDD 2000.12, DoD Antiterrorism Program
(d) DoDO 2000.12H, DoD Antiterrorism (AT) Handbook
(e) NAVMC 3500.103, Marine Corps Antiterrorism (AT) Manual
(f) MCO 3302.1E, Marine Corps Antiterrorism Program
(g) AreaO 3302.1A, SOP for 43 Area All Hazard Plan
(h) MCO 5530.14A, Marine Corps Physical Security Program Manual
(i) 1st Marine Division AT Plan
(j) 43 Area Guard Force Augmentation Plan

Encl: (1) Terrorism Threat Assessment (S) / (Not Attached)
(2) MCI-West Camp Pendleton All Hazard Threat Assessment (FOUO) / (Not Attached)
(3) 11th Marines FPCON Action Set Matrix (FOUO) / (Not Attached)
(4) 11th Marines Barrier Drill Procedures (FOUO) / (Not Attached)
(5) 11th Marines Random Antiterrorism Measures Program (FOUO)
(6) Risk Management Methodology to 11th Marines Antiterrorism Plan 2020
(7) 11th Marines Asset List (FOUO) / (Not Attached)
(8) Emergency Lockdown Procedures
(9) Shelter in Place Procedures
(10) Glossary

1. Situation

a. General. The threat of terrorist attacks is one of many challenges facing 11th Marines and the 43 Area. This constantly evolving threat shows no signs of abating, but rather of growing in intensity and sophistication. Recent terrorist attacks accentuate the need for antiterrorism programs to keep pace with the asymmetrical and amorphous threats we confront. However, the threats that endanger the security and well-being of 11th Marines Regiment elements, personnel, and operations are not limited to terrorism. Manmade threats, natural hazards, and unintentional and intentional acts are additional threats that the 11th Marines AT program must also address.

b. Enemy Forces. For the purposes of this plan, there is no specified enemy force. However, an all-hazards threat approach will be used to identify threats or hazards that have a probability of occurring within Area 1. Annually, MCIWEST-MCB CAMPEN publishes an All Hazard/Threat Assessment (AHTA) that identifies a comprehensive list of threats and hazards which have a likelihood or probability of occurrence. This assessment is specifically tailored to Camp Pendleton, California and aids in the development of this AT plan.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

c. Friendly Forces

(1) The Camp Pendleton Provost Marshal (PMO) is responsible for the primary organic security element and has the responsibility of securing the perimeter of the installation, controlling entry to the installation, and providing installation security. The provost marshal mission requires its individual patrolmen and sentries to maintain the capability of employing their weapons expeditiously as the situation dictates. Therefore, on-duty military police are armed with loaded weapons.

(2) Additional friendly forces include all units aboard Camp Pendleton; local, state, and federal law enforcement agencies; and city, county, and state disaster response organizations.

(3) An antiterrorism working group (ATWG) will convene quarterly with a representative from (see this document under task for representatives and responsibility.)

a. Assumptions. 11th Marines is a potential target for terrorism, criminal activity, and civil disturbances and is also subject to man-made or natural disasters. An opposing threat can be difficult to predict, but opposing forces should be regarded as armed and dangerous. Therefore, necessary precautionary measures should be taken to ensure the safety of personnel, facilities and equipment. Base guard/PMO alone is inadequate to prevent a determined terrorist force from breaching perimeter security due to the overall accessibility of the base's area. Any terrorist attack will affect both military and civilian activities. Mutual assistance between the military, civilian law enforcement organizations and emergency management agencies is necessary to protect against an ever-changing threat.

b. Intelligence. MCIWEST-MCB CAMPEN provides tenant commands with intelligence on manmade threats and natural hazards through resources via the Mission Assurance (MA) Branch and the Installation Emergency Manager. The AT Officer, in conjunction with the 11th Marines Intelligence Officer, will request any threat intelligence that is required. The Regiment Intelligence Officer must coordinate and continue to coordinate with the MEF Counter Intelligence Marines for CI insider briefs.

2. Cancellation. None.

3. Mission. 11th Marines implements force protection measures and integrates antiterrorism efforts with Camp Pendleton and higher headquarters in order to deter, detect, and delay potential threats while defending personnel, facilities, and equipment against the effects of criminal threats, terrorist threats and natural disasters.

4. Execution

a. Commander's Intent. To develop an operational capability that provides a defense in depth against all threats in order to protect military personnel, civilian employees, families, facilities, and equipment from acts of terrorism, criminal acts, and destructive (or potentially destructive) events by creating proactive and reactive measures in accordance with reference (b).

b. Concept of Operations. The protection of the 11th Marines personnel and assets from natural disasters (such as severe weather) and manmade incidents (ranging from hazardous material spills to terrorist acts) presents many complex challenges. Managing an appropriate response capability to these diverse incidents requires an innovative, comprehensive, and integrated approach. This AT plan establishes a baseline posture from which the command can respond to potential or realized hazards and threats to maintain or restore operational capabilities. Effective immediately, all personnel will follow the guidelines in this plan in order to protect personnel, facilities, and equipment from terrorist acts or other hazards. All personnel will maintain a heightened awareness and report any suspicious activity to

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

appropriate authorities. This plan will provide guidance for the antiterrorism program and includes the five essential program elements: [risk management, planning, training and exercises, resource applications, and a comprehensive program review.]

(1) 11th Marines employs an interior guard (43 Area Guard) to provide security over fixed locations and assets within the area of responsibility. The interior guard's primary mission is to preserve order, protect property, and enforce regulations within the jurisdiction of the Regimental/Area Commander. This mission requires designated personnel to be armed and capable of effectively employing their weapons should the situation dictate; they must be armed with loaded weapons.

(2) Risk Management. Risk management consists of two major functions: risk assessment and risk planning. All components of risk management will be factored in when determining the hierarchical rating from which asset is most at risk to those least at risk of degrading 11th Marines' ability to perform its primary mission.

(a) Risk Assessment. A risk assessment will be conducted annually by the AT Working Group (ATWG) using the process identified in reference (a). Identified changes to the threat may require more frequent ATWG meetings. The risk assessment will include the AHTA, a criticality assessment, and a vulnerability assessment.

1. All Hazards Threat Assessment (AHTA). The AHTA is used to create the Installation Threat/Hazard Matrix. The AHTA provided by MCIWEST-MCB CAMPEN and is contained in enclosure (2). This enclosure is updated annually.

2. Criticality Assessment. Utilizing the Regiment's approved Mission Essential Tasks (METs) with their associated conditions and standards, assets associated with the execution of these METs can be identified. The criticality assessment will examine those assets whose degradation or destruction will affect, or the consequence of loss will affect, the Regiment's ability to complete its approved METs (core or assigned). Assets include people, physical entities, systems or information that provides a service or capability.

3. Vulnerability Assessment. A vulnerability assessment will be conducted on every critical asset listed in enclosure (7). Each asset will be assessed for its vulnerability to specific threats provided in the AHTA and Installation Threat/Hazard Matrix. The unit antiterrorism officer (ATO) will conduct the vulnerability assessment using the vulnerability worksheets contained in references (b) and (d).

4. Risk Assessment. A risk assessment will be conducted on every critical asset listed in enclosure (7). 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 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, and vulnerability assessments, a risk assessment is produced for risk analysis.

5. Risk Analysis. The risk analysis will be conducted on every critical asset listed in enclosure (7). While the risk assessment process seeks to evaluate and identify risk, risk analysis and response is the process of determining options and actions to reduce the risk of loss to the asset, and thus reduce impact on mission execution. The options/actions step includes risk mitigation in the form of procedural recommendations and countermeasure strategies in the form of programmatic recommendations.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

(b) Risk Planning. When all critical assets have been assessed, controls measures will be implemented to mitigate the risks to each asset in order to deter terrorist activity from occurring and/or minimize the effects of potential attacks.

(c) Planning. This AT plan will lay the foundation to prepare, mitigate, deter, detect, delay, and defend personnel, property, and resources from the effects of natural disasters or manmade incidents. The planning phase is continuous as new threats arise or existing threats change.

(d) Training and Exercises. Required annual training will be conducted for all active duty Marines, Sailors and civilian employees in addition to updated briefs on threats both aboard the installation and in the local area. Training exercises will be used to validate the plan and the awareness of personnel within the unit.

(e) Resource Application. After conducting the risk management process, identified shortfalls that cannot be sourced internally will be elevated to higher headquarters for assistance. Additional resource procurement options may be available in order to meet requirements.

(f) Comprehensive Program Review. The AT plan will be reviewed annually to ensure the accuracy of content against updated references and inspection checklists. Additionally, an assessment of new threats will be conducted to identify potential threats not identified in the previous AHTA.

c. Tasks. This is not all-inclusive; all staff should be prepared to conduct other tasks, as directed.

(1) Adjutant (S-1)

(a) Serve as a member of Crisis Management Team (CMT) and AT Working Group (ATWG).

(b) Coordinate suspicious package/improvised explosive device (IED) training for mail clerks.

(c) Maintain key personnel rosters for notifying/recalling essential personnel with in preparing and/or supervising those actions indicated for the appropriate FPCON measures.

(2) Intelligence Officer (S-2)

(a) Provide intelligence support as required.

(b) Provide guidance for maintaining classified and unclassified material to support this plan.

(c) Serve as a member of the CMT and the ATWG.

(d) Develop a comprehensive foreign travel check to ensure personnel executing leave, or official travel outside the continental United States (OCONUS) complete all foreign travel requirements prior to departure. Ensure personnel executing leave OCONUS receive area of travel country specific threat information brief. The threat brief will include the following information:

- Department of State travel advisories.
- United States embassy locations.
- Time conversion.
- Customs regulations.
- Health precautions.
- Currency information.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

- Clothing recommendations.
- Transient accommodations.
- Travel precautions and information.

(3) Operations Officer (S-3)

- (a) Serve as a member of the CMT and as the chairperson of the ATWG.
- (b) When the Commanding Officer activates the CMT, ensure all members are notified and briefed on the situation.
- (c) In cooperation with the ATO, coordinate, document, and ensure completion of Level I Antiterrorism Awareness training for all personnel, to include civilians who may be attached to the unit.
- (d) Provide operational security (OPSEC) training to 11th Marines in accordance with applicable orders and directives.
- (e) In cooperation with the ATO, coordinate and ensure semi-annual training on emergency procedures for Emergency Lockdown and Shelter in Place, enclosures (8) and (9) respectively.
- (f) Ensure the development and dissemination of unit OPSEC programs and policies.
- (g) Establish reporting procedures for OPSEC violations

(4) Antiterrorism Officer

- (a) Complete (at a minimum), ATO Level II training appointed in writing.
- (b) Develop and manage a comprehensive site specific AT plan.
- (c) Conduct annual review of AT plan; conduct ATWG meetings quarterly, attend HHQ ATWG.
- (d) Update the AT plan as required to maintain compliance with applicable orders/directives.
- (e) Compile a prioritized list of mission essential assets.
- (f) Identify all critical assets and potential vulnerabilities.
- (g) Assess incident response capabilities and establish risk priorities.
- (h) Develop site-specific FPCON measures, random antiterrorism measures (RAM), and AT courses of action.
- (i) Maintain/supervise execution of the unit action set matrix in accordance with enclosure (3).
- (j) Identify, compile, and submit antiterrorism resource requirement projects and unfunded requirements, as required.
- (k) Coordinate individual and organizational antiterrorism training requirements and annual site antiterrorism exercises.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

(l) Report statistics of annual antiterrorism training requirements, and exercises as required.

(m) Maintain a turnover/desktop procedures binder.

(n) Ensure the execution of monthly RAMs and report completion of monthly RAMs to 1st Marine Division, as required.

(o) In accordance with reference (a), complete special event vulnerability assessments for any event open to the public in which more than 300 personnel will be in attendance.

(5) Logistics Officer (S-4)

(a) Identify equipment or resource shortfalls and submit requests for support as required.

(b) During an AT emergency, monitor all unit assets assigned to an AT emergency (as well as other potential assets) as required.

(c) Coordinate the requisition, receipt, movement, safeguarding, and issue of weapons and ammunition, as required.

(d) Be prepared to open/extend the hours of operations of the unit armory as needed.

(e) Provide logistics support as needed.

(f) Serve as a member of the CMT and the ATWG.

(g) As required coordinate emergency maintenance to:

1. Remove debris/refuse.

2. Repair/restore roads systems, drainage systems, sewage treatment and collection facilities, and water distribution systems.

3. Cut off or restore water, steam, and electrical power, natural gas, and ventilation systems as required during emergencies.

4. Coordinate material handling equipment.

(h) Compile and submit damage assessment reports as required.

(i) Contain or clean-up hazardous materials (HAZMAT), and coordinate support from MCIWEST MCB CAMPEN when incidents range beyond the unit's capabilities.

(j) Develop and maintain a temporary or moveable barrier plan consistent with specific FPCON measures in accordance with enclosures (3) and (4).

(k) Review the barrier plan and be prepared to assist in employment of the barrier plan if required.

(l) Coordinate 24-hour maintenance capabilities during emergencies.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

(m) Periodically inspect facilities for damage that would render them unsafe during an emergency, and make recommendations for repairs that would mitigate damage from terrorism.

(6) Supply Officer

(a) Ensure AT funding requirements have been identified, prioritized and is included in the unit budgeting process.

(b) Identify, with assistance from the ATO, where the lack of AT funding may have adverse impacts on the unit AT plan.

(c) Identify and implement procedures to capture AT related expenses during normal operations, exercises, and actual incidents.

(d) Establish procedures for emergency purchasing.

(e) Serve as a member of the CMT and the ATWG.

(7) Safety Officer

(a) Implement programs to address health and safety in support of this plan.

(b) Provide training assistance for the implementation of this plan.

(c) Monitor compliance with federal and state health and safety regulations.

(d) Ensure safety reports and inquiries are conducted as required.

(e) Serve as a member of the ATWG.

(8) Chaplain

(a) Provide counseling to victims, families of victims, and other service members as necessary.

(b) Coordinate with local churches, religious groups, and military chaplains for additional services, as required.

(c) Provide ministries as required.

(9) Medical Officer

(a) Establish procedures for treatment and evacuation of casualties. Upon notification of a mass casualty, be prepared to deploy medical assets to help triage, treat, and evacuate casualties as necessary.

(b) Provide support at evacuation shelters as directed.

(c) Initiate notifications to personnel who augment the medical program, when required, and be capable of warning other agencies when assistance may be required.

(d) Establish triage procedures for treating personnel who are exposed to chemical, biological, or

radiological contaminants.

(e) Provide inoculations and prophylactics as required.

(10) Communication Officer (S-6)

(a) Be prepared to provide communications support to AT efforts.

(11) OIC's

(a) Be prepared to serve as an Area Commander. Coordinate requirements outlined in this plan with the Commanding Officer.

(b) Create a level of awareness, appreciation, and readiness commensurate with the threat.

(c) Be prepared to support FPCON levels.

(d) On order, implement internal security procedures, orders, and SOP's that appropriately supplement the Regiment's AT/FP plan.

(e) Ensure all personnel within your battery complete AFTP Level I training annually and submit rosters to the ATO.

(f) Designate an officer/SNCO to serve on the AT/FPWG as required.

(g) Be prepared to provide personnel and other resources as required.

(h) Upon designation of FPCON level Charlie, be prepared to provide an AT/FP mission-capable, platoon-sized unit and three armed security squads as a reserve force.

(i) Implement RAMS as directed.

d. Coordinating Instructions

(1) Action Set Matrix. The Action Set Matrix is a set of clearly defined actions and coordination required to execute effective FPCON measures. All personnel must be prepared to execute the actions as outlined in enclosure (3).

(a) The 43 Area Guard Force Augmentation plan, reference (j), outlines requirements for 11th Marines and subordinate units to provide Marines to augment the guard force during heightened FPCON measures or credible threat periods as directed by the Commander.

(b) 43 Area tenant units will be prepared to provide additional and long standing guard force augmentation for prolonged heightened security periods when directed by the Commander or installation AFTP posture.

(2) Sections and Buildings. The S-4 facility manager maintains the overall responsibility for buildings within the Regiment area of operation. Section heads are responsible for each section and enforcement of posted access rosters.

(3) Lighting. The facilities manager will inspect the lighting quarterly and provide findings to the

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

appropriate command representative.

(4) Fencing/Barriers. The facilities manager will inspect the barriers/fencing and provide findings to the appropriate command representative.

(5) Operations Security. In accordance with reference (d), all command website information will be submitted to and screened by the website manager.

(6) Counter-Surveillance/Detection. All unit personnel will familiarize themselves with the "Eagle Eyes" Program. The website is located at: <https://usmceagleeyes.org>. All hands will report any suspicious activity using the "Eagle Eyes" phone number which is 910-451-3333.

(7) Alert Notification Procedures. The S-1 will maintain key personnel rosters for the purpose of notifying or recalling essential personnel with responsibilities in preparing and/or supervising those actions indicated for the appropriate FPCON measures. All available mass notification tools will be utilized to notify all personnel aboard the MCB CAMPEN of elevated FPCONs or emergency situations.

(8) Access Controls. PMO is responsible for pedestrian, vehicular, commercial, and package/mail access onto MCB CAMPEN. Access to each section area is the responsibility of the using entity. Access rosters will be posted and enforced. Within 43 Area, there are access rosters posted on all hatches that have an office behind it. Those that are not on the access roster will not be granted access.

(9) On-Site Security Elements. Military police assigned to MCIWEST-MCB CAMPEN provide routine security within 11th Marines area of operations. If an incident occurs, military police are the initial response force.

(10) Training

(a) All personnel are required to complete AT Level I training annually. The AT Level I training can be completed via a lecture briefing or web based training. Resources may be accessed using the following websites:

1. <https://www.marinenet.usmc.mil/MarineNet/Home.aspx>

2. <https://atlevel1.dtic.mil/at/>

(b) The operations officer is responsible for tracking all training statistics pertaining to AT Level I training, and reporting training statistics to higher headquarters as required by references (a) through (d).

(11) Installation AT Exercises. In accordance with reference (d), annual exercises will be conducted for testing and validation of this AT plan. The plan addresses the raising and lowering FPCONs LAW higher headquarters. The focus of each exercise should be to test an aspect of the unit's ability to operate at a heightened FPCON or to react to a likely incident. Additionally, the Regiment will execute different portions of this plan during the annual exercise to include reporting requirements to higher headquarters. Details outlining participation will be published via separate correspondence. After action reviews will be maintained in the AT turnover binder for a minimum of two years.

(12) Random Antiterrorism Measures (RAM)

(a) The RAM program provides the Commanding Officer flexibility to authorize the elevation of FPCONs to alter the external appearance of the security posture or to implement higher FPCONs measures to mitigate a specific threat not warranting the full implementation of a higher FPCON.

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

However, the Commanding Officer cannot lower a higher headquarters FPCON without written concurrence. The declaration, reduction, and cancellation of FPCONs remain the responsibility of the commander issuing the order. All personnel are directed to adhere to these measures when implemented; enclosure (5) provides coordinating guidance.

(b) The 11th Marines RAM program will be conducted in accordance with the monthly installation RAM guidance in order to reduce installation vulnerabilities to terrorists and criminal activities. The 11th Marines ATO will be the issuing authority for monthly RAMs tasking to 43 Area tenant units.

(c) RAM are a set of protective measures in addition to those in effect through current FPCON levels, and implemented to prevent patterns of security to be observed by hostile forces.

(d) Tenant units, via their Officer of the Day and Staff Non-Commissioned Officer duty standers will be the primary coordinators for RAMs execution within their respective units. Duty standers must verify scheduled RAMs over a 24 to 48 hour period to ensure proper execution including: coordination; manpower sourcing as necessary; timely execution; and logging the conduct of RAMs within the unit's official chronological duty log book and the 43 Area Guard's RAMs log book.

(e) In the event the Regiment or subordinate element is unable to conduct RAMs in accordance with higher headquarters and installation guidance, a supplemental RAM will be conducted and documented within the same month. As well as a MFR to the Regimental ATFP.

(13) Emergency Lockdown Procedures. The guidance procedures are contained in enclosure (8).

(14) Shelter in Place. The guidance for shelter in place procedures is contained in enclosure (9).

(15) Bomb Threat, Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Defense, and Weapons of Mass Destruction (WMD).

(a) The guidance for receiving a bomb threat is covered in reference (i).

(b) CBRN/WMD. All CBRN/WMD detection, response, coordination and sustainment assets will be provided by MCIWEST-MCB CAMPEN and the installation Emergency Manager.

(16) Mass Casualty Plan. Reference (f) contains guidance for responding to a mass casualty event, as MCIWEST-MCB CAMPEN will assume command and control of an event involving mass casualties.

(17) Destructive Weather and/or Natural Disasters. The guidance for destructive weather and/or natural disasters is contained in reference (f) and AreaO 3140.1C 43 Area Flood Plan.

(18) HAZMAT Response Plan. In accordance with reference (f), all HAZMAT response, coordination and sustainment assets will be provided by MCIWEST-MCB CAMPEN.

(19) AT Measures for High Risk Personnel. Currently, there are no high risk personnel assigned to 11th Marines.

(20) AT Construction and Building Considerations. The guidance for construction and building considerations is contained in reference (f).

(21) AT Measures for Logistics and other Contracting. The guidance for logistics and other

contracting is contained in reference (f).

(22) Special Events. The unit ATO is required to conduct special event vulnerability assessments for any off-site event during which 300 or more personnel are expected to be in attendance. Such as Marine Corps Birthday Ball, Mess Nights, etc.

(23) AT Working Group. The AT WG will consist of the following personnel billets or a representative from their shop:

- Executive Officer
- Operations Officer
- Antiterrorism Officer
- OIC's
- Adjutant
- Intelligence Officer
- Logistics Officer
- Supply Officer
- Safety Officer

5. Administration and Logistics

a. Administration

(1) This order contains revisions. Summary of revisions: added training requirements for emergency procedures as coordinated by the S-3 Officer; added 43 Area Guard Augmentation plan, reference (j) including tenant unit responsibilities; and added RAMs reporting requirements to the Random Antiterrorism Measures instructions.

(2) For any considerations not covered in this plan refer to reference (f). This plan will be reviewed annually or as directed by higher headquarters to assess new threats not covered in this plan. All documentation pertaining to AT will be maintained in the AT officer's turnover binder.

(3) The AT officer may update the enclosures of this order as necessary to maintain their relevance. The operations officer is granted By Direction authority to certify any revisions to the enclosures. A summary of revisions will be published to the command.

b. Logistics. The logistics officer will receive and coordinate all internal and external logistical support requirements.

6. Command and Signal

a. Command

(1) The normal chain of command and existing command relationships remain in effect during any training exercises or real-world terrorist incidents that occur.

(2) The 43 Area Guard Force is responsible for the day-to-day force protection activities and reports to the commanding officer.

(3) Area Guard Command Post Location: Bldg. 43526/Phone (760)725-4420

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

(4) Succession of Command: 1, Executive Officer, 2, Operations Officer.

b. Signal

(1) This plan is effective on the date signed.

(2) The following means will be used to effect rapid mass dissemination of information and maintain communications with higher headquarters, adjacent, supporting, attached, and detached units, base PMO, and civilian authorities:

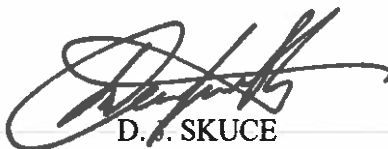
(a) Phone (FPCON Normal through Delta)

(b) Radio (FPCON Alpha through Delta)

(c) E-mail (FPCON Normal through Bravo)

(d) Command, Control, Communication, Computer and Intelligence (C4I) Suite

(3) In the event an actual emergency occurs after normal working hours, the OOD will contact PMO/911 to report the incident to military and civilian authorities and utilize the recall roster to contact essential personnel and responders.



D. J. SKUCE

Copy to:
Distribution List A

**Enclosure (1): (Terrorism Threat Assessment) to 11th Marines Antiterrorism
(AT) Plan 2020**

1. The Terrorism Threat Assessment is marked "Secret" therefore, it is maintained separately from this Plan due to its sensitivity.
2. To request a copy of the Terrorism Threat Assessment, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

**Enclosure (2): (MCI-West Camp Pendleton All Hazard Threat Assessment)
to 11th Marines Antiterrorism (AT) Plan 2020**

1. Although the MCI-West Camp Pendleton All Hazard Threat Assessment is marked "For Official Use Only," it is maintained separately from this Plan due to its sensitivity.
2. To request a copy of the All Hazard Threat Assessment, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

**Enclosure (3): (11th Marines FPCON Action Set Matrix) to 11th Marines
Antiterrorism (AT) Plan 2020**

1. Although the 11th Marines FPCON Action Set Matrix is marked "For Official Use Only," it is maintained separately from this Plan due to its sensitivity.
2. To request a copy of the FPCON Action Set Matrix, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

**Enclosure (4): (11th Marine Barrier Plan) to 11th Marines Antiterrorism
(AT) Plan 2020**

1. Although the 11th Marines Barrier Plan is marked "For Official Use Only," it is maintained separately from this Plan due to its sensitivity.
2. To request a copy of the Barrier Plan, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

Enclosure (4)

FOR OFFICIAL USE ONLY

Enclosure (5): (11th Marines Random Antiterrorism Measures (RAM) Program) to 11th Marines Antiterrorism (AT) Plan 2020

1. The 11th Marines Random Antiterrorism Measures (RAM) Program is marked "For Official Use Only" and is updated monthly. Therefore, the current version is maintained separately from this Plan due to its sensitivity and update requirement.
2. To request a current copy of the RAM Program, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

Enclosure (5)

FOR OFFICIAL USE ONLY

43 AREA RANDOM ANTITERRORISM MATRIX													
MON 20XX		11MAR REG CDO		1/11		2/11		5/11		MAINT BN		AREA GUARD	
		RAM	TIME	RAM	TIME	RAM	TIME	RAM	TIME	RAM	TIME	RAM	TIME
1	WEDNESDAY												
2	THURSDAY											8	
3	FRIDAY												
4	SATURDAY												
5	SUNDAY												
6	MONDAY												
7	TUESDAY												
8	WEDNESDAY											8	Unit Des
9	THURSDAY	8	Unit Des										
10	FRIDAY					4	Unit Des					1	1700-2000
11	SATURDAY	1	Unit Des	1	Unit Des	1	Unit Des	1	Unit Des	1	Unit Des		
12	SUNDAY												
13	MONDAY			4	Unit Des	8	Unit Des						
14	TUESDAY									8	Unit Des		
15	WEDNESDAY											7	Unit Des
16	THURSDAY	2&12	0700-1000	2&12	0700-1000	2&12	0700-1000	2&12	0700-1000	5	0700-1000	20	0700-1000
17	FRIDAY												
18	SATURDAY			1	Unit Des			1	Unit Des			1	0800-1100
19	SUNDAY												
20	MONDAY												
21	TUESDAY											8	Unit Des
22	WEDNESDAY			8	Unit Des								
23	THURSDAY												
24	FRIDAY									4	Unit Des	1	1700-2000
25	SATURDAY			1	Unit Des								
26	SUNDAY	1	Unit Des			1	Unit Des	1	Unit Des	1	Unit Des		
27	MONDAY	4	Unit Des										
28	TUESDAY					3	Unit Des					8	Unit Des
29	WEDNESDAY							8	Unit Des				
30	THURSDAY												

Enclosure (5)

FOR OFFICIAL USE ONLY

RAM	Actions Required
1	Conduct "button-up" of your facility/facilities. Reduce access/egress to one controlled entrance.
2	Conduct 100% identification checks of all personnel entering your facility and log them into a logbook if required; require an escort to remain with all visitors during their visit.
3	Post entry controller(s) to conduct spot check of personnel entering the facility.
4	Lock down your facility and conduct 100% identification check of all personnel.
5	Conduct security checks/inspections of all assigned government vehicles and ensure doors are locked when not in use. Do random checks on all other vehicles in your assigned area of responsibility.
6	Conduct security checks/inspections of all parking lots in the vicinity of your facility looking for suspicious vehicles, personnel, packages or items
7	Detail a person to conduct a check of trash receptacles/storage containers outside of your facility for suspicious packages, items or people.
8	Detail a person to conduct a walk-around of your facility ensuring exterior entries not in use are secured and have not been tampered with (i.e., windows, doors, storage rooms, HVAC vents). Look for suspicious packages, items or people.
9	Test facility intercom/mass notification systems.
10	Conduct exercise bomb threat evacuation of your facility in accordance with local directives. Alternate using primary, alternate, and tertiary rally point. (NOTE: Ensure coordination is established with PMO and installation Force protection Branch prior to exercise.)
11	Conduct and maintain a separate after action report (AAR) file on unit telephone notification/recall of all assigned personnel.
12	Conduct a 100% inspection of baggage, purses, suitcases, packages, briefcases and parcels entering and leaving the building, facility, or warehouse.
13	Check on base utility and communication systems and critical CE facilities. Inspect locks and securing methods for evidence of tampering.
14	Ensure all critical systems/assets (power, water, natural gas, communications, military fuel farm, etc.) have back-up capability during emergency situations.
15	Conduct a walking patrol through high occupancy facilities (i.e. barracks, bowling center, Base Exchange, Commissary, etc.). (PMO, CDO, SDO, OOD,DNCO ONLY)
16	Conduct a MWD explosive/narcotic walking patrol through high occupancy facilities (i.e. barracks, billeting, bowling center, Base Exchange, Commissary, Other MCCA facilities, etc.) (PMO/MWD/CID ONLY)
17	Conduct a MWD security check/inspection of vehicles entering the installation. (PMO/MWD/CID ONLY)
18	Conduct MWD security checks/inspections of vehicles exiting the installation. (PMO/MWD/CID ONLY)
19	Conduct 100% HANDS ON ID checks of all personnel in vehicles entering the installation. (PMO ONLY)
20	Conduct 100% HANDS ON ID checks of all personnel in vehicles exiting the installation. (PMO ONLY)
21	Conduct 100% ID check of all personnel entering installation via MBTA public transportation bus. (PMO ONLY)
22	Require vehicle operators/owners to provide vehicle registration and/or proof of insurance upon entering the installation. (PMO ONLY)
23	Randomly select vehicles entering installation and conduct a hands-on inspection of the vehicles license plates; check license plate number against registration and ensure it is properly affixed. (PMO ONLY)
24	Remind drivers as they enter the installation to lock their vehicles and to check their vehicle before entering and

Enclosure (5)

	driving the vehicle. (PMO ONLY)
25	Conduct perimeter patrols of the installation on accessible roads covering Mainside, Camp Wilson, EAF and Housing areas and/or coordinate with Bearmat to patrol Range Training Areas (RTA) without the interruption of training. (PMO/SRT ONLY)
26	Conduct walk through of large parking areas (base exchange, commissary, MCCC parking areas, Golf Course, etc.) with explosive/narcotics MWD team. (PMO/WMD/CID ONLY)
27	Conduct check of key facilities and soft targets (i.e. daycare facilities, Youth & Teen center, Officer/Enlisted Clubs, theater, etc.), and areas where large groups of personnel congregate with explosive/narcotic MWD team. (PMO/MWD/CID ONLY)
28	Conduct periodic walk-through of the mail rooms by explosive/narcotic MWD teams. (PMO/MWD/CID ONLY)
29	Conduct walking patrols and/or surveillance in selected Military Family Housing areas.(PMO/MWD/CID ONLY)
31	Post MWD at installation entry control points. (PMO/MWD ONLY)
32	Discretely conduct checks of the exterior of senior base official's quarters/offices. Recommend coordination with the occupants of the quarters/office prior to performing. (PMO ONLY)
33	Conduct surveillance (SALUTE Report) at remote locations of Mainside, Camp Wilson, EAF, or selected Military Family Housing areas. (PMO/CID ONLY)
34	Coordinate with Bearmat and perform surveillance via vehicle and walking patrols at remote training areas when training is not being conducted or when training will not be interrupted (i.e. areas adjacent to Rifle Range Road, Sand Hill and RTAMS, etc.) focusing on unimproved roads that provide access from the civilian community. (PMO/SRT ONLY)
35	Based upon the current barrier plan at exposed billeting locations, perform frequent (hourly) and aggressive vehicle and/or walking patrols to identify and report suspicious vehicles or people. Unit OOD, DNCO or ADNCO will document this RAM in their duty log book. (PMO/CDO/OOD/DNCO/ADNCO only)
36	Conduct observation and surveillance at key locations utilizing the portable watch tower (Skywatch), (i.e. base boundaries, training areas, housing areas, etc.) Coordinate with Bearmat for use in RTA(PMO/SRT ONLY)
37	Coordinate and utilize the Headquarters Regiment SAF for vehicle inspections or 100% identification of personnel entering the installation. (PMO/MWD/SRT/SAF ONLY)
38	Coordinate and conduct regularly scheduled range sweeps in accordance with the monthly TEEP and report any unauthorized or suspicious person(s) or vehicle(s). (Bearmat/Mercy Air ONLY)
39	Coordinate and test secondary communication methods for notification and evacuation (simulated) of all active Range Training Areas. (G-3/Bearmat/TTECG ONLY)
40	Coordinate utilization of Unmanned Aerial Vehicles (UAV) and conduct range sweeps during monthly scheduled training/testing. Report all unauthorized suspicious person(s) or vehicle(s). (Bearmat/VMU-1/VMU-3 ONLY)
41	Implement and conduct installation entry point evaluation of commercial Vehicles delivering food to/on installation customers. (USA Vet ONLY)
42	Coordinate and utilize the Headquarters Regiment SAF to support perimeter patrolling of identified vulnerable areas. (PMO/SRT/SAF ONLY)
43	Obtain/report all COCOM-related or Marine Corps Title 10 Mission Essential Tasks (METs) and/or core functions your organization supports.
44	At regular intervals, remind all personnel, including family members, to report the following to PMO or to the Eagle Eye Program ---- (1 Suspicious personnel, particularly those carrying suitcases or other containers, (2 Those observing, photographing, or asking questions about military operations or security measures, (3 Unidentified vehicles parked or operated in a suspicious manner on, or in the vicinity of installation, units, or facilities, (4 Abandoned parcels or suitcases, (5 Any other activity considered suspicious.
PMO ONLY	Based upon statistics and analysis, perform a DUI/DWI check point, random vehicle inspections with MWD or other appropriate (high visibility) security measures or RAM at installation entry control points. Utilize and submit separate correspondence, Law Enforcement Sensitive (FOUO) to the Commanding General or his designated representative for approval and execution of these actions. (PMO/MWD/CID ONLY)

Enclosure (5)

FOR OFFICIAL USE ONLY

Enclosure (6): (11th Marines Risk Management Methodology) to 11th Marines Antiterrorism (AT) Plan 2020

1. Risk Management (RM) Worksheet. The RM Worksheet can be used in conjunction with Chapter 3, NAVMC 3500.103, to understand the antiterrorism (AT) risk management process. It is a useful guide through each step of the risk management process; however, it may not provide as effective analysis as more advanced risk management tools. The RM Worksheet is referenced as Enclosure (1) to this guide.

a. Criticality Assessment Component (Step 1)

(1) The first component of conducting a risk assessment is to conduct a criticality assessment that identifies assets and mission impact or consequence of loss of assets that support execution of the command's mission. 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) The RM Worksheet provides the following guidance to determine the overall Criticality Rating for each asset.

(a) High — Indicates that compromise to the targeted asset would have grave consequences leading to mass casualty or mission failure; or indicates that a compromise to assets would have serious consequences resulting in loss of life or severe mission degradation

(b) Medium — Indicates that a compromise to the assets would have moderate consequences resulting in potential loss of life or severe injury and loss of mission essential resources that would impair operations for a limited period of time

(c) Low — Indicates little or no impact on human life or the continuation of operations

(3) Basic instructions to complete Criticality Assessment Component (Step 1) of the RM Worksheet are attached as Enclosure (2) to this guide.

b. Threat Assessment Component (Step 2)

(1) Execution of the 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 (AHTA) 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. Mission Assurance Programs subject to a Marine Corps Mission Assurance Assessment are typically responsible for the maintenance of the local AHTA.

(a) Threat and Hazard Definitions

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

2. 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) In an operational environment where the AHTA is not available, the G-2, S-2, Regional Security Officer, and other intelligence sources are options to identify potential threats, hazards, and weapons and tactics and will aid in determining likelihood or probability of occurrence of each.

(3) The RM Worksheet provides the following guidance to determine the overall Threat Rating for each asset assessed.

Enclosure (6)

FOR OFFICIAL USE ONLY

(a) High — Indicates that a credible threat exists against the assets based on our knowledge of the adversary's capability and intent to attack the assets, and based on related incidents having taken place at similar facilities; natural hazard occurs frequently

(b) Medium — Indicates that there is a potential threat to the assets based on the adversary's desire to compromise the assets, and the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents. Indicates there is a significant capability with low or no current intent that may change under specified conditions; natural hazard - occurs annually.

(c) Low — Indicates little or no credible evidence of capability or intent, with no history of actual or planned threats against the assets. Source of Threat Information; natural hazard - rarely to never occur.

(4) Basic instructions to complete Threat Assessment Component (Step 2) of the RM Worksheet are attached as Enclosure (3) to this guide.

c. Vulnerability Assessment Component (Step 3)

(1) A Vulnerability Assessment is a systematic examination of the characteristics of an asset, application, or its dependencies to identify vulnerabilities that could be susceptible to the effects of any number of threats or hazards (including weapons and tactics in an operational environment). Vulnerability assessments must be conducted by team of subject matter experts with backgrounds in different functional areas such as Physical Security, Antiterrorism, Infrastructure and Emergency Management and Plans. Vulnerabilities are defined as a weakness or susceptibility of a 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.

(2) 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. Efforts to complete Risk Mitigation and Countermeasure Strategies (Steps 6 & 7) should be made during the Vulnerability Assessment phase.

(3) The RM Worksheet provides the following guidance to determine the overall Vulnerability Rating for each asset.

(a) High — Indicates that there are no countermeasures, or existing countermeasures are ineffective or easily defeated by an adversary or natural hazard.

(b) Medium — Indicates that there are countermeasures in place, but at least one weakness exists that some known adversaries or natural hazards would be capable of exploiting.

(c) Low — Indicates that multiple layers of effective countermeasures exist and few or no known adversaries or natural hazards would be capable of exploiting the vulnerability.

(4) Basic instructions to complete Vulnerability Assessment Component (Step 3) of the RM Worksheet are attached as Enclosure (4) to this guide.

d. AT Program Effectiveness Component (Step 4)

(1) AT Program Effectiveness should not only include defense in depth effectiveness (barrier plan, RAM program, risk assessment, etc.), but should include assessing security response and protection measure priorities that should be identified for locations housing assets, including those assets owned by tenant commands, within the overall security response priority planning.

Enclosure (6)

(2) The RM Worksheet provides the following guidance to determine the overall AT Program Effectiveness.

(a) High — Effective AT Program in place; minimal vulnerabilities or concerns identified in most recent Vulnerability Assessment; no significant gaps in the security posture; AT Plan is current and has been exercised; robust RAM Program; Defense in Depth effectively employed; incident response measures have been fully developed, resourced, and exercised.

(b) Medium — AT Program in place; some vulnerabilities or concerns identified in most recent Vulnerability Assessment; no significant gaps in the security posture; AT Plan is valid but not current or has not been exercised; RAM Program exists; some Defense in Depth employed; incident response measures have been developed, resourced, and exercised.

(c) Low — Ineffective AT Program in place; major vulnerabilities were identified in most recent Vulnerability Assessment; no or ineffective RAM Program; no Defense in Depth; incident response measures not developed, resourced, or exercised.

(3) Basic instructions to complete AT Program Effectiveness Component (Step 4) of the RM Worksheet are attached as Enclosure (5) to this guide.

e. Risk Analysis Component (Step 5)

(1) 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 (including weapons and tactics in an operational environment), 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 or overall risk rating is produced. Risk is determined by the following equation: $\text{Criticality Rating} \times \text{Threat/Hazard Rating} \times \text{Vulnerability Rating} = \text{Risk Rating}$. A risk rating is produced for each specific threat/hazard – vulnerability – asset pairing of data. The RM Worksheet considers AT Program Effectiveness in the equation.

(2) The RM Worksheet provides the following guidance to determine the overall Risk Rating for each asset.

(a) The Overall Risk Rating is based on the four elements above. Enter a rating of High (H) - Medium (M) - Low (L) for the Overall Risk Rating. If the Overall Risk Rating is noticeably different than the threat, vulnerability, asset criticality, and AT/FP plan effectiveness, explain the reason for the difference in the justification section above.

(b) For example if Threat = High, Vulnerability = High, Criticality = Medium, and AT/FP Plan Effectiveness = Low, and the Overall Risk Rating = Low, the Overall Risk Rating does not reflect the ratings of the individual components, and therefore must be explained.

(3) Basic instructions to complete Risk Analysis Component (Step 5) of the RM Worksheet are attached as Enclosure (6) to this guide.

f. Risk Mitigation and Countermeasure Strategy Components (Steps 6 & 7). Remediation is defined as actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. Remediation involves identifying countermeasures that can be implemented before undesirable events or attacks occur that could exploit the identified vulnerabilities. ATOs will prioritize their remediation efforts on those assets with highest impact to supported missions if those assets were lost; address the threats and hazards (including weapons and tactics in an operational environment) that have the highest rated probability of occurrence; and address the most significant asset vulnerabilities identified that could be exploited by the most likely threats or hazards (including weapons and tactics in an operational environment). The Residual Risk portion of the step should be completed following completion of Overall Risk Rating (Step 5). Basic instructions to complete Risk Mitigation and Countermeasure Strategy Components (Steps 6 & 7) of the RM Worksheet are attached as Enclosure (7) and Enclosure (8) to this guide.

Enclosure (6)

The following enclosures used in the RM Worksheet are found on the Antiterrorism SharePoint located at:
<https://eis.usmc.mil/sites/hqmcppo/PS/PSM/AT/SitePages/Home.aspx>

Enclosures:

- (1) RM Worksheet (blank)
- (2) Basic instructions to complete Criticality Assessment Component (Step 1) of the RM Worksheet
- (3) Basic instructions to complete Threat Assessment Component (Step 2) of the RM Worksheet
- (4) Basic instructions to complete Vulnerability Assessment Component (Step 3) of the RM Worksheet
- (5) Basic instructions to complete AT Program Effectiveness Component (Step 4) of the RM Worksheet
- (6) Basic instructions to complete Risk Analysis Component (Step 5) of the RM Worksheet
- (7) Basic instructions to complete Risk Mitigation Component (Step 6) of the RM Worksheet
- (8) Basic instructions to complete Countermeasure Strategy Component (Step 7) of the RM Worksheet

Enclosure (6)

FOR OFFICIAL USE ONLY

**Enclosure (7): (11th Marines Asset List) to 11th Marines Antiterrorism (AT)
Plan 2020**

1. Although the 11th Marines Asset List is marked "For Official Use Only," it is maintained separately from this Plan due to its sensitivity.
2. To request a copy of the 11th Marines Asset List, please contact the Anti-Terrorism Officer, 11th Marines, at 760-725-4420.

Enclosure (7)

FOR OFFICIAL USE ONLY

Enclosure (8): EMERGENCY LOCKDOWN PROCEDURES FOR BUILDINGS

When an Active Shooter event takes place or an announcement is made via the "Giant Voice" or Mass Telephone Notification System to initiate a local EMERGENCY LOCKDOWN, execute the following:

IF PERSONNEL ARE CAUGHT OUTSIDE. Leave the area, or building in the opposite direction of the known threat if possible. If shots are being fired, attempt to run in a zigzag type pattern, instead of running in a straight line. Assemble at a designated building or assembly area for accountability.

"HOW TO" EXECUTE EMERGENCY LOCKDOWN PROCEDURES:

- If unable to leave your location, proceed to an area that can be secured, e.g., classroom or closet.
- Get inside and lock the doors and windows, pull the shades or curtains and turn the lights off.
- Cover the door window panes with a cardboard insert or other material to block a visual inside the room
- Have the group inside the room huddle at the "blind-side" section of the room, furthest away from the door, hidden from sight.
- If possible, call 911, quietly and report the building/room number and as many details as possible:
 - Location of the shooter/attacker
 - Number and physical description of shooters/attackers
 - Number and type of weapons held by the shooter/attackers
 - Number of victims/casualties at your location
- **DO NOT PULL THE FIRE ALARM!** Attackers have done this maneuver in the past to get students outside or cause additional chaos. In various schools or businesses this can trigger the sprinkler systems, again causing more stress.
- If possible, report the building/room number, names or numbers and condition of personnel within your room/space to the 911 operator. Text message as the primary means if possible. Talk quietly and quickly via cell phone when possible. **DO NOT LET THE ATTACKERS HEAR YOUR VOICES!**
- Should the fire alarm sound, do **NOT** evacuate the building unless directed to do so by security forces.
- If it is not possible to lock the doors, barricade them with furniture or other office equipment in front of the door to act as a barricade to the attackers. Some doors open into the hallway. In this situation, find another room quickly or use what is available to restrict the entry of an attacker, e.g., wedge the door, or place as many large, heavy items in front of the door as possible.
- Cover any glass window openings in the door if possible. Close all blinds and drapes for concealment from any outside observation.
- Turn off the lights in the room. Place cell phones on vibrate only! Utilize message texting as the primary means of communicating with outside agencies, if possible!
- Attempt to take the shooter/attacker down **ONLY AS A LAST RESORT!** If necessary:
 - Devise a plan of attack, and work as a team
 - Do whatever is necessary to keep yourself safe and neutralize the threat!
 - Concentrate on surprise, speed and focus of effort in stopping the attacker(s).
- Remain under lockdown until otherwise directed by security force personnel, or recognized supervisors.

WHEN SECURITY FORCES ARRIVE

- Remain calm and follow the security forces instructions –security does not know if you are the attacker.
- Put down any items e.g., bags, jackets, cell phones, etc. and keep your **hands in plain sight**.
- Keep your hands open and in plain sight at all times.
- Do exactly what the police/security forces tell you to do. Do **NOT ATTEMPT** to assist security force!

AFTER CRISIS ACTIONS

- **Do not leave the area** – ALL personnel will be accounted for and will be asked to provide verbal and/or written statements pertaining to the incident.
- After the lockdown order has been lifted, managers, faculty and staff should attempt to restore order and comfort/assist as quickly as possible.

Commanders, directors and section heads should be accountable for personnel and report personnel status to the command S-1, or designated department as soon as possible.

Enclosure (9): BOMB THREAT & SHELTER IN PLACE PLAN

What Shelter-in-Place Means:

First Responders on the scene are the best source of information. Following their instructions during and after emergencies regarding sheltering, food, water, and clean-up methods is your safest choice. One of the instructions you may be given in an emergency where hazardous materials have been released into the atmosphere is to **shelter-in-place**. This is a precaution aimed to keep you safe while remaining indoors. (This is not the same procedure as going to a shelter in case of a storm). Shelter-in-place means selecting a small, interior room, with no or few windows, and taking refuge there. It does not mean sealing off your entire home or office building. If you are told to shelter-in-place, follow the instructions provided below.

Why You Might Need to Shelter-in-Place:

Chemical, biological, or radiological contaminants may be released accidentally or intentionally into the environment. Should this occur, information will be provided by local authorities on television and radio stations on how to protect you and your family. This information will most likely be provided on television and radio, it is important to keep a TV or radio on, even during the workday. The important thing is for you to follow instructions of local authorities and know what to do if they advise you to shelter-in-place.

How to Shelter-in-Place

At Work:

- Close your office/building. Bring everyone into a specific room(s). Shut and lock the door(s).
- If there are students, staff members, or visitors in the building, provide for their safety by asking them to stay – **NOT** leave. When the alarm is sounded and the command is directed to shelter-in-place, all personnel are expected to take those steps now, where they are, and not drive or walk outdoors.
- Unless there is an imminent threat, direct all students, staff members, or visitors to call their emergency contact to let them know where they are and that they are safe.
- Turn on call-forwarding or alternative telephone answering systems or services. If the school/staff section has voice mail or an automated attendant, change the recording to indicate that the school/staff section is closed, and that staff and visitors are remaining in the building until authorities advise that it is safe to leave.
- Close and lock all windows, exterior doors, and any other openings to the outside.
- If you are told there is danger of explosion, close the window shades, blinds, or curtains.
- Have employees familiar with your building's mechanical systems turn off all fans, heating and air conditioning systems. Some systems automatically provide for exchange of inside air with outside air – these systems, in particular, need to be turned off, sealed, or disabled.
- Gather essential disaster supplies, such as nonperishable food, bottled water, battery-powered radios, first aid supplies, flashlights, batteries, duct tape, plastic sheeting, and plastic garbage bags.
- Select interior room(s) above the ground floor, with the fewest windows or vents. The room(s) should have adequate space for everyone to be able to sit in. Avoid overcrowding by selecting several rooms if necessary. Large storage closets, utility rooms, pantries, copy and conference rooms without exterior windows will work well. Avoid selecting a room with mechanical equipment like ventilation blowers or pipes, because this equipment may not be able to be sealed from the outdoors.
- It is ideal to have a hard-wired telephone in the room(s) you select. Call emergency contacts and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
- Use duct tape and plastic sheeting (heavier than food wrap) to seal all cracks around the door(s) and any

vents into the room.

- Write down the names of everyone in the room, call the security manager or operations section and report who is in the room with you, and their affiliation with your school/staff section (student, staff member, or visitor).
- Keep listening to the radio, television, Computer Frost Call, or Mass Telephone Notification Message until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk within the command.

In Your Vehicle:

If you are driving a vehicle and hear advice to “shelter-in-place” on the radio, take these steps:

- If you are very close to home, your office, or a public building, go there immediately and go inside. Follow the shelter-in place recommendations for the place you pick described above.
 - If you are unable to get to a home or building quickly and safely, then pull over to the side of the road. Stop your vehicle in the safest place possible. If it is sunny outside, it is preferable to stop under a bridge or in a shady spot, to avoid being overheated.
 - Turn off the engine. Close windows and vents.
 - If possible, seal the heating/air conditioning vents with duct tape.
 - Listen to the radio regularly for updated advice and instructions.
 - Stay where you are until you are told it is safe to get back on the road. Be aware that some roads may be closed or traffic detoured. Follow the directions of law enforcement officials.
- Remember that instructions to shelter-in-place are provided for durations of a few hours, not days or weeks. There is little danger that the room in which you are taking shelter will run out of oxygen and you will suffocate.

At Home:

- Close and lock all windows and exterior doors.
- If you are told there is danger of explosion, close the window shades, blinds, or curtains.
- Turn off all fans, heating and air conditioning systems. Close the fireplace damper.
- Get your family disaster supplies kit <http://www.redcross.org/services/disaster/beprepared/supplies.html>, and make sure the radio is working.
- Go to an interior room without windows that's above ground level. In the case of a chemical threat, an above-ground location is preferable because some chemicals are heavier than air, and may seep into basements even if the windows are closed.
- Bring your pets with you, and be sure to bring additional food and water supplies for them.
- It is ideal to have a hard-wired telephone in the room you select. Call your emergency contact and have the phone available if you need to report a life-threatening condition. Cellular telephone equipment may be overwhelmed or damaged during an emergency.
- Use duct tape and plastic sheeting (heavier than food wrap) to seal all cracks around the door and any vents into the room.
- Keep listening to your radio or television until you are told all is safe or you are told to evacuate. Local officials may call for evacuation in specific areas at greatest risk in your community.

Enclosure (10): (Glossary) to 11th Marines Antiterrorism (AT) Plan 2020

1. Access control. For the purposes of these standards (UFC 04-010-01), any combination of barriers, gates, electronic security equipment, and/or guards that can limit entry or parking of unauthorized personnel or vehicles.
2. All Hazards Threat Assessment (AHTA). The AHTA accomplishes two goals: 1) identification of a comprehensive list of threats and hazards, and 2) identification of the likelihood or probability of occurrence of each threat or hazard. The AHTA is also based on the fusion of information (strategic, operational, and local/tactical) derived from liaisons between civil and military LE; public safety agencies and departments; and meteorological, environmental, public health, and medical syndromic surveillance sources.
3. Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.
4. Antiterrorism Executive Committee (ATEC). An executive level committee that meets at least semi-annually to develop and refine AT program guidance, policy, and standards. The ATEC is briefed by the ATO and makes recommendations to the commander for resource allocations priorities. ATECs are found at both the installation and operational commands culminating at the MARFOR level, e.g. Supporting Establishment: Installation, Regions, MARFOR; Operational Forces: Unit, MSC, MEF, and MARFOR.
5. Antiterrorism SharePoint Portal. Restricted website portal for ATOs that contains current information, tools, and resources.

<https://ehqmc.usmc.mil/org/hqmcppo/PS/PSM/AT/SitePages/Home.aspx>
6. Antiterrorism Officer (ATO). The principal military or civilian advisor charged with managing the AT Program for the commander or DOD civilian exercising equivalent authority.
7. Asset. A distinguishable entity that provides a service or capability to a Marine Corps element. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations.
8. AT Program. The AT program is one of several security-related programs that fall under the overarching Combating Terrorism and Force Protection programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DOD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and plan for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The essential elements of an AT program are risk management, planning, training and exercises, resource application, and a program review.
 - a. Risk Management (RM). RM involves the application of a standardized process to identify, assess, and manage risk and enable decision making that balances risk and cost with mission benefits. RM allows the commander to decide how best to employ allocated resources to reduce risk, or, where

Enclosure (10)

circumstances warrant, acknowledge risk. RM consists of two core activities: risk assessment and risk planning.

(1) Risk Assessment (RA). 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.

(2) Risk Response/Planning. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation.

b. Planning. The process of developing specific guidance and execution-oriented instructions for subordinates.

c. Training and Exercises. The development of individual, leader, and collective skills, and the conduct of comprehensive exercises to validate plans for AT, incident response, terrorism consequence management, and continuity of essential military operations.

d. Resource Application. The process of applying risk management to vulnerabilities, and where the resultant risk is not acceptable after applying mitigation measures, elevate the vulnerability with a resource request using the existing Planning, Programming, Budgeting, and Execution (PPBE) system, the Combatant Commander Initiative Fund (CCIF), the Physical Security Program, and other funding mechanisms. Central to success in resource application is tracking and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

e. Comprehensive Program Review. The systematic assessment of the AT program against the standards prescribed by this Plan.

9. Antiterrorism Working Group (ATWG). A cross-functional, interdisciplinary working group at the installation, operating, or higher headquarter level whose purpose is to oversee the implementation of the AT program, develop and refine AT plans, and address emergent or emergency AT program issues. ATWG membership includes the ATO, the Commander (or a designated representative), key members of the principal staff, to include CBRNE and CIP expertise, subordinate and tenant unit representatives, and other representatives as required to support AT planning and program implementation.

10. C4I Suite. The purpose of the Common Operational Picture (COP) tool, C4I Suite, is to allow the Navy and Marine Corps the interoperability to communicate threat information and to share and report capabilities through the proper chain-of-command.

11. Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Incident. An emergency resulting from the deliberate or unintentional release of nuclear, biological, radiological, or toxic or poisonous chemical materials, or the detonation of a high-yield explosive.

12. Combatant Commander Initiative Fund (CCIF). CCIF is a program established by Congress and managed by the Joint Staff (J-7) that provides funds for individual projects submitted by combatant commands and approved by the Chairman of the Joint Chiefs of Staff. The intent is to support emergent combatant command joint warfighting readiness capabilities and national

Enclosure (10)

security interest. Funding is provided directly to the combatant command upon approval of individual initiatives by the Chairman.

13. Consequence Management. Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, man-made, or terrorist incidents.

14. Criticality Assessment (CA). An assessment of the total impact (failure or severe degradation) on the execution of missions or functions supported by an asset, should that asset be unavailable for any reason. The CA identifies assets whose degradation or destruction impacts the command's ability to execute its assigned mission or functions.

15. Defense In Depth. Physical security systems designed to employ a layered defense to provide graduated levels of protection from the installation boundary to identified assets.

16. Design Basis Threat. The threat (aggressors, tactics, and associated weapons, tools, or explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.

17. Emergency Operations Center (EOC). Pre-determined location that uses a common operating picture and information management system in order to execute and support actions required by the Installation Emergency Management Plan, supports incident command, and facilitates coordination of incident information and consequence management.

18. Force Protection (FP). Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

19. Force Protection Condition (FPCON). A DOD-approved system standardizing DOD's identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates coordination among DOD Components and support for AT activities.

20. Hazards. Non-hostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to critical assets and infrastructure. Probability of hazard occurrence is based on capability and history of occurrence.

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

22. High-Risk Personnel (HRP). Personnel who, by their grade, assignment, symbolic value, or relative isolation are likely to be attractive or accessible terrorist targets.

23. Higher Headquarters Assessment (HHA). An overall assessment by a higher headquarters of how an organization is managing its AT program, to include

Enclosure (10)

management and compliance effort by subordinate organizations.

24. Incident Response Measures. A set of procedures established for response forces to deal with the effects of a terrorist incident.

25. Intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning both conventional and asymmetric threats and adversaries. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

26. Marine Corps Critical Asset Management System-Next Generation (MCCAMS-NG). The primary data management system that supports CIP life cycle activities for the Marine Corps. The system captures data focused on tying core Marine Corps operational and Title 10 capabilities, functions, and missions to the assets and infrastructure "critical" to the execution of those capabilities, functions, and missions.

27. Mission Assurance. A process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD Mission Essential Functions (MEFs) in any operating environment or condition.

28. Mission Assurance Assessment Team (MAAT). Conducts all-hazard risk assessment on prioritized Marine Corps installation infrastructure to include: communications, public works, transportation, electrical power and water supply systems.

29. Mission Essential Tasks. To accommodate constraints on training resources, commanders must identify the tasks most essential to their assigned or anticipated missions, with priority given to their wartime missions. These essential tasks are referred to as mission essential tasks (METs). Commanders select the METs that are inherent in their assigned missions from the Marine Corps Task List (MCTL), and the METs serve as a basis for reporting readiness in the Defense Readiness Reporting System.

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

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

32. Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. Risk = Threat X Criticality X Vulnerability. This formula produces a risk ratio used to prioritize mission critical assets and

Enclosure (10)

supporting infrastructure.

33. Risk Management Worksheet. This Risk Management Worksheet can be used in conjunction with Chapter 3 of NAVMC 3500.103 to understand the AT Risk Management process. It is a useful guide through each step of the process; however, it may not provide as effective analysis as more advanced risk management tools.

34. Special Event. An activity characterized by a large concentration of 300 or more DOD personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

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

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

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

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

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

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

36. Threat Assessment

a. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat.

b. The product of a threat analysis for a particular unit, installation, or activity.

37. Terrorism Threat Level. An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history, trends, and targeting.

38. Threat. An adversary having the intent, capability, and opportunity to cause loss or damage to mission critical assets and infrastructure.

39. Threat Working Group (TWG). Installation and separate facility level and higher group that meets at least semi-annually to develop and refine the threat assessment. TWG membership shall include the ATO; Provost Marshal, local, state, Federal, and host-nation law enforcement agencies and the Intelligence Community.

40. Vulnerability. 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.

41. Vulnerability Assessment. A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. When assessing asset vulnerability, it is important to identify the degree of vulnerability is present.

42. Weapons of Mass Destruction (WMD). Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.



UNITED STATES MARINE CORPS
11TH MARINES
BOX 555503
CAMP PENDLETON, CALIFORNIA 92055-5503

3000
AFP
25 Aug 20

From: Commanding Officer, 11th Marines
To: Distribution List

Subj: 11TH MARINES ANTITERRORISM FORCE PROTECTION PLAN

Ref: (a) DoD Instruction O-2000.16, DoD (Antiterrorism) Standards
(b) DoD Instruction O-2000.16, DoD (Antiterrorism) Force Protection Condition (FPCON)
(c) DoDD 2000.12, DoD Antiterrorism Program
(d) DoDD 2000.12H, DoD Antiterrorism (AT) Handbook
(e) NAVMC 3500.103, Marine Corps Antiterrorism (AT) Manual
(f) MCO 3302.1E, Marine Corps Antiterrorism Program
(g) AreaO 3302.1A, SOP for 43 Area All Hazard Plan
(h) MCO 5530.14A, Marine Corps Physical Security Program Manual
(i) 1st Marine Division AT Plan
(j) 43 Area Guard Force Augmentation Plan

Encl: (1) Terrorism Threat Assessment (S) / (Not Attached)
(2) MCI-West Camp Pendleton All Hazard Threat Assessment (FOUO) / (Not Attached)
(3) 11th Marines FPCON Action Set Matrix (FOUO) / (Not Attached)
(4) 11th Marines Barrier Drill Procedures (FOUO) / (Not Attached)
(5) 11th Marines Random Antiterrorism Measures Program (FOUO)
(6) Risk Management Methodology to 11th Marines Antiterrorism Plan 2020
(7) 11th Marines Asset List (FOUO) / (Not Attached)
(8) Emergency Lockdown Procedures
(9) Shelter in Place Procedures
(10) Glossary

1. Situation

a. General. The threat of terrorist attacks is one of many challenges facing 11th Marines and the 43 Area. This constantly evolving threat shows no signs of abating, but rather of growing in intensity and sophistication. Recent terrorist attacks accentuate the need for antiterrorism programs to keep pace with the asymmetrical and amorphous threats we confront. However, the threats that endanger the security and well-being of 11th Marines Regiment elements, personnel, and operations are not limited to terrorism. Manmade threats, natural hazards, and unintentional and intentional acts are additional threats that the 11th Marines AT program must also address.

b. Enemy Forces. For the purposes of this plan, there is no specified enemy force. However, an all-hazards threat approach will be used to identify threats or hazards that have a probability of occurring within Area 1. Annually, MCIWEST-MCB CAMPEN publishes an All Hazard/Threat Assessment (AHTA) that identifies a comprehensive list of threats and hazards which have a likelihood or probability of occurrence. This assessment is specifically tailored to Camp Pendleton, California and aids in the development of this AT plan.