UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

I MEFO 3302.1A
G-3/ATFP

AUG 23 2017

I MARINE EXPEDITIONARY FORCE ORDER 3302.1A

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: FORCE PROTECTION (FP) PROGRAM

Ref: (a) DODI 2000.16 (Vol I/II), DOD Antiterrorism Standards, 17 Nov 2016
(b) DODO 2000.12, DoD Antiterrorism Program, 8 May 2017
(c) DODI 5240.06, Counterintelligence Awareness and Reporting, 21 Jul 2017
(d) DODI 5240.18, Counterintelligence Analysis and Production, 17 Nov 2009
(e) DODI 5240.22, Counterintelligence Support to Force Protection, 15 Oct 2013
(f) DOD Foreign Clearances Guide
(g) SECNAV 3850.2E, Dept of the Navy Counterintelligence, 3 Jan 2017
(h) NAVMC 3500.103, Marine Corps Antiterrorism Manual, 27 Oct 2010
(i) CMC Policy Memorandum 1-11, Advocacy, 23 Feb 2011
(j) USMC Protection Advocate Charter, June 10 2013
(k) MROC Decision Memorandum 07-2011, 20 Jan 2011
(l) MA Operational Advisory Group (OAG) Charter, Apr 2012
(m) MCO 3058.1, Marine Corps Mission Assurance, 23 Oct 2014
(n) MCO 3302.1F, Marine Corps Antiterrorism Program (Draft)
(o) MCO 3440.8, Installation Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE) Protection Program, 08 Jan 2008
(p) MCO 3501.36A, Marine Corps Critical Infrastructure Program (CIP), 25 Jan 2008
(q) MCO 3850.1J, Policy and Guidance for Counterintelligence (CI) and Human Source Intelligence (HUMINT) Activities, 27 Aug 2007
(r) MCO 5239.2B, Marine Corps Cyber Security, 05 Nov 2015
(s) MCO 5530.14A, Marine Corps Physical Security Program Manual, 5 Jun 2009
(t) MCO 5580.2B, Marine Corps Law Enforcement Manual, 27 Aug 2008
(u) USPACOMINST 0536.2, USPACOM Antiterrorism Program, 30 Oct 2015
(v) MARFORPAC OPORD 06-01, Antiterrorism, 3 Nov 2006
(w) I MEF Capstone 2015-2019
(x) I MEF FY2017 Campaign Plan
(y) MEFO 3030.1, I MEF Continuity of Operations Plan, 21 Sep 2016
(z) I MEF Interim Arming Policy MSG, DTG 282355Z SEP 16
(aa) I MEF Security Augmentation Force (SAF) Support Plan, MSG DTG 172136Z MAR 16
(bb) MCIWEST-MCB CAMPENO 3006.1A, Camp Pendleton Mission Assurance Order, 2 Oct 2014

Encl: (1) Antiterrorism/Force Protection (ATFP) Planning
(2) Risk Management (RM)
(3) Critical Infrastructure Protection (CIP)
(4) Resource Application

(7) Operational Forces Higher HQ Protection Program Review Benchmarks
(8) JTF Protection Planning Considerations
(9) Acronyms

1. Situation

a. General

(1) Purpose. To publish comprehensive Force Protection (FP) policy and establish processes to align and synchronize the management of protection-related programs within the I Marine Expeditionary Force (MEF).

(2) Background. I MEF forces whether operating abroad or in garrison, face a complex array of manmade and naturally occurring threats and hazards. Among them, I MEF faces a growing number of potential adversaries with the ability to asymmetrically cripple force deployment, warfighting, and sustainment capabilities by targeting both critical military and civilian infrastructure necessary to support global operations. In addition, I MEF faces potential threats through catastrophic natural disasters and technological failures with potential to create high impact second and third order effects that can degrade or negate mission accomplishment. The unpredictable and increasing sophistication of some of these threats may result in incidents occurring with little to no warning. These threats however, can be assessed and prioritized in order to develop strategies to prevent or mitigate their effects. Force Protection is the process through which to protect and ensure the continued function and resilience of capabilities and assets to include; personnel, equipment, facilities, networks, information, information systems, infrastructure, and supply chains critical to the performance of the Command's Mission Essential Tasks (METs) and Mission Essential Functions in any operating environment or condition. Through FP, I MEF will be more proactive and efficient with protection efforts and better postured to meet operational and/or tenant based requirements in response to a crisis.

b. References (i) through (n) are the primary sources of higher headquarters information relative to the overall FP program. This Order amplifies and clarifies policies and practices for operational implementation, and applies to all personnel assigned to or attached to I MEF. I MEF forces as tenants aboard Marine Corps Bases and Stations, will support installation Mission Assurance (MA) efforts in consonance with Reference (cc). Regardless of geographic location or whether nested under service component MA programs, the safety and security of personnel and equipment remain inherent responsibilities of the Commander, whether deployed or at home base/station.

c. Enemy. The enemy is defined as any natural or manmade hazard or adversary capable of threating or inflicting harm to I MEF personnel, facilities, and equipment. I MEF forces are vulnerable to a range of threats and hazards within diverse operating environments while executing their worldwide missions. These (often asymmetric) threats may range from criminal activities, cyber intrusions, and natural disasters to insider threats/disgruntled employees to home-grown violent extremists (HVE) and terrorist attacks.

d. Friendly

(1) Higher

(a) Marine Corps Forces Pacific (MARFORPAC)

(b) Headquarters Marine Corps (HQMC)

(2) Adjacent

(a) Marine Corps Installations - West (MCI-W)

(b) Marine Corps Base Camp Pendleton, CA

(c) Marine Corps Air Station Camp Pendleton, CA

(d) Marine Corps Air Station Miramar, CA

(e) Marine Corps Air Station Yuma, CA

(f) Marine Corps Air Ground Combat Center Twentynine Palms, CA

(g) Marine Corps Mountain Warfare Training Center Bridgeport, CA

(h) Marine Corps Logistics Base Barstow, CA

(3) Subordinate

(a) 1st Marine Division (1st MARDIV)

(b) 1st Marine Logisitics Group (1st MLG)

(c) 3rd Marine Aircraft Wing (3rd MAW)

(d) I MEF Information Group (I MIG)

(e) 11th Marine Expeditionary Unit (11th MEU)

(f) 13th Marine Expeditionary Unit (13th MEU)

(g) 15th Marine Expeditionary Unit (15th MEU)

(4) Supporting Agencies

(a) Department of Homeland Security (DHS)

(b) Department of State (DOS)

(c) Federal Bureau of Investigation (FBI)

(d) Naval Criminal Investigative Service (NCIS)

(e) State and Local Emergency Management/Law Enforcement Agencies

e. Attachments/Detachments. None.

2. Cancellation. I MEFO 3302.1

3. Mission. I MEF executes continuous and integrated protection related programs and activies using a comprehensive FP program in order to ensure mission execution in all-threat/all-hazard environments and in support I MEF operational readiness.

4. Execution

a. Commander's Intent

(1) Purpose. This Order aligns, integrates, and synchronizes multiple protection related plans, programs, and policies to gain efficiencies and generate synergy across the FP spectrum. It also promulgates a comprehensive and standardized risk management (RM) process that provides commanders, at all levels, with consistent risk-based information and recommendations. These protection related programs include but are not limited to; AT/FP, CIP, CBRN, PhySec, and MEF LE employment.

(2) Method. FP is a proactive, integrating process that links various protection related programs and activities in order to efficiently manage risk and risk mitigation efforts within units at all levels. Through this systematic framework, commanders can better prioritize their risk decisions in order to optimize mission performance, resiliency under all conditions, and find efficiencies in an increasingly fiscal and resource constrained environment. Further, synchronization of subordinate organization capabilities and efforts will promote synergy and enable I MEF to effectively manage the spectrum of threats and hazards necessary to ensure mission success.

(3) End State. A comprehensive, focused, and efficient FP process that attains optimal protection, preserves I MEF mission essential functions and capabilities, and guides reconstitution efforts following an all-threat/all-hazard incident or occurrence.

b. Concept of Operations. The execution, management, and reporting of FP revolves around five primary elements; planning, risk management, training & exercises, resource generation/application, and continuous program review. These elements apply to all FP programs and provide the integrating framework to ensure overall success. The enclosures within this Order address these specific elements in addition to other protection related functions.

(1) Organizational Responsibilities. The I MEF Assistant Chief of Staff, G-3 (AC/S, G-3) has the overarching responsibility for execution, management, and reporting of I MEF FP functions. The I MEF G-3 (or appointed representative) shall be the MEF's representative for all MEF FP coordination and reporting to higher, adjacent, and supporting commands and entities. Major Subordinate Commands/Elements (MSC/MSE), with direction and guidance from the I MEF CE and identified references, shall develop, implement, and report on FP programs within their respective organizations. I MEF will integrate FP and protection related concepts with current and projected warfighting requirements. FP plans must be designed to address an all-threat/all-hazards risk assessment, and synchronize with, and support the Marine Corps Planning Process (MCPP) for all missions.

(2) FP Assessment Benchmarks. I MEF and MSC/MSEs will ensure compliance with the FP assessment benchmarks (Enclosure 7) in both garrison and expeditionary environments. Commanders shall conduct FP program reviews, using these benchmarks to evaluate the effectiveness and efficiency of FP programs. Program reviews shall also include assessments of the degree in which programs comply with other standards for individual protection-related

programs. For example, when assessing the ATFP program, the associated standards prescribed in Reference (n), shall be used in addition to the FP assessment benchmarks in order to fully evaluate the effectiveness and integration of the AT program component.

(3) Force Protection Executive Committee (FPEC). The FPEC is chaired by the AC/S, G-3 and shall be composed of select members of the Principle Staff (G-shops), other staff, and subject matter experts as required. It will develop and refine FP program guidance, policy, and standards in addition to approving FPWG charters, adjudicating recommendations, and determining resource allocation priorities. The FPEC shall meet at least semiannually and maintain associated minutes for two years.

(4) Force Protection Working Group (FPWG). The FPWG oversees implementation of the FP program, develops and refines components therein, and addresses emergent FP issues. It will serve as the focal forum for integrating FP functions across multiple protection and other related programs. The FPWG executes the following; synchronizes FP activities, tracks FP related projects and resource requirements, reviews higher and lower regulations for compliance and standardization; and performs other functions as required by the FPEC. The FPWG will also serve to interface with the corresponding MCI-W/CAMPEN Mission Assurance Working Group (MAWG) IOT efficiently synchronize efforts and mutually supporting functions. The FPWG is chaired by the MEF FP Officer and will be comprised of designated core and adjunct members. Additional staff and subject matter experts may be tasked to participate on an as needed basis. The FPWG will meet at least quarterly and maintain meeting minutes for two years.

(a) FPWG Core Members:

1. I MEF Force Protection Officer/Chief

2. I MEF CBRN Officer/Chief

3. I MEF EOD Officer/Chief

4. MSC/MIG ATFP Officers/Chiefs (MIG, DIV, MAW, & MLG)

5. MEU ATFP Officers/Chiefs (composited/CONUS)

6. 1st LE Battalion ATFP Officer/Chief

7. I MEF G-2X/CI Chief

(b) Adjunct Members:

1. Naval Criminal Investigative Service (NCIS)

2. MCI-W Mission Assurance Officer

3. MCI-W ATFP Officer

4. MCI-W/MCB CAMPEN Provost Marshal's Office (Rep)

5. Representatives and/or subject matter experts from other staff sections may be requested on an as needed basis.

6. Other local area LE, DOJ, and governmental agencies may be requested on an as needed basis.

(5) Threat Working Group (TWG). The TWG develops and refines threat assessments and coordinates/disseminates threat warnings, reports, and related summaries. The I MEF FP Officer shall serve as a member of the MCI-W/CAMPEN TWG, or designate representatives on behalf of the FPWG.

(6) Physical Security Working Group (PSWG). Each MSC/MSE is responsible for the establishment of a physical security (PHYSEC) program within their respective commands in accordance with (IAW) Reference (t). When required, the PSWG shall be integrated into the FPWG to facilitate information sharing and collaboration. The PSWG develops recommendations to mitigate identified vulnerabilities and presents these measures to the FPWG for consideration.

(7) Continuity of Operations (COOP). COOP efforts shall be centrally coordinated at the I MEF CE level, but decentrally executed. Each MSC/MSE CE is responsible for the establishment of COOP related plans within their respective commands to mitigate critical vulnerabilities to assets tied to mission essential functions. Reference (t).

(8) Critical Infrastructure Protection (CIP) and Critical Asset Identification Process (CAIP). The CAIP provides a common analytical framework for identifying Task Critical Assets (TCAs) and corresponding Supporting Infrastructure Critical Assets (SICAs) that, if disrupted or destroyed, could preclude the MEF and subordinate MSC/MSEs from performing assigned Mission Essential Tasks (METs). The determination and characterization of these assets are critical to the development of prioritized protection strategies and resource allocation toward mitigating measures. The mechanism for managing this data is the Marine Corps Critical Asset Management System (MC-CAMS). References (m) and (q) and Enclosures (2) and (3) further define CIP/CAIP goals.

(9) All-Threats and Hazards RM Methodology. The RM methodology will be used to examine risk to mission critical assets and identification of risk trends and issues. Execution of the RM methodology includes completion of risk assessments and risk planning for mission critical assets and supporting infrastructure. I MEF will implement an effective RM process to:

(a) Identify and assess risk, per the reference.

(b) Identify protection-related capabilities and gaps that impact the ability to execute missions, core capabilities, and functions, and provide prioritized recommendations and funding assessments to inform Service level resource planning, capabilities development, and acquisition processes IAW relevant programming and force development guidance. The Planning, Programming, Budgeting, and Execution (PPBE) process will be used to obtain and execute resources, particularly for unfunded requirements. I MEF will assist in the prioritization of capabilities, gaps, and resource requirements supporting the Marine Corps Force Development System (MCFDS), PPBE, and other decision-support processes.

(c) Define and fully justify Commanders' Risk Decision Packages (RDPs) for prioritization and fiscal consolidation. Projects identified in RDPs will be developed and submitted for funding consideration by the Third Quarter of each Fiscal Year (FY). This process is outlined within Enclosure 5.

(d) Ensure coordination, synchronization, and integration of individual protection-related programs.

(e) Nest with higher, adjacent, and supporting commands in order to exploit all risk-reduction options.

(10) Marine Corps Mission Assurance Operational Advisory Group (OAG). The Marine Corps Mission Assurance (MA) OAG is the principle forum for establishing community priorities, developing consistent and relevant messaging, and promoting interaction between the operating forces; supporting establishment; the Protection Advocate, Deputy Commandant for Plans, Policies and Operations (DC, PP&O); Marine Corps Installations Command (MCICOM); Marine Corps Systems Command (MARCORSYSCOM); Training and Education Command (TECOM); Manpower and Reserve Affairs (M&RA); and the Capabilities Development Directorate (CDD). The OAG will convene semi-annually and will include representation from I MEF as a permanent, voting member.

(11) Destructive Weather. Destructive Weather operations will be conducted in accordance with Reference (cc).

c. Tasks

(1) AC/S, G-1

(a) Manage/refine the I MEF SAF Support Plan (Reference bb), in coordination with the AC/S G-3 IOT provide appropriate support to MCI-W/MCB CAMPEN as required during elevated Force Protection Conditions (FPCONs).

(b) Implement process controls to ensure all travelers comply with the requirements of Reference (f).

(c) Provide representation to the FPEC and FPWG to address administration and manpower equities in conjunction with FP plans, policies, and operations, as required.

(2) AC/S, G-2

(a) Provide appropriate Geographic Combatant Command (GCC) threat/hazard assessment guidance to MSC/MSE's to support intelligence and counterintelligence product development and analysis.

(b) Provide Foreign Intelligence and Counterintelligence threat awareness and Indications and Warning (I&W) analysis.

(c) Within the rules and regulations governing Intelligence Activities and Operations, coordinate intelligent efforts with appropriate Law Enforcement Agencies and other agencies to ensure the collection, analysis, and dissemination of the most current and comprehensive threat information.

(d) Assist deploying units/personnel with threat and country specific training and briefings as required.

(e) As required, provide representation to the FPEC, FPWG, and TWG IOT address intelligence, surveillance, and counter-surveillance issues and activities relevant to FP.

(3) AC/S, G-3

(a) Designate at least one ATO Level II certified FP Officer in writing.

(b) Facilitate and ensure the integration of Risk Management into the MCPP.

(c) Ensure deploying forces are prepared to meet GCC AT plans and other requirements of this Order.

(d) Notify Commander Marine Forces Pacific (COMMARFORPAC) when the I MEF Crisis Action Team (CAT) is activated in response to any threat/hazard that materializes.

Note: while situationally dependent COMMARFORNORTH, COMMARFORCOM, and MCICOM will be concurrently notified in most cases.

(e) Maintain connectivity throught the MEF Operations Center (MOC) to the Command, Control, Communications, Computers, and Intelligence (C4I) site suite for rapid threat dissemination and real-time threat sharing. The C4I Suite can be accessed via the following URL; https://c4isuite.atfp.cnic.navy.mil/usmc/Pages/index.aspx.

(f) Maintain cognizance over, and provide representation to the FPWG and adjacent advisory forums.

(g) Exercise overall responsibility for the I MEF CIP in order to manage all matters pertaining to the identification, prioritization, and risk management for Task Critical Assets (TCAs) and Supporting Infrastructure Critical Assets (SICAs). Ensure CIP is integrated with all other FP protection-related programs in order to establish a uniform risk-based approach to protection. As required, establish a Critical Infrastructure Program Working Group (CIPWG) to coordinate and address program requirements and issues.

(h) Chair the I MEF FPEC semi-annually. Ensure FP issues are developed with courses of action and recommendations for CG I MEF decision.

(i) Ensure the I MEF Command Duty Officer (CDO) instructions are aligned with this Order and other protection related measures as required.

(4) I MEF FP Officer

(a) Exercise overall staff cognizance for matters pertaining to Force Protection.

(b) Assist in the prioritization of capabilities, gaps, and resource requirements supporting the Marine Corps Force Development System (MCFDS), Planning, Programming, Budgeting, and Execution (PPBE), and other service level decision support processes. In coordination with the AC/S G-8, assist in FP resource prioritization to address unfunded program deficiencies.

(c) Assist I MEF planners and MSC/MSEs in developing and implementing plans to address and manage indentified risks as part of the MCPP.

(d) In conjunction with host installations, coordinate annual all-threats/all-hazards protection exercises to ensure the integration of various Operating Force (OPFOR) protection-related requirements. Coordinate with MCI-W for support to triennial Marine Corps Mission Assurance

Assessments (MCMAA). Develop and manage a corrective actions plan to address any deficiencies identified by the MCMAA Team.

(e) Provide oversight for annual program reviews of all MSC/MSEs in order to ensure compliance with the program standards contained in the MA benchmarks, Enclosure (7). Provide assistance on corrective measures as required.

(f) Develop and manage the annual CAIP in order to identify critical assets associated with missions, capabilities, and functions.

(g) Document MEF critical assets, risk assessments, and RM plans utilizing the Marine Corps Critical Asset Management System (MC-CAMS).

(h) Assist with the coordination of I MEF resources as may be required by MCI-W during emergencies and/or response to other critical incidents to include SAF, CBRN, or other personnel and equipment as required.

(i) Coordinate Anti-Terrorism Officer (ATO) Level II and other FP related training.

(j) Coordinate with MCI-W as required for inclusion into working groups, FPCON changes, and implementation of Random Antiterrorism Measures (RAMs), per Reference (cc).

(k) Chair the I MEF FPWG and other FP advisory forums as required in order to discuss issues and develop course of actions for FPEC consideration and decision.

(5) AC/S, G-4

(a) Support the identification of critical transporation assets/nodes (air, sea, rail, and road) that facilitate I MEF force deployment.

(b) Provide relevant, timely, and accurate information to AC/S, G-3 with regard to movement of personnel, supplies, and equipment that require security during transit.

(c) Assist security efforts in the event of an incident that requires additional equipment, engineering, or facility support; e.g. implementation of barrier plans in an expeditionary environment.

(d) Coordinate with the AC/S, G-3 to identify I MEF facilities for use as emergency shelters and other support necessary in response to critical incidents or other operational requirements.

(e) As required, provide representation to the FPEC, FPWG, and TWG to address logistics, maintenance, and transportation issues and activities relevant to FP.

(6) AC/S, G-5

(a) Be prepared to evaluate impacts of Force Protection related issues to I MEF participation in OPLANs/CONPLANs; provide detailed planning to MARFOR requirements, as required.

(b) Provide a model for generating MAGTFs to respond to emergent crises.

(c) Provide representation to the I MEF Force Protection Working Group as required.

(d) Provide support, scientific and technological expertise, and advice for FP planning, program performance, and process improvement in order to enhance overall protection of forces and mission execution.

(7) AC/S, G-6

(a) Coordinate and maintain daily status of Information Operations Conditions (INFOCONs) in response to I&W of computer network threat reports. Integrate INFOCON status with FP program status reports in order to develop integrated and complete threat pictures.

(b) Advocate for the protection and resiliency of critical telecommunications nodes that support I MEF assigned missions, core capabilities, and functions in conjunction with CIP activities.

(c) Support the incorporation of FP concepts into information systems that meet Department of Defense (DoD) Information Assurance (IA) requirements per Reference (s).

(d) Assist with security efforts in the event of an incident that requires additional secure and unsecured communications support.

(e) Provide representation to the FPEC, FPWG, and TWG to address C4I issues, as required.

(8) AC/S, G-7

(a) Ensure AT training is incorporated into unit-level training plans and pre-deployment exercises.

(b) Provide representation to the FPEC, FPWG, and TWG to address C4I issues, as required.

(9) AC/S, G-8

(a) Ensure FP funding requirements are identified, prioritized, and included in the budgeting process for inclusion in the Program Objective Memorandum (POM) cycle. In coordination with the MEF FP Officer, identify gaps in funding which adversely impact I MEF's FP program.

(b) Implement procedures to capture FP related expenses and establish procedures for emergency purchases, if required.

(c) Incorporate FP program funding into annual budget processes.

(d) Provide representation to the FPEC, FPWG, and TWG to address budgetary issues, as required.

(10) Staff Judge Advocate

(a) Provide expertise and guidance on legal issues that impact the planning and execution of the FP program.

(b) Provide representation to the FPEC, FPWG, and TWG to address legal matters, as required.

(11) Security Manager

(a) Establish security measures and provide guidance for maintaining classified and unclassified material to support this plan.

(b) Coordinate with the FP Officer, staff sections, NCIS, and other agencies, as appropriate, concerning breaches of security.

(c) Provide representation to the FPEC, FPWG, and TWG, as required.

(12) Public Affairs Officer. Provide representation to the FPEC, FPWG, and TWG to address public affairs and media issues, as required.

(13) Commanding Officer, I MIG

(a) Develop and implement an AT plan for the I MEF CE and I MIG.

(b) Develop a Physical Security (PHYSEC) program and ensure that I MEF CE facilities and areas of responsibility comply with the AT, PHYSEC requirements, IAW the associated references.

(14) Common Tasks for all MSC/MSEs

(a) Develop FP element programs and other protection-related programs, as required based on mission requirements, to support this Order and requirements related to MA benchmarks Enclosure (7).

(b) Designate trained/certified AT/FP and other protection-related program officers in writing, as required, to ensure application of the FP process and RM methodology.

(c) Develop and implement plans to address and manage identified risk, as part of the planning process, in both garrison and expeditionary environments. Ensure deploying forces have clearly outlined AT plans with the required elements and force protection measures necessary to meet GCC and other requirements identified in this Order.

1. Ensure deploying personnel are provided AT planning information (e.g., airfield, port, movement route information, threat, vulnerability, and criticality assessment data) to enable them to perform their mission(s) and develop tailored AT plans. Ensure deploying units having 300 or more personnel, assigned or under the operational control of a designated commander, have assigned a Level II certified ATO. This ATO will be designated in writing by the respective unit commander.

2. Ensure AT plans are developed for units at separate or leased facilities/spaces, training exercises, and special events.

(d) Be prepared to provide support and personnel for a SAF, as required with MCI-W during an emergency or terrorist event and/or increases in FPCON per Reference (bb).

(e) Conduct annual risk self-assessments and program reviews of subordinate commands to ensure compliance with FP program standards and MA benchmarks, Enclosure (7).

(f) Provide representation to the FPEC, FPWG, and TWG, as required.

d. Coordinating Instructions

(1) The C4I suite shall be used during critical incidents to report events for shared situational awareness with higher and adjacent units, while omitting detailed personal information or information that is considered sensitive. The C4I suite, when used in conjunction with established tactical systems, provides the capability to communicate across all levels and share threat information in real time.

(2) MC-CAMS is the primary FP support tool for managing mission and asset data and for RM activities. MC-CAMS is further explained in Enclosures (2) and (3) of this Order.

(3) Commanders with off-installation or stand-alone facilities shall conduct risk management activities as part of their annual FP process and supporting activities. I MEF tenants aboard other installations shall coordinate with, and support, the host installation's FP governance structure and associated RM activities. Under the joint basing concept, other service/agency tenants will coordinate with, and support, host installation FP and RM processes.

(4) I MEF, in conjunction with MCI-W/MCB CAMPEN and Marine Forces Pacific (MARFORPAC), shall establish FPCON levels and implement RAMs, as dictated by higher headquarters and/or host installation requirements.

5. Administration and Logistics

a. The Deputy Commandant, Plans, Policy & Operations (DC, PP&O) is the Service appointed Protection Advocate for questions and overall guidance related to FP. The AC/S G-33 is the Office of Primary Responsibility (OPR) and point of contact for FP correspondence related to this Order.

b. Recommendations for changes to this Order should be submitted to the AC/S G-3 (Attn: FP Officer) via the chain of command.

6. Command and Signal

a. Command. This Order is applicable to military and civilian personnel assigned or attached to I MEF.

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

LEWIS A. CRAPAROTTA

DISTRIBUTION: I/II

Antiterrorism/Force Protection (ATFP) Planning

1. Antiterrorism (AT) Programs

a. Commanders are responsible for developing comprehensive AT programs, which shall ensure unity of effort resulting in a coordinated defensive posture for protecting personnel and assets from acts of terrorism and destructive events. The threat of diverse hazards requires the development of multi-faceted, comprehensive AT programs. Commanders shall ensure AT considerations are included in all plans, operations, and daily activities. AT programs shall follow an all-hazards approach, be proactive in nature, and be coordinated and synchronized throughout appropriate commands, down to the battalion/squadron level.

b. Commanders shall ensure AT programs are coordinated and synchronized with this plan and/or host installation AT plans. Deployed units shall ensure AT plans comply with the supported command's AT plan to include COCOM requirements.

c. The development and maintenance of the AT program elements should be ongoing and continuously refined to ensure the relevance and viability of all defensive measures employed, in order to reduce vulnerabilities to all-hazard based threats.

d. AT Program Elements

(1) AT Planning

(2) Risk Management

(3) Training and Exercises

(4) Resource Application

(5) Comprehensive AT program review (MA Benchmarks)

e. Risk Management (RM). The RM process outlined in Reference (m) and Enclosure 2 of this order shall be applied in all aspects of AT program implementation and planning, including operational plans and decisions; development of risk mitigation measures; and the prioritization and allocation of resources.

f. All Hazards Threat Assessments (AHTA). Using the AHTA methodology (refer to Enclosure 2), prepare and update annual threat assessments to support operational planning and risk decisions for unique mission requirements including, but not limited to, in-transit forces, training and exercises, operational deployments, and special events. Commanders shall implement effective processes to integrate and fuse all sources of available threat information from local, state, federal and host nation agencies, as appropriate, in order to provide for a continuous analysis of threat information to support the threat warning process.

g. Vulnerability Assessments (VA). Within 90 days of a completed assessment, commanders shall prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report to the first general officer, flag officer, or civilian equivalent director in the chain of command (as appropriate based on the level of activity), the results of the assessment. VAs are conducted at least annually and for:

(1) Facilities populated daily by 300 or more personnel (mass gathering) or any event or activity determined to be a special event or other activity involving a gathering of 300 or more Department of Defense (DoD) personnel.

(2) Facilities responsible for emergency response or PHYSEC plans and programs, or determined to host critical infrastructure.

(3) Sea and air ports of embarkation and debarkation; movement routes (sea, air, ground, and rail); assembly, staging, reception, and final bed down locations, in support of any battalion, squadron, ship, or equivalent operational deployment; similar sized in-transit movement or training exercise; and any movement or shipment of military cargo (including Military Sealift Command voyage charters).

2. Anti-Terrorism Officer (ATO). Commanders shall appoint an AT Level II-trained ATO, in writing, down to the Battalion/Squadron level, for separate facilities, and for deploying units having 300 or more personnel assigned or under the operational control of a designated commander. ATOs shall:

a. Develop a comprehensive AT program and plan, which includes the above elements and considerations.

b. Advise the commander on all AT-related issues.

c. Ensure required AT training is conducted and documented.

d. Annually exercise and review the AT plan. When in garrison, command annual exercise objectives can be integrated into the host installation ATFP exercises in order to meet this requirement.

e. Request access to the Headquarters Marine Corps AT Portal at https://eis.usmc.mil/sites/hqmcppo/PS/PSM/AT/SitePages/Home.aspx; this portal provides references pertaining to doctrine, policy, planning, training, and lessons learned.

3. AT Plans

a. Commanders shall develop tailored AT plans for preventing, responding to, and recovering from, crisis incidents. The AT plan should be combined with other protection-related programs, such as CIP, CBRN and PHYSEC. AT plans shall address the following, as applicable:

(1) Command and control for overall AT plan execution.

(2) Task organization of AT organizations and capabilities.

(3) Specific threat risk mitigation measures to establish a local baseline defensive posture.

(4) Specific FPCON measures and RAMs to enable elevated security postures and FPCON levels.

(5) Physical security measures.

(6) Designation and protection of High Risk Personnel (HRP).

(7) Construction and building considerations.

(8) AT measures in support of logistics and contracted services.

(9) Identification/protection of critical assets and infrastructure.

(10) AT measures for in-transit movements of personnel.

(11) Terrorism consequence management measures, including CBRN and Weapons of Mass Destruction (WMD) mitigation planning.

(12) Mass notification/warning and personnel recall/accountability procedures

b. The minimum elements of an AT plan include; intelligence, personnel, operations, exercises and training, resource application, and coordination as outlined in reference (a).

c. Deploying units shall submit their AT Plan for approval to the next higher command, and this AT plan shall be forwarded to the appropriate Marine Forces (MARFOR)/Combatant Commander (COCOM) for approval, as required.

d. Commanders will approve and sign AT plans, giving AT plans the full authority of military orders.

4. AT Program Coordination. Commanders shall coordinate their AT program and plan requirements with the host installation/separate facility commander, or civilian equivalent director. I MEF tenant units shall participate fully in installation AT programs. I MEF units coordinate AT programs by:

a. Ensuring AT plans support the next higher level of command, host installation or supported commander.

b. Participating in training, exercises, and working groups.

c. Coordinating for resources and support.

5. Physical Security. Commanders shall comply with the requirements of reference (t). PHYSEC measures are multi-layered and include the integration and synchronization of the following essential elements:

a. Access Control.

b. Material Control.

c. Personnel.

d. Restricted Areas.

e. Electronic Security Systems (ESS).

f. Security Forces.

6. FPCON. FPCON progressively increases protective measures implemented by units in anticipation of, or in response to, the threat of a terrorist attack. The FPCON is the principal means through which commanders apply an

operational decision on how to best guard against the terrorist threat. FPCON measures assist commanders in reducing the risks of terrorist attacks and other security threats to DoD personnel, units, and activities. FPCON consists of five progressive levels of increasing AT protective measures; see Reference (a), Chapter 2 for definitions of baseline FPCON levels.

a. When units implement these measures for their site-specific circumstances, they should account for, as a minimum, COCOMs/Service requirements and local laws. Once a FPCON is declared, all listed security measures are implemented immediately unless waived by the first one-star Commanding General in the respective unit's chain of command.

(1) Site-specific AT measures and action sets shall be developed for potential terrorist targets consistent within each FPCON level. Ensure these measures are coordinated with subordinate, adjacent, and higher commands, and local applicable agencies.

(2) Site-specific AT measures, linked to an FPCON and PHYSEC actions, shall be classified "CONFIDENTIAL." When separated from the AT or PHYSEC plan, specific AT measures linked to an FPCON and site-specific FPCON levels may be downgraded to "FOR OFFICIAL USE ONLY", if appropriate.

(3) I MEF site-specific measures (Action Set Matrix [ASM]), based upon MCIWEST/MCB Camp Pendleton measures, are kept separate from this order. The I MEF ASM is promulgated, as required. MSC/MSEs shall ensure site-specific measures are developed in both garrison and expeditionary environments, and comply with host installation or Area of Responsibility (AOR) FPCONs.

b. Commanders may raise the FPCON above the established baseline and return the FPCON to the baseline, based solely on command determination of the threat. However, commanders may not lower the FPCON below the established baseline.

c. I MEF units stationed within the CONUS shall comply with installation FPCONs, to include procedures for lowering and raising.

7. Random Anti-Terrorism Measures (RAMs). Commanders shall develop and implement RAMs as an integral component of the overall AT program. To maximize the effectiveness and deterrence value, RAMs should be implemented without a set pattern in terms of the measures selected, time, place, or other variables. RAMs, at a minimum, shall consist of the random implementation of higher FPCON measures in consideration of the local terrorist capabilities. Random use of other PHYSEC measures should be used to supplement FPCON measures.

a. Commanders shall employ RAMs in conjunction with site-specific FPCON measures in a manner that portrays a robust security posture from which terrorists cannot easily discern ATFP, security, or other patterns or routines. Subordinate and tenant units should be used in RAM planning and execution.

b. In garrison, I MEF unit commanders shall implement RAMs in coordination with the host installation.

c. While deployed, I MEF unit commanders shall implement RAMs per AOR requirements.

8. In-Transit Security

a. Commanders with force protection responsibility for transiting forces shall ensure the development and execution of in-transit security plans and conduct of pre-deployment VAs. Commanders shall implement appropriate AT measures to reduce risk and identify vulnerabilities. Deploying commanders shall adhere to COCOM requirements for tracking and security while transiting through or to the COCOM's AOR. Commanders remain responsible for the protection of their personnel regardless of location. In the current threat environment, intra-theater transiting forces require the same degree of attention as other transiting units in order to effectively deter, disrupt, and mitigate acts of terrorism. In-transit forces include all DoD or DoD-chartered ships and aircraft, as well as DoD elements that could present lucrative terrorist targets (i.e., minimally those elements, units, or groups consisting of more than 50 personnel). Commanders may lower this threshold of unit size at their discretion based on the assessed threat or other considerations.

b. Requirements

(1) Develop and execute in-transit security plans, as required. This planning process, in addition to the use of RM planning techniques, shall measure the activity against the risk to the in-transit element and shall enable the commander to determine whether to suspend or continue the transit.

(2) Ensure all DoD-sponsored travelers, while transiting to outside CONUS locations, are in compliance with the travel policies set forth in the DoD Foreign Clearance Guide.

(3) Disseminate travel warnings and FPCON information via Secret Internet Protocol Router Network (SIPRNET) and Non-Classified Internet Protocol Router Network (NIPRNET) messages, emails, and via telephone.

(4) Ensure the development and compliance of AT awareness training and education programs outlined in Enclosure (7) of this order, as well as AOR-specific AT training.

(5) Ensure in-transit forces, units, and individuals are provided with detailed threat information covering transit routes and sites that will be visited by the deploying unit or individuals. Such information shall include focused information on potential terrorist threats (e.g., tailored production and analysis), and guidance on the development of AT protection risk mitigation measures, to aid in the development of tailored AT planning. Similar tailored information shall also be provided to intra-theater transiting units and individuals.

9. Information/Intelligence Flow and Reporting. Accurate and timely collection and dissemination of threat information/intelligence is vital to the fight against terrorism and other threats and hazards. Commanders must use and analyze all available information/intelligence to prevent, detect, deter, or mitigate threats against personnel and assets. Commanders must task the appropriate organization under their command or control to gather, analyze, fuse, and disseminate appropriate terrorism threat information/intelligence. If no organic intelligence capability exists, commanders must arrange for intelligence support from Higher Headquarters (HHQ) or another entity. All available sources (e.g., local, State, Federal law enforcement agencies, Host Nation, Department of State, intelligence agencies, HQMC-

produced AHTA) shall be leveraged, and the information/intelligence shall be integrated, fused, and disseminated, as appropriate.

a. Terrorism Threat Levels (TTL)

(1) The Director, Defense Intelligence Agency (DIA), establishes the DoD TTL identifying the potential threat to DoD interests in a particular country, including the United States. The DoD TTL applies whether or not U.S. personnel are present in the country. The COCOM may also set TTLs for specific personnel, family members, units, installations, or geographic regions in countries within the COCOM AOR, using the definitions and criteria established by the Director, DIA.

(2) Thorough analysis of the threat is critical to understanding Force Protection (FP) concerns. The threat analysis process directly impacts FP plans and resource allocation. The DoD uses the following factors to assess terrorist threats confronting DoD personnel, facilities, material, and interests: operational capability, intentions, activity, and operating environment. DoD TTL are located at http://dciis.dia.smil.mil/threat/WorldWide.html or on the MARFORNORTH website at https://www.mfn.usmc.smil.mil. Though a general TTL is given for each country, the actual terrorist threat in that country may vary from region to region based on the modus operandi of existing groups. The DoD uses four threat levels to define the degree to which the environment is conducive to conducting terrorist operations in a specific country, region, or locale:

(a) HIGH. Anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred modus operandi. There is a substantial DoD presence, and the operating environment favors terrorists.

(b) SIGNIFICANT. Anti-U.S. terrorists are operationally active and attack personnel as their preferred method of operation, or a group uses large casualty-producing attacks as its preferred method, but has limited operational activity. The operating environment is neutral.

(c) MODERATE. Terrorists are present but there is no indication of anti-U.S. activity. The operating environment favors the host nation/U.S.

(d) LOW. No terrorist group detected, or the terrorist group activity is non-threatening.

(3) Commanders shall, as appropriate:

(a) When local information indicates gaps, forward timely requests for information via appropriate intelligence collection and production channels.

(b) When operational, develop Priority Intelligence Requirements (PIR) and Commander's Critical Information Requirements (CCIR) to focus collection and analysis efforts.

(c) Provide units in transit with tailored terrorist threat information.

(d) Integrate counter-surveillance, surveillance detection, counter-intelligence (CI), and other specialized skills, as a matter of routine in all AT programs.

(e) Identify an official as the focal point for the integration of operations and local or Host-Nation intelligence, CI, and criminal intelligence information.

(f) Incorporate proactive techniques to detect and deter terrorists, particularly in support of assets or activities conducted in areas designated with SIGNIFICANT or HIGH threat levels. These activities shall include, but are not limited to: in-transit forces, HRP, special events, and high-value military cargo shipments.

(g) As required, request counterintelligence support.

(h) Forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD elements and personnel or assets for which they have responsibility, including the provision of such information to appropriate interagency officials.

(i) Ensure that personnel are trained to maximize the use of information derived from law enforcement liaison, and from intelligence and CI processes and procedures. This includes intelligence procedures for handling PIR for in-transit units and implementation of procedures to conduct intelligence preparation of the battle space and mission analysis.

b. <u>DoD Terrorist Threat Warnings</u>. Terrorist threat warnings are accomplished within the DoD through two mechanisms:

(1) <u>Terrorist Threat Warnings, Alerts, and Advisories</u>. The Intelligence Community System issues fully coordinated terrorist threat warnings, alerts, and advisories. The FBI is responsible for coordinating and issuing Intelligence Community Warnings for threats within CONUS.

(2) <u>Defense Indications and Warning System (DIWS)</u>. The DIWS is a second independent system. All DIWS members, at any level, may issue unilateral threat warnings referred to as Terrorism Warning Reports (TWRs), which are intended to expedite warnings and to be treated as distinct from a threat level change report. TWRs should not be confused with Defense TWRs, which only the DIA issues. Warnings within the DoD system generally stay within the system and are primarily for use by DoD activities.

c. <u>National Terrorism Advisory System (NTAS)</u>

(1) The NTAS replaced the color-coded Homeland Security Advisory System. This new system more effectively communicates information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. It recognizes that Americans all share responsibility for the nation's security, and should always be aware of the heightened risk of terrorist attacks in the United States and the actions they should take.

(2) After reviewing the available information, the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued. NTAS Alerts will only be issued when credible information is available. These alerts will include a clear statement that there is an <u>imminent threat</u> or <u>elevated threat</u>.

(a) Imminent Threat Alert: Warns of a credible, specific, and impending terrorist threat against the United States.

(b) Elevated Threat Alert: Warns of a credible terrorist threat against the United States.

(3) Using available information, the alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses and governments can take to help prevent, mitigate or respond to the threat. NTAS Alerts will be based on the nature of the threat. In some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels.

(4) NTAS Alerts contain a "sunset provision" indicating a specific date when the alert expires - there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

(5) Types of NTAS Alert Announcements. NTAS Alerts will be issued through State, local, and tribal partners; the news media; and directly to the public via the following channels:

(a) Official DHS NTAS webpage - http://www.dhs.gov/alerts

(b) Email signup - http://www.dhs.gov/alerts

(c) Facebook - http://facebook.com/NTASAlerts

(d) Twitter - http://www.twitter.com/NTASAlerts

(e) Data feeds, web widgets, and graphics - http://www.dhs.gov/alerts

d. Naval Criminal Investigative Service (NCIS). The NCIS maintains and operates the Multiple Threat Alert Center (MTAC) and provides support to I MEF, via MCIWEST/MCB Camp Pendleton installations, by collecting, processing, and disseminating information/intelligence regarding terrorists and other individuals or groups whose interests are hostile to U.S. personnel, installations, or activities (criminals, subversive, or extremist groups who oppose U.S. policy or presence). The goal is to warn commanders of possible attacks and provide a time, place, and method to assist them in making decisions on protecting personnel, installations, activities, and materiel. In addition to Marine Corps internal CI capabilities pursuant to reference (g), the NCIS also provides Counter Intelligence (CI) support; NCIS conducts CI operations to identify, neutralize, and defeat threats to personnel, assets, and information. Commanders shall provide NCIS with the CCIRs and PIR to focus their collection and analysis efforts.

e. MARFORNORTH Information Fusion Cell (IFC). The IFC provides commanders within the MARFORNORTH AOR with threat information/intelligence by facilitating and disseminating threat information received from United States Northern Command (USNORTHCOM) J2, as well as various joint service components, law enforcement agencies, and other local, State, and Federal agencies. The MARFORNORTH IFC provides a reach-back capability to USNORTHCOM

J2 for threat warnings, analyses, and assessments. The MARFORNORTH Command Operations Center (COC) serves as the continuous (24/7) coordination center of operations serving MCIWEST/MCB Camp Pendleton. The COC acts on behalf of the MARFORNORTH IFC to disseminate threat information/intelligence.

f. Analysis and Production. MARFORNORTH IFC is the focal point for all FP-related threat information/intelligence support. The IFC shall oversee correlation of law enforcement information/intelligence to provide a domestic summary consistent with pertinent DoD policy and guidance. The MARFORNORTH IFC provides MCIWEST/MCB Camp Pendleton commanders with indications and warnings of terrorist attacks, global situational awareness, global counterterrorism summaries, and analysis on foreign terrorist CBRNE capability.

g. Medical Threat Assessments. Threat assessments concerning current medical threats are available through the DIA Armed Forces Medical Intelligence Center on SIPRNET at http://www.afmic.dia.smil.mi.

h. C4I Suite. The C4I Suite is used to facilitate dissemination of service and MARFORPAC directed information reporting requirements, supporting the development of accurate assessments of threat trends, and providing a common, shared, situational awareness of the operational environment. The use of the C4I suite does not relieve the commander of meeting other reporting requirements directed by higher authority such as message traffic or voice reports.

(1) I MEF commands with 24/7 Operations (e.g., Command Duty Officers [CDO] or COC) will continuously monitor the C4I Suite for updates and changes. The chat and notices functions in the C4I Suite will be the primary tools for threat/information dissemination. The C4I Suite can be accessed at https://c4isuite.atfp.cnic.navy.mil/usmc/mcicom/mciwest/default.aspx

(2) Registration. To register for a C4I account and gain access to the system, go to the C4I registration site located at the following addresses:

(a) https://c4isuite.atfp.cnic.navy.mil (NIPR)

(b) https://c4isuite.atfp.cnic.navy.smil.mil (SIPR)

(3) Commanders shall refer to reference (t) for further registration and usage information.

i. Dissemination. The MARFORNORTH IFC shall disseminate TTL changes, suspicious activity reports, threat warnings, FP advisories, OPREP-3 SIRs, and OPREP-3 BLUE DARTs to subordinate commands via telephone, email, and official message. The MCIWEST/MCB Camp Pendleton G-3/5 or CDO shall further disseminate this information to I MEF G-33 Antiterrorism Officer, commanders/CDOs via the same means.

j. Legal Considerations and Intelligence Oversight. There are several regulations, executive orders, and laws that specifically govern the use of DoD intelligence assets and organizations in domestic operations. The purpose of the DoD intelligence oversight program is to ensure that personnel do not improperly collect, retain, or disseminate information about US persons and corporations. However, this does not affect counterintelligence collection by authorized intelligence agencies.

10. Suspicious Activity Reporting (SAR). Given the volume and dynamic nature of threat reporting, it is imperative that the Marine Corps leverage automated systems for reporting, storing, analyzing, and disseminating suspicious activity reports that affect Marine Corps forces, assets, and facilities. The Marine Corps has incorporated an enterprise-wide SAR program which includes; Eagle Eyes (EE), the Marine Corps Suspicious Activity Reporting Tool (MCSART), while also supporting the FBI managed eGuardian program.

a. eGuardian

(1) The eGuardian system shall serve as the exclusive DoD law enforcement suspicious activity reporting (SAR) system and shall be employed by DoD Law Enforcement Officers (LEOs), analysts, and technical contractors assigned, attached, or detailed to law enforcement agencies. Marine Corps law enforcement agencies and activities shall use the eGuardian system for reporting, storing, and sharing unclassified SAR of incidents that may be indicative of potential threats or suspicious activity related to I MEF personnel, facilities, or forces in transit.

(2) Timely reporting of suspicious activity enables the Marine Corps to identify and address threats at the earliest opportunity. SAR and force protection threat information shall be immediately available to, and shared among, appropriate Marine Corps law enforcement, antiterrorism, and other appropriate security personnel in support of I MEF missions to the maximum extent permitted by law, regulation, Executive Order (E.O.), and DoD issuances for force protection purposes.

(3) Information obtained through eGuardian shall not be disseminated outside of the DoD without the approval of the originating agency, a representative of a fusion or intelligence center, a member of the Joint Terrorism Task Force (JTTF), or an FBI eGuardian administrator.

(4) Only DoD law enforcement personnel or analysts within DoD law enforcement organizations will enter SARs into the eGuardian system. SARs may be reported to law enforcement from private citizens, DoD personnel, or may come directly from law enforcement personnel who observe or investigate activities.

(5) I MEF commands without organic law enforcement organizations or entities will report SARs to their supporting DoD law enforcement element.

b. Eagle Eyes (EE)

(1) EE is the official Marine Corps community awareness SAR program. The program is designed to leverage the awareness of community members and non-Law Enforcement and security personnel to report suspicious activity. The EE program provides the opportunity for anyone to report suspicious activity through the EE website or locally designated phone numbers.

(2) The EE program educates our Marines, families, Civilian Marines, and Contractors on typical activities terrorists engage in prior to attack and to recognize elements of potential terrorist or criminal activities.

(3) All I MEF personnel are encouraged to report suspicious activity through the official website, www.usmceagleeyes.org, providing detailed information and, when possible, imagery from mobile devices, CCTV, security cameras, or other imagery capture devices. Individuals can also report by

calling the local EE phone number, security personnel, or USMC LE.

(4) All reports submitted through the EE website are automatically uploaded into the MCSART and analyzed by designated and specially trained personnel.

c. Marine Corps Suspicious Activity Tool (MCSAT). The MCSAT provides a repository of descriptive data on individuals, vehicles, and activities to ensure historical SAR information remains accessible. This will help Marine Corps protection officials to detect and analyze suspicious persons and patterns of behavior within an area over long periods of time.

(1) The MCSAT can be accessed via the following link; https://77swan.com/Main/Login.mvc

11. FPCON Integrated Action Sets (Action Set Matrix). This section is FOR OFFICIAL USE ONLY and is kept separate from this Order. All MSC/MSE AT/FP Officers and Command Operations Centers must develop and maintain a copy of specific action sets for each FPCON in their desktop procedures. Copies are available via the I MEF Antiterrorism Officer.

12. Automated Travel Tracker/Individual Antiterrorism Plan (TT/IATP).

a. The CG I MEF mandates the use of the TT/IATP program as delineated in this document. The TT/IATP program provides a capability to maintain visibility of and account for I MEF personnel while traveling (leave or official TAD) globally, as well as the ability to transmit warnings, advisories, and other time-sensitive information via email or text messaging. It also provides a mechanism for travelers to develop and route their individual AT plan for approval when traveling to travel restricted areas. The TT/IATP program supplements but does not replace the requirement for theater, country, special area, or personnel clearances as required by the Foreign Clearance Guide (FCG).

b. Applicability. Applies to all Marines, Sailors, Civilian Employees and Contractors assigned to I MEF.

(1) Active Duty Personnel. All active duty military personnel will enter their travel information into the TT/IATP program prior to traveling to any country outside of CONUS. This applies to official/ unofficial travel when travel is not part of a unit deployment or a PCS move. It does not apply to travel within the foreign country of assignment. A TT/IATP entry is not required when traveling as part of an organization or unit deployment if the organization AT plan applies to and covers all travelers, unless personnel wish to travel outside the mission's diplomatic umbrella as part of unofficial travel while deployed, then an IATP/ TT is required.

(2) DOD Civilian/ Contractors.

(a) Official Travel. All other DOD personnel will enter their travel information into the TT/IATP program prior to traveling to a foreign country outside of CONUS when traveling in an official capacity. This applies to official travel when not part of a unit deployment or PCS move, but does not apply to travel within the foreign country of assignment. A TT/IATP entry is not required when traveling as part of an organization or unit deployment if the organization AT plan applies to and covers all travelers.

(b) Unofficial Travel. TT/IATP submission is not required for unofficial travel but is highly recommended.

(3) Family Members/ Civilian Dependents. TT/IATP submission is required for official travel only, however it is highly recommended for unofficial travel as well. ISOPREP and SERE are not required for travel.

c. PACOM Restricted Areas. Personnel traveling to a PACOM Travel Restricted area require a TT/IATP entry. The TT/IATP entry must be approved by an O7 or above (civilian equivalent) in the traveler's chain of command prior to submission of theater clearance in APACS (unless otherwise directed).

d. Mexico Travel. All travel to Mexico requires - at minimum, O-5 level approval. Additional approvals may be required based upon the specific areas of travel within Mexico. The DoD Foreign Clearance Guide is the definitive source for identifying these requirements. If the location requires a country/theater clearance request, the location is considered restricted. Personnel traveling to Mexico will select one of the following choices from the location drop-down menu within IATP/TT (refer to Para E below);

(1) "Mexico - Non-Prohibited/Unrestricted Areas for Leave". All IATP entries to unrestricted areas within Mexico require an O5 Commander or above approval. Use this option for leave, special liberty, or other non-official occurrences and for those locations (per the FCG) that do not require any additional APACs country/theater clearance approvals.

(2) "Mexico - Non-Prohibited/Unrestricted Areas for TAD/TDY". Use this option for official TAD/TDY travel to those locations (per the FCG) that do not require any additional APACs country/theater clearance approvals.

(3) "Mexico - Restricted Areas". All IATP entries to restricted areas within Mexico require an O6 Commander or above approve. Use this option for any location (official and non-official/leave travel) that requires a country/theater clearance or is otherwise designated as "restricted" or "prohibited" within the FCG.

e. IATP/ TT Submission. IATP can be accessed at the following URL: https://iatp.pacom.mil/. Since the TT/IATP program is hosted on a secure but unclassified portal, commanders may waive the requirement to input data into the system for sensitive travel. Should the command deem such travel as classified or of such a sensitive nature to require waiving the TT/IATP requirement, commands should submit the subsequent APACS request via the classified APACS program on the Secure IP Routed Network (SIPRNet). When doing so commands must develop procedures to track travelers and small deployed elements and provide them with warnings, advisories, and other time-sensitive information. Any waiver of TT/IATP program use will be clearly annotated in the comments section of the applicable APACS request.

(1) Sequential process for Pre-travel requirements.

(a) Approval of leave via the chain of command.

(b) AOR specific brief (within 90 days of travel).

(c) Level I ATFP awareness training completed (within 12 months).

(d) SERE 100.1 V2 Level A (within 36 months).

(e) ISOPREP/ verified in PRMS (within 12 months).

(f) If going to ROK, USFK required training.

(g) If going to Japan, USFJ required briefs.

(h) IATP/TT (submitted ahead of APACS).

(i) APACS submission and approval (if required).

(j) Travel (**Only after Leave, IATP/ TT and APACS approval**).

f. IATP Approvers. The IATP approver must be of equal or higher rank to the individual submitting the IATP. The Approver levels are outlined below:

(1) PACOM restricted area: General/ Flag Officer (GO/FO) or Senior Executive Service (SES) personnel.

(a) DOD FCG **must** be referenced for all other travel requirements for destinations within other COCOM AORs.

(2) Minimum required approval level for Restricted area not in the PACOM AOR may/may not require GO/ FO/ SES level approval. Always check the DOD Foreign Clearance Guide for clarification.

(3) Minimum required approval level for travel to unrestricted area is typically set by COCOM: O3/ GS12, O4/ GS13, O5/ GS14, or O6/ GS15.

(4) Contractors **cannot** approve an IATP.

13. Aircraft and Personnel Automated Clearance System (APACS). Personnel will submit a clearance request via APACS. APACS automates the process of requesting and approving classified and unclassified diplomatic and personnel clearances via a common, centralized and secure database. APACS is mandatory for processing DOD-sponsored foreign travel in all COCOMs effective 01 May 2008 and is available for both classified and unclassified request. (https://apacs.dtic.mil or https://apacs.dtic.smil.mil).

a. Theater Clearance. Theater Clearance is granted by a geographic Combatant Command (or through a component commander or other delegated authority) for official travel to or within its geographic Combatant Command area of responsibility (AOR). Theater clearance requirements do not apply to: personnel in unified or overseas Service commands traveling to units of those commands, intra-theater troop movements, personnel deploying to support formally approved exercises or deployments, or aircrew members who perform aircrew duties exclusively.

b. Country Clearance. Country Clearance is granted by a foreign government through a U.S. Embassy for official travel within that country. The U.S. Embassy Chief of Mission (COM) may delegate country clearance-granting authority for DoD personnel to the U.S. Defense Attache Office (DAO) or another defense-related entity in country. Country clearance covers only the visit to the country specified and for the purpose requested. Country clearance requirements do not apply to; personnel in unified or overseas Service commands traveling to units of those commands, intra-theater troop movements, personnel deploying to support formally approved exercises or deployments, or aircrew members who perform aircrew duties exclusively.

c. Special Area Clearance. Department of State, through the Secretary of Defense/Under Secretary of Defense for Policy (SECDEF/USD(P)), approves or disapproves Special Area clearance requests. Special Area clearance requirements do not apply to personnel in Unified or overseas Service Component commands traveling to units of those commands, intra-theater troop movements, personnel deploying to support formally-approved exercises or deployments, or aircrew members who perform aircrew duties exclusively.

14. DoD Foreign Clearance Guide (FCG). The DoD FCG contains information that may be sensitive, is based on bilateral arrangements between US and foreign government officials, and is not releasable outside the US Government unless approved by a competent authority. This document provides necessary information for aircraft international mission planning and execution, personnel travel to foreign countries, as well as general information on foreign locations. The DoD FCG is directive in nature for all DoD and DoD-sponsored travel abroad, travelers must ensure they comply with this Guide. The DoD Foreign Clearance Guide is available in both classified (SIPR) and unclassified (NIPR) versions at the following links; https://www.fcg.pentagon.smil.mil or https://www.fcg.pentagon.mil respectively. It is a good practice to check both versions, particularly for restricted areas travels to ensure complete information is obtained for planning. Prior to commencing travel, personnel should review Department of State Travel Warnings, Travel Alerts, and individual country specific information at https://www.travel.state.gov.

Risk Management (RM)

1. General. The Risk Management (RM) framework prioritizes FP program actions and requirements based on resource constraints (fiscal and personnel). This framework drives the common operational risk picture and facilitates collaboration with higher, adjacent, and subordinate commands, as well as other stakeholders, in both garrison and expeditionary environments. It also alleviates gaps within FP program execution, resulting in a seamless approach to risk reduction, while ensuring unity of effort. Commanders shall develop a RM process, as outlined in this section and reference (m), in garrison and expeditionary environments.

a. Marine Corps Critical Asset Management System (MCCAMS). MCCAMS is a mission and asset oriented data management system designed to provide operational and contingency planning support for FP and RM requirements. MCCAMS shall be used to manage RM data, including risk assessments (RA) and risk reduction planning results and related information. Where appropriate, MCCAMS will automate the sharing of RM data with other DoD components and data management systems.

b. The operational RM process for Marine Air-Ground Task Force (MAGTF) operations is inherent within the MCPP. Force Protection/Mission Assurance must be adequately considered in phases 1-4 of the MCPP; Figure 1 depicts this process.

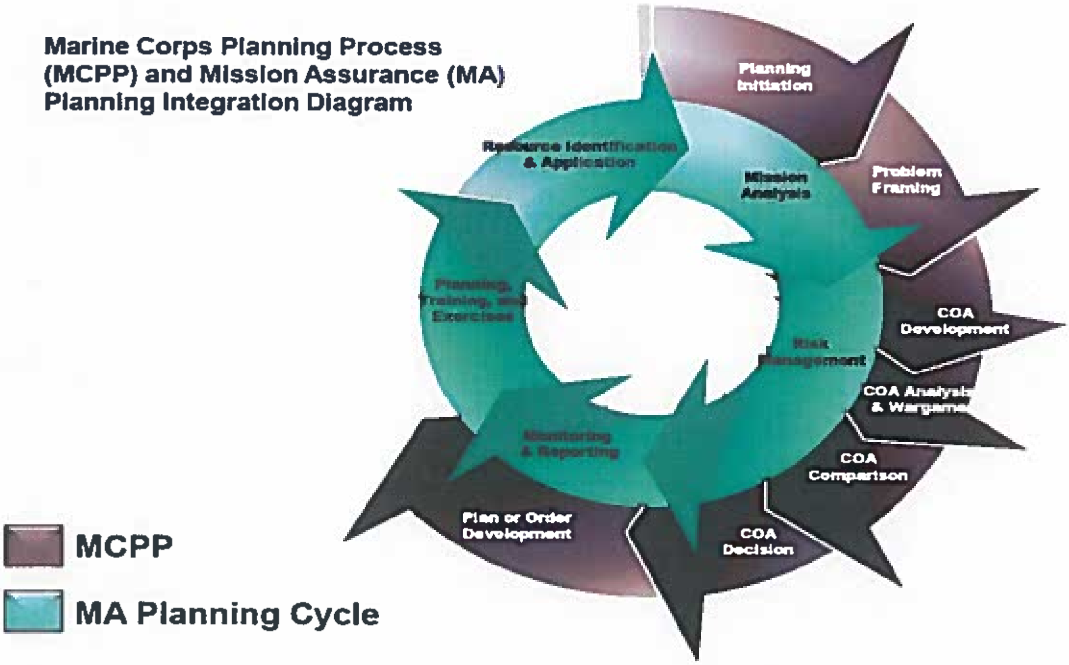
Marine Corps Planning Process
(MCPP) and Mission Assurance (MA)
Planning Integration Diagram
Planning Initiation
Resource Identification & Application
Mission Analysis
Problem Framing
Planning, Training, and Exercises
COA Development
Risk Management
COA Analysis & Wargame
Monitoring & Reporting
COA Comparison
Plan or Order Development
COA Decision
MCPP
MA Planning Cycle

Figure 1. MCPP and MA Planning Integration Diagram

c. Proper planning and Course of Action (COA) development that eventually produces the Letter of Instruction, Operations Order (OPORD), Task Order (TASKORD), or AT plan for deployments, operations, and exercises, should incorporate all relevant Force Protection RM requirements.

d. Protection programs, such as AT, PHYSEC, CIP, etc., must be adequately considered in the COA Development, Comparison and Decision phases of the MCPP.

e. The below questions should be addressed as part of the MCPP process, with COAs that reduce risk to mission accomplishment:

(1) Has the staff identified risk(s) in the problem-framing phase of the MCPP?

(2) Has the MAGTF concept of operations been adjusted to address the risks identified in the RA performed in support of OPORDs and exercises?

(3) How are criticality, threats/hazards, and vulnerabilities reflected in the unit's MCPP efforts? These terms are further explained in this section.

2. <u>Risk Management (RM) Process</u>. RM is a process used to identify, assess, and mitigate risk, and then enable decision making that balances risk and cost with mission benefits. RM allows the commander to decide how best to employ limited resources and security measures in order to reduce or mitigate risk, or, where further reduction and mitigation is not possible, acknowledge risk, which is then weighed against the benefits gained as a result of mission execution. Risk Management consists of two core activities: Risk Assessment and Risk Planning, as depicted in Figure 2 below.

MCMAA Risk Management Process

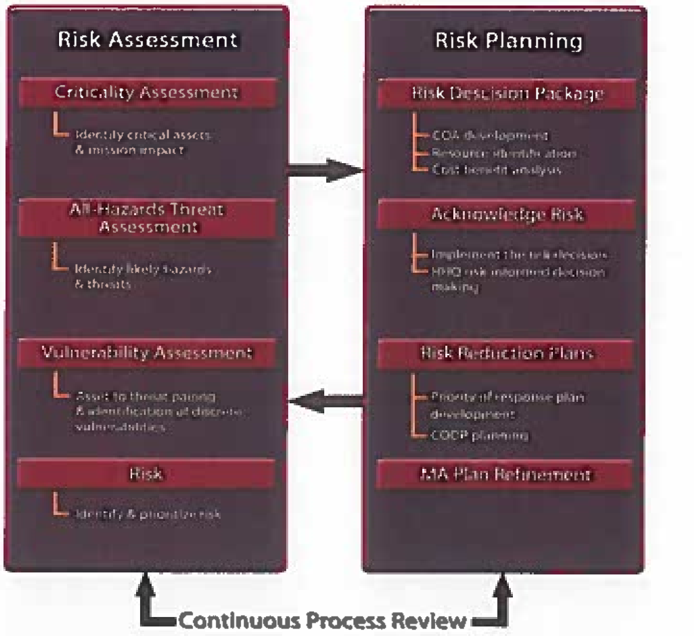
Risk Assessment
Criticality Assessment
Identify critical assets & mission impact
All-Hazards Threat Assessment
Identify likely hazards & threats
Vulnerability Assessment
Asset to threat pairing & identification of discrete vulnerabilities
Risk
Identify & prioritize risk
Risk Planning
Risk Descision Package
COA development
Resource identification
Cost benefit analysis
Acknowledge Risk
Implement the risk decisions
HHQ risk informed decision making
Risk Reduction Plans
Priority of response plan development
COOP planning
MA Plan Refinement
Continuous Process Review

Figure 2. Risk Management Process

a. <u>Risk Assessment (RA)</u>. A RA involves the collection and evaluation of data concerning the criticality of the assets based on mission impacts, probable threats and hazards, and degrees of vulnerability in order to determine the overall risk posture of the asset. A RA incorporates three core components: criticality assessment, all-hazards threat assessment, and vulnerability assessment.

(1) Criticality Assessment (CA). A CA is an assessment of the total impact (failure or severe degradation) upon the execution of missions or functions supported by an asset, should that asset be unavailable for any reason. More specifically, the CA will identify assets whose degradation or destruction impacts the command's ability to execute its assigned mission or functions, as well as the mission impact or consequence from loss of assets for supported missions. Commanders are required at minimum, to conduct an annual CA utilizing the following process steps: 1) identify missions, functions and associated standards and conditions for mission/function execution; and 2) identify assets whose loss or unavailability will result in mission failure or severe degradation (mission impact).

(a) Mission Analysis. The mission analysis provides the core foundation for the Critical Asset Identification Process (CAIP). The overall objective of mission analysis is to gain an understanding of the specific missions that are being executed by a command, as well as how those missions are then being executed. The output of this analysis will identify an inventory of assets associated with the execution of each mission or task assigned to a command. This asset inventory represents a starting point for the execution of the CAIP to identify assets critical to mission execution. Mission analysis cannot be performed satisfactorily without close coordination between subordinates, tenants, host installations, and other key stakeholders.

(b) Commander's Guidance. Commander's guidance is utilized to enable the development of a mission statement, help understand the scope or parameters of required mission execution, and ultimately support the identification and prioritization of critical assets, based on their impacts to supported missions. Utilizing command-approved Mission Essential Tasks (METs) or Mission Essential Functions (MEFs), together with their associated conditions, standards, and/or core functions, commanders shall identify and validate assets that, if degraded or unavailable for any reason, would impact the command's ability to execute assigned missions, tasks and functions. Assets can be personnel, equipment, facilities, information, information systems, infrastructure, and supply chains, which support the execution of the command's mission and associated critical functions. The CAIP must be used to conduct the CA. In addition, there are other assets that may not be critical to the execution of the mission or function, which may be identified during the criticality process and included in the overall RA. For example, non-critical assets could include high-population, mass-gathering facilities such as chow halls.

(c) Asset Identification. There are three major sub-processes involved in identifying critical and non-critical assets, all of which are outlined in the DoD and Marine Corps CAIP. The first involves analysis of command-approved missions, tasks and/or functions to identify Task Critical Assets (TCAs). The second involves analysis of each TCA to identify any related Supporting Infrastructure Critical Assets (SICAs). The third involves the analysis of each SICA to identify any further SICA(s), going at least one node outside of the fence-line or "span of control". During this analysis, baseline elements of information must be collected for each asset and entered into the MCCAMS. Both DoD and the Marine Corps directed the use of the CAIP as the methodology to be used to identify two categories of assets - those that are critical to the execution of missions, tasks and core functions, and those assets that are not critical, but are likely targets for terrorists (e.g., mass gathering facilities), regardless of whether the asset is owned by the Marine Corps, other DoD components, governmental entities, or the private sector. The latter is achieved primarily through installation MA processes and supported by the tenant organizations.

(d) Asset Criticality Rating. Aligning one or more missions and related mission impacts to an asset will produce a criticality rating for that asset. This rating reflects an evaluation of the total mission impact an asset may have on all missions, tasks and functions supported by that asset. This criticality rating is produced by use of either the MCCAMS (primary) or Marine Corps Asset Prioritization Methodology (MC-APM) tool (supplemental), when mission and mission impact data are populated accordingly. Along with threat/hazard and vulnerability ratings, the criticality rating contributes to producing a risk rating for an asset.

(2) All Hazards Threat Assessment (AHTA). Execution of the RM process is also requires an assessment of the threat and hazard environment in which Marine Corps forces operate and in which these missions are executed. The development of an AHTA will accomplish 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 and thus enabling a prioritized analysis. An AHTA must be conducted and/or updated and validated annually, tailored to the local environment, while ensuring all available threat and hazard information is integrated to meet the command's efforts to manage risk to missions, personnel, and assets. The AHTA also supports a consistent view of the threat/hazard (T/H) environment to support protection-related programs and response planning - i.e. by codifying the postulated threat(s). A collaborative effort among the membership of the FPWG and TWG will be required to develop the AHTA. The AHTA will also be based on the fusion of information (strategic, operational, and tactical). 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 other factors being equal. As part of the command RM process, commanders shall develop an integrated and prioritized T/H matrix that reflects the likelihood of assessed threats and hazards.

Example 1

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

Integrated and Prioritized Threat & Hazard Matrix

Installation / Site Name	Threat / Hazard Name	Assessed T/H Probability Rating
Camp Zebra	Flooding - Hurricane	Critical .80
	Explosive – 220 lb. VBIED	High .60
	Aged Equipment – No Spares	Medium .47
	Electromagnetic Pulse	Low .05

Based on work done to assess each individual threat/hazard scenario, an integrated and prioritized threat/hazard matrix can be developed for the entire installation.

Figure 3. Individual Threat/Hazard Analysis Data Matrix

(a) Threat and Hazard Analysis. An analysis shall be conducted to identify a baseline of T/H analysis that could adversely impact command assets (see Figure 3). When discussing execution of vulnerability assessment, the assessor must align one or more identified threats/hazards to one or more vulnerabilities of asset(s) that could be exploited by the threat or hazard. The results of this annual AHTA analysis must be integrated into all aspects of the RM process.

(b) Threat and Hazard Probability Ratings and Definitions. Once a baseline of threats and hazards has been identified, the assessor must conduct an analysis to determine the likelihood or probability of occurrence of each threat and hazard. There are four categories of T/H probability ratings: critical, high, medium, and low. The use of these ratings and definitions will facilitate the uniform assessment of the likelihood or probability of occurrence of any individual threat or hazard. Probability is defined as the estimate of the likelihood that a threat will occur.

(c) Threat/Hazard Ratings

1. Low (.01 to .25): Indicates little or no credible evidence of a threat to the asset or the immediate area where the asset is located.

a. For the identified threat, there is little or no credible evidence of capability or intent and no demonstrated history of occurrence against the asset or similar assets.

b. For the identified hazard, there is a rare history, or no documented history, of occurrence in the immediate area or region where the asset is located.

2. Medium (.26 to .50): Indicates a potential threat to the asset or the immediate area where the asset is located. Also indicates there is a significant capability with low or no current intent, which may change under specific conditions and low or no demonstrated history.

a. For the identified threat, there is some evidence of intent, but there is little evidence of a current capability or history of occurrence, but there is some evidence that the threat could obtain the capability through alternate sources. Alternatively, the identified threat evidences a significant capability, but there is little evidence of current intent and little or no demonstrated history.

b. The identified hazard has a demonstrated history of occurring, on an infrequent basis, in the immediate area or region where the asset is located.

3. High (.51 to .75): Indicates a credible threat against the asset or the immediate area where the asset is located.

a. The identified threat has both the capability and intent, and there is a history that the asset or similar assets are, or have been targeted on an occasional basis.

b. The identified hazard has a demonstrated history of occurring on an occasional basis in the immediate area or region where the asset is located.

4. Critical (.76 to 1.00): Indicates an imminent threat against the asset or the immediate area where the asset is located.

a. The identified threat has both the capability and intent and there is a history that the asset, or similar assets, are being targeted on a frequent or recurring basis.

b. The identified hazard has a demonstrated history of occurring on a frequent basis in the immediate area or region where the asset is located.

(d) Threat/Hazard Categories

1. Human-caused intentional threats include insider threat, cyber-attack, active shooter/lone offender, foreign intelligence threat, terrorism (to include domestic terrorists, transnational terrorists, and terrorist use of CBRNE), crime (to include non-violent crime, violent crime, gang activity and narcotics), and conventional/strategic military and civil disturbance.

2. Hazards are broken down into three categories: natural hazards, accidental events, and technologically-caused events.

a. Natural Hazards. Natural Hazards include geological, meteorological and biological. Geological categories include volcanos, tsunamis, earthquakes, and landslides. Meteorological categories include hurricanes, tornados, drought, winter weather, fire, extreme heat, lightning, hail, wind, rain, and flooding. Biological categories include diseases that impact humans or animals such as plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome, pandemic disease, bovine spongiform encephalopathy, etc.

b. Accidental and Technologically-Caused Events. Accidental events can cause disruption to the operation of assets, as well as the execution of missions supported by those assets. Accidental events can take many forms, such as those that result from human error (man-made), to those accidental events that may be caused by technology or technological failures. Incidence ranges and frequency must align with the hazard probability definitions, (low, medium, high, and critical) to determine overall probability rating. Technologically-caused events include aging assets and infrastructure that are past their normal life cycle and fail in some way; equipment failure caused by power surges or "dirty" power; equipment overheating (such as servers when Heating, Ventilation, and Air Conditioning (HVAC) system components fail); or software bugs that disrupt systems and networks. Statistics are gathered onsite at specific locations and generally are not available from national databases.

(e) Sources of Threat Assessment Data. DC, PP&O PS has established a detailed list of authoritative sources that support the development of the AHTA. The AHTA methodology can be found on the Headquarters Marine Corps (HQMC) Mission Assurance Assessment SharePoint at https://ehqmc.usmc.mil/org/ppo/PS/PSM/MAAT/Shared%20Documents/Forms/AllItems.aspx.

(3) Vulnerability Assessment (VA). A VA is an important subset of the RA process. The VA answers the basic question, "what can go wrong should the asset be exposed to threats and hazards of concern?" A VA involves identifying the characteristics of an asset that could cause it to suffer degradation or loss (incapacity to perform its designated function), as a result of having been subjected to one or more threats or hazards. More

specifically, a VA is a systematic examination of the characteristics of a system, asset, application, and its dependencies, in order to identify vulnerabilities that could be susceptible to the effects of threats or hazards. The VA must be conducted by a team of subject matter experts with backgrounds in different functional areas such as PHYSEC, AT, CIP, IA, and CI. VAs shall be conducted as follows:

(a) Identify and assess all vulnerabilities to the installation, facilities and assets, to specifically include all identified critical assets. Vulnerabilities can result from a wide variety of factors such as design and construction flaws, environmental factors, proximity to other structures or systems, factors influencing accessibility, personal behavior of people working in or around the assets, or operational practices associated with the assets or the installation. Vulnerabilities can also be a function of vulnerabilities to other assets or areas that are not in close proximity to the asset. For instance, vulnerabilities in access or perimeter control may lead to an adversary gaining access.

(b) Align specific threats and hazards to asset vulnerabilities. A threat-vulnerability pairing is conducted to link likely threats and hazards to specific asset vulnerabilities that may be susceptible to a given threat or hazard. This process is crucial because individual assets may have varying degrees of vulnerability to with respect to specific threats or hazards. Pairing a threat or hazard with an asset vulnerability will allow for greater precision and understanding of individual threat susceptibility. This, in turn, will support the preparation of effective risk reduction plans designed to lower overall risk by incorporating and addressing both T/H and vulnerability analysis in those plans.

(c) Identify degrees of vulnerability. When assessing and identifying vulnerabilities, the assessor must make a judgment call concerning the significance or degree of an identified vulnerability. For example, lack of standoff around a high population building may be identified as a vulnerability based on Unified Facilities Criteria (UFC) requiring 18 feet of standoff distance with an actual standoff distance of 17 feet. In this particular case, the significance or degree of vulnerability would be rated relatively low, as would the impact of exploiting that vulnerability from a threat such as a 220 pound Vehicle Borne Improvised Explosive Device (VBIED) that the UFC requirement was designed to address. Identifying the degree of vulnerability helps establish a vulnerability score, which, in turn, supports the establishment of an overall RA rating. Degrees of vulnerability are defined in the MCCAMS and MCARA tools.

(d) Vulnerability Rating Definitions

1. Low (.01- .25): Indicates multiple effective layers of integrated countermeasures are in place and there are no known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to the asset.

2. Medium (.26 to .50): Indicates multiple effective countermeasures are in place; however, at least one known weakness exists through which adversaries, natural hazards, or accidental disruption would be capable of causing loss of or disruption to the asset.

3. High (.51 to .75): Indicates some effective countermeasures are in place, but multiple known weaknesses exist through

which adversaries, natural hazards, or accidental disruptions could be capable of causing loss of or disruption to the asset.

4. Critical (.76 to 1.00): Indicates minimal effective physical, design, technical, procedural, or behavioral countermeasures are in place, and many known weaknesses through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of, or disruption to, critical assets.

(e) Risk Rating. Based on the values produced from the CA, AHTA, and VA, a RA rating or score is established. Risk is determined by the following equation: criticality rating x T/H rating x vulnerability rating = risk rating. MCCAMS provides an integrated set of metrics to enable establishment of a risk rating. The risk rating is produced for each specific T/H and vulnerability/asset pairing of data.

b. Risk Planning (RP). The objective of the RM methodology is to enable the management of risk based on a holistic approach that populates across individual programs and capabilities such as AT, CIP, PHYSEC, CBRN, COOP, etc. Since some risk will always be present, RM seeks to achieve an acceptable level of risk in the execution of a command's missions and functions. While the RA process seeks to identify and evaluate risk of loss to assets based on an asset's criticality (mission impact), the probability of threats and hazards occurring, and associated degrees of vulnerabilities, RP is the process of determining options or courses of action to reduce the risk of loss to the asset, and thus reduce impact on mission execution. To support the development of risk reduction plans, commands can leverage elements of the FP governance process such as the FPEC and FPWG, or establish a risk reduction planning team consisting of experienced personnel with requisite expertise. Risk reduction planning involves two areas of implementation: risk reduction plan development and acknowledgement of risk.

(1) Risk Reduction Planning. Commanders shall implement effective and efficient risk reduction courses of action, whenever possible. Examples include, but are not limited to, PHYSEC measures, personal protection measures, cyber security measures, and/or building redundancy in assets critical to mission execution. Risk planning courses of action can involve efforts to implement risk reduction measures before an event occurs that could adversely impact missions and assets, as well as measures that are implemented after an event, or after receipt of warning of an impending event.

(a) Risk Decision Package (RDP). RDPs are essentially one or more courses of action designed to address and reduce identified risk to assets and missions. RDPs should be developed to assist commanders in risk decisions. RDPs must be developed and documented in MCCAMS for all Defense Critical Assets (DCA) and Tier I-III critical assets, at a minimum. The following elements must be included in a RDP:

1 Executive Summary

2 Mission Details

3 Threat/Hazard Details

4 Asset/Vulnerability Details

5 Initial Risk Rating

6 Proposed risk reduction course of action and the estimated reduction in risk (revised risk rating) anticipated to be accomplished by executing the course of action.

(b) Acknowledgement of Risk. A commander may decide to acknowledge risks to assets, where appropriate, rather than dedicating resources to reduce identified risks. Generally, risk may be acknowledged by the commander when the impact of loss or the anticipated reduction in risk is not significant enough to justify the cost or the minimal benefit of the proposed risk reduction countermeasure. In addition, the commander may acknowledge risk, temporarily, where resources are not currently available to support desired risk reduction courses of action. In these cases, documenting acknowledgement of a risk in MCCAMS is also the first step to identifying such a risk up the chain of command.

1. Higher Headquarters Risk-Informed Decision Making. HHQ risk-informed decision making involves a chain-of-command-driven process in which a risk-related unfunded resource requirement is submitted to HHQ for funding consideration. Commanders must prioritize proposed risk reduction courses of actions that cannot be implemented at their level. When effective and efficient countermeasures cannot be implemented immediately, commanders must prioritize any remaining risks to compete for funding solutions.

2. Marine Corps MA-Enterprise (MCMA-E) Risk Management. The MA staff, at all levels within the Marine Corps, continuously updates their RA to alert the commander to emerging threats, and associated vulnerabilities, which must be addressed. At the installation level, typical factors to consider in the development of risk reduction plans include, but are not limited to, the following: PHYSEC and access control; information security and information assurance; personnel security; facility design; critical asset and infrastructure resilience and redundancy; emergency response planning and resourcing; and training and exercises.

(c) Other Risk Reduction Planning and Coordination Considerations

1. Capability Assessment. A capability assessment is a command, or unit-level evaluation designed to identify capabilities for responding to an event, whether caused intentionally or by a natural or unintentional man-made disaster or hazard. Commanders shall conduct capability assessments and consider contingency planning activities. Planners should make full use of their capability assessment when developing courses of action that will rely on the command's response capabilities as an integral part of the risk reduction plan.

2. Confirm Stakeholders, Prioritize Risk, and Identify Options. It is important to identify asset owners, mission owners, and other stakeholders that have a vested interest in reducing risk to missions and assets. The MCCAMS shall be used to prioritize risk to assets, as well as to prioritize impact of critical assets on all missions supported by the asset. These tools and processes generate priority values for impact to missions and the identification of risk. Risk reduction efforts shall focus on obtaining optimal risk reduction and the most effective and efficient use of resources.

3. Analyze Options and Determine the Best Approach. This step focuses on analysis of one or more courses of action to determine the action that represent the best fiscal options. Use of the MCCAMS will assist

commanders in analyzing options and determining the best courses of action to implement. Executive level planning groups shall include a cost-benefit analysis to balance risk to the asset and/or mission with the resource requirements necessary to achieve a reduced level of risk.

4. Develop and Coordinate the Risk Reduction Plan. This step requires that a Plan of Action and Milestones (POA&M) be developed outlining details of what needs to be done, how it is to be done, who is involved, and the timeframe to complete implementation of the Risk Reduction Plan. The plan must include details concerning the asset, the threats/hazards the asset is vulnerable to, information concerning the command's decision to reduce risk, and the resource requirements needed to execute the plan.

5. Implement the Risk Reduction Plan. Once the plan is approved, track the milestones developed in the above POA&M and measure success. Plan effectiveness can be assessed during the command's annual exercise, or by a HHQs RA, such as an MCMAA.

(d) Required Risk Reduction Plan. Commanders shall coordinate with their host installations for the inclusion of their asset response priorities. Each I MEF mission critical asset shall have a COOP to ensure continuous mission capability and execution. These COOPs also serve as asset reconstitution plans.

(2) Process Review. Assessing risk and conducting risk reduction planning should form part of a continuous cycle. While there are annual requirements to conduct RAs, a command's missions, threats/hazards, and vulnerabilities can change at any time, and should be re-evaluated, as these changes occur, to update the identified risk to the command's missions and assets.

(a) Update Critical Asset Risk Profile/Rating. Critical asset risk profiles/ratings shall be updated annually or when changes in criticality, threats/hazards, or vulnerabilities occur. Significant increases in risk profiles/ratings may require changes in risk reduction plans or strategies and resource generation priorities.

(b) Program Review. Once the annual RM process is complete, it is essential that a thorough review of the overall process be conducted. This is typically done during the annual program review.

(c) Refine RM Plan. Necessary revisions to the RM plan can be documented and initiated during this portion of the process. As noted, the RM process must be executed as a cycle. By using this framework, revisions can be made as required, and the MA program can be continually improved.

(d) Coordinate with Stakeholders. When applicable, commanders shall ensure stakeholders in the military and local communities are involved in the process review. This collaboration will ensure that supporting plans align with the RM process. Stakeholders from the local community can also identify strengths and weaknesses, focusing on collaboration between the military and civilian agencies. Interfacing and coordinating preventive and/or response measures with local stakeholders may ensure a more robust security and response posture; however, coordination with local stakeholders should never be done at the risk of endangering DoD personnel, assets, or Marine Corps missions.

(e) Exercise and Modify Risk Reduction Plans. The final stage in the RM process review is to exercise risk reduction plans that have been implemented during annual FP/MA exercises, and make adjustments, as needed.

Critical Infrastructure Protection (CIP)

1. General. Critical Infrastructure Protection (CIP) is an integral part of the FP program; as such, CIP supports and synchronizes with the other FP program elements and operations. CIP provides a consistent, unifying structure of integrating Risk Management (RM) in support of mission critical assets and supporting infrastructure to facilitate continuity of operations. Understanding the operational dependencies of I MEF critical assets on related infrastructure is critical to overall Force Protection efforts. It is paramount to preserve the ability to plan and deploy forces and capabilities as directed by COCOMs, either in CONUS or OCONUS.

a. There are insufficient resources (human, material, financial) to mitigate/remediate all risk to mission critical assets; thus, a uniform, comprehensive RM program must be implemented to inform commanders and decision makers on how best to allocate these limited resources in relation to mission impact.

b. The contents and processes discussed herein also apply OCONUS in support of geographic and/or functional COCOMs.

c. Intelligence support to CIP must supplement periodic AHTAs coupled with procedures for warning and responding to impending threats. The host installation ATHAs, developed annually with assistance from the Marine Corps Mission Assurance Assessment Team (MAAT), can be used to support the I MEF risk analysis process when in garrison. OCONUS these efforts must be informed by the intelligence assessment(s).

2. Purpose. The CIP program identifies, assesses, prioritizes, and protects mission critical assets to ensure the successful deployment/employment of forces and capabilities in the execution of global missions.

a. To increase the likelihood of mission success for I MEF commands, full spectrum, protection responsibilities and activities must be performed in-depth by all hands. Through the implementation of CIP, the command shall take the necessary action to enhance security and resilience for personnel, facilities, mission critical assets, and supporting infrastructure in an all-threats/hazards context, in accordance with the references. Thus, the I MEF CIP must focus on identifying mission critical assets and their supporting infrastructure, analyzing the impact their loss would have on our missions, and executing a RM program that reduces the risk to acceptable levels. This effort will require detailed planning, coordination, and collaboration with all stakeholders, especially MCI-W/MCB CAMPEN and other host installations upon which I MEF units are located.

b. The end-state of CIP is the attainment of optimal protection that preserves I MEF's mission execution and continuity of operations. An expectation of avoiding all risk is unrealistic, and to strive for this objective would likely have an adverse impact on I MEF's ability to accomplish assigned missions. Thus, commanders must conduct RM, while keeping in mind the need to balance risk to their forces against mission imperatives.

3. Process and Requirements

a. I MEF CIP will be centrally executed and managed at the MEF/MSC CE levels. MSCs shall coordinate with their subordinate commands for the execution of CIP, and the MSCs shall forward CIP information requirements to the MEF G-3 FP Officer for management. The I MEF CIP Officer shall be responsible for entering and maintaining all CIP data within MCCAMS.

b. I MEF CIP will address five primary areas/activities: Mission Analysis; Risk Management; Monitoring and Reporting; Planning, Training, and Exercises; and Resource Identification and Application. These areas/activities shall be accomplished on an annual basis and in close coordination with host installation commands and other tenants, as applicable. Moreover, the areas/activities shall be executed in a phased manner, in accordance with the following milestones: Mission Analysis - complete First Quarter Fiscal Year (FY); RM - complete by end of Third Quarter FY (completion of this milestone is dependent on completion of the asset verification and validation process for each mission critical asset); Resource identification and application - complete during Fourth Quarter FY. This serves as a general guideline while the monitoring/reporting, planning, training, and exercise activities are continuous and ongoing throughout the FY.

c. The following addresses the CIP areas/activities to be executed:

(1) Mission Analysis. The Critical Asset Identification Process (CAIP) is the identification and analysis of I MEF missions, core capabilities, and METs, with their associated conditions and standards, to identify Task Critical Assets (TCAs) and their associated Supporting Infrastructure Critical Assets (SICAs). Specifically, CAIP requires the CIP Officer to do the following:

(a) Obtain METS from the Defense Readiness Reporting System (DRRS) Officer and review the minimum performance standards and conditions necessary to achieve mission success. The conditions and standards serve to focus the analysis to determine single points of failure for TCAs.

(b) Work with the appropriate SME to analyze the METs, in order to identify specific TCAs and SICAs associated with the execution of each MET. The analysis will examine those assets whose degradation or destruction impacts the command's ability to execute its assigned mission or function. Capture the TCA Basic Elements of Information (BEI) per reference (m). TCAs and the respective BEI information shall then be entered into MCCAMS to support RM activities and information sharing. Once the BEI is entered, the identified TCAs shall be associated to their command METs, identified within the MCCAMS Mission Folder.

(c) Coordinate with the host installation(s) MA CIP Officer for SICA identification and information-interdependency analysis. Associate the SICA(s) to the TCA(s), as required, to reflect appropriate asset dependency in MCCAMS.

(d) As the mission owner, I MEF G-3 FP will facilitate completion of the TCA validation process, utilizing MCCAMS. Once the asset is fully verified and validated up the chain of command, the "criticality algorithm" within MCCAMS will generate a criticality score for each TCA fully validated in the system. This criticality score shall be used in conjunction with the TCA RA and the overall TCA risk score.

(2) Risk Management (RM). RM is discussed in Enclosure (2) of this order. The following will further elaborate on how CIP is integrated with RM:

(a) Risk Assessment (RA). RA involves the collection and evaluation of data in three core areas: criticality, threat/hazards, and vulnerability. Based on the values produced from the three core areas, a risk assessment rating, or score, is produced that permits prioritization of TCAs by risk-to-mission execution/mission impact. TCA criticality will be determined in MCCAMS, through an internal calculus, by the association of the identified TCA to the METs and/or functions it supports. Utilizing the AHTA, each applicable threat/hazard rating shall be entered for the TCA(s) in MCCAMS. Lastly, the TCA owner/asset SMEs shall conduct a systematic examination (assessment) of the characteristics of the TCA(s) to identify vulnerabilities that could be susceptible to the effects of threats and hazards. This VA shall consider a wide variety of factors such as: design and construction flaws; environmental factors; proximity to other structures or systems; factors influencing accessibility; personal behaviors of people working in or around the TCAs; or operational practices associated with the TCAs. Once the VA is complete, a VA score is determined by using the degrees of vulnerability definitions contained in reference (m) and in MCCAMS. Select a VA score for each TCA entered into the system. When all core area data and scores are entered, MCCAMS will calculate an overall risk rating score for the TCA. This score shall then be used for TCA risk planning, which is the next core activity of RM.

(b) Risk Planning. Risk planning is the process of determining options and actions to reduce the risk of loss to the TCA(s), and thus reduce the impact on mission execution. The options/action steps include mitigating the effects the threat will have on the TCA, mitigating the effects of loss once the threat/hazard event occurs, reconstituting the TCA's capabilities after loss or disruption, acknowledging the risk, or simply transferring the risk decision to a higher echelon of command. Risk planning also includes remediation. Remediation focuses on identifying countermeasures that can be implemented before undesirable events, or attacks, occur that could exploit the identified vulnerabilities. To complete risk planning, I MEF G-3 FP shall use selected members of the FPWG, and other SMEs as needed, to develop Risk Reduction Plans. To support risk reduction planning, Risk Decision Packages (RDPs) shall be developed to assist the commander, or his/her designated representative, in making risk decisions.

(c) A process review can be considered as the audit process. Once the RA is complete, it is essential that a thorough review of the overall process be conducted. This is normally done during the Annual program review. The review components that must be completed by I MEF G-3 FP include: identify RA weaknesses based on results of external assessments or from exercise results; refine plans to address lessons learned; coordinate with stakeholders; and train and orient the FPWG on process review results.

(3) Monitoring and Reporting. This area/activity involves pre-event coordination associated with intelligence gathering and reporting; hazard identification and awareness; and monitoring and reporting of asset operational status. The goal of this area/activity is to achieve a fully integrated and coordinated common operating picture for CIP mission critical

assets up and down the chain of command. The following details specific actions to be accomplished in this area/activity:

(a) When operational, develop the Commander's CCIR with regard to CIP in order to guide intelligence collection efforts by appropriate intelligence agencies.

(b) Provide a list of command TCAs to host installation(s) for incorporation into their CIP planning and collaboration with the NCIS, and local/state/federal authorities and entities.

(c) Coordinate the completion of an annual AHTA for each command TCA to determine the likelihood, and mission impact, of the threat/hazard event occurring. Whenever possible, I MEF commanders should use their host installation's AHTA developed to support their RA process. Working closely with the host installation TWG, develop triggers that will require a change in the protection status of command TCAs.

(d) In accordance with current procedures and orders, notify HHQ of any changes to Tier I and II TCA operational readiness posture, within 24 hours, via an Operational Reporting Procedures-3 Serious Incident Report (OPREP-3 SIR). Additionally, use the proper means and format to inform the chain of command of any threat/hazards triggers being observed and identified necessitating a change in protection status.

(4) Planning, Training, and Exercises

(a) Planning. Planning activities must address the following regarding mission critical assets:

1. All Operations Plans (OPLANs) and orders must consider and plan for the availability and protection of TCAs. Execution of the MCPP will ensure that CIP equities are taken into consideration for the full range of military operations. In particular, CIP can be integrated when conducting analysis of missions, developing courses of action to meet mission requirements, and war-gaming courses of action against threats.

2. The working group format is the directed means for executing not only CIP planning, but also all FP planning activities. References (m) and (n) discuss the specific requirements and composition of the Working Groups. To execute CIP activities, the primary I MEF organizational execution framework will be the CIPWG. The CIPWG shall provide diverse expertise in developing issues, and courses of action, to address asset protection requirements. The CIPWG shall be integrated into the FPWG to the greatest extent possible in order to generate synergy with similar program requirements, to reduce administrative burden, and to gain efficiency. The CIP Officer shall develop a CIP agenda and capture actions/decisions/ pending issues in the minutes for each working group meeting.

3. As part of the planning process, the following planning activities must be completed: Threat/force protection planning to support the calculation of risk to TCAs; base operating support agreements; security and protection priority plans; all-hazards response plans; COOP; mutual aid, assistance, and support agreements for joint military-civilian emergency response activities at host installations and within the AOR (e.g., host nation bilateral security agreements).

(b) Training. The purpose of training is to build the organizational and individual competence needed to carry out CIP responsibilities throughout the command on a continuous basis. CIP training includes formal training, utilizing Mobile Training Teams provided by HQMC, and individual training, conducted by I MEF CIP Officers and other designated individuals. At a minimum, CIP training shall be given to I MEF CE FPWG members to prepare them for their duties. The training shall include an initial CIP orientation, CAIP, and CIP RM process. Whenever possible, CIP training shall be incorporated with other FP training (i.e., antiterrorism, COOP, etc.). This training can be accomplished using Computer Based Training via the Marine Corps Mission Assurance Support Tool, or the MarineNet website. The I MEF Force Protection Officer shall maintain a current list of these computer-based training offered courses.

(c) Exercises. Per reference (m), all commands are required to conduct a CIP inject exercise annually. An inject is an exercise (either full scale or seminar/table top) that exercises the risk response measures associated with a TCA, after a threat or hazard has hypothetically disrupted or degraded its capability or functionality. The OPFOR shall fulfill this CIP inject exercise requirement by incorporating their inject exercise objectives into the host installation's CIP inject exercise. Exercise objectives should focus on post-event CIP actions such as critical asset incident response, mitigation or COOP execution/reconstitution. CIP injects can be done as part of the host installation's full-scale exercise, or as part of a table-top/seminar exercise. CIP exercise after-action reports shall be uploaded into MCCAMS for information sharing across the Marine Corps.

(5) Resource Identification and Application

(a) As part of the risk planning and resource application process, I MEF G-3 FP shall identify and submit CIP funding requirements to the appropriate command comptroller, for prioritization and entry into the PPBES. Funding requests for risk response actions must be supported and prioritized based on TCA RDPs developed during the RM process. To facilitate project management, CIP funding requirements and application will be entered into MCCAMS, in the Projects Sub-folder contained in the RM Folder.

(b) CIP officers shall be aware of the milestones set by their financial managers/Comptrollers, during the PPBE process, to ensure critical information is provided, at the appropriate time, to the appropriate agencies for both programming future funding and executing the budget.

(c) Once funding is received, the CIP Officer must coordinate with the G-8, and the specific TCA owner, in order to ensure funding objectives are achieved in an appropriate and timely manner.

4. Information

a. MEF and MSC METs are maintained within the I MEF G-3. The MSC DRRS officer can also provide an updated list of MSC METs for use in completing CIP activities.

b. MCCAMS is the primary repository for CIP data. TCA data shall be entered/updated as soon as feasible, and will be reviewed not less than quarterly. The I MEF CIP officer shall coordinate with MARFORCOM for required access to MCCAMS.

c. When informing HHQs and COCOM(s) of disruptions or significant degradations in Tier I and II TCA readiness or status, utilize OPREP 3 procedures.

d. MA/CIP program reviews shall be conducted at the I MEF/MSC CE levels only. MARFORPAC shall conduct the I MEF G-3 FP program review, and the I MEF FP section shall conduct program reviews on the MSC CE FP programs.

5. CIP Officer Responsibilities

a. Develop, implement, and maintain effective CIP plans, in order to ensure that all CIP processes, areas/activities are completed, per established milestones and in accordance with the references.

b. Chair and train a CIPWG for program execution. This WG shall be integrated into the FPWG in order to facilitate information sharing, generate synergy, and reduce administrative burden.

c. Utilizing selected members of the CIPWG, execute the mission analysis area/activity for the I MEF CE. Identify TCAs and SICAs, associated with the execution of each command MET, with recommendations for verification and validation. Support the MSC mission analysis area/activity and provide SICA association for the identified TCAs.

d. Utilizing the CIPWG, execute RM for the identified TCAs and support completion of the MSC RM process. Identify a prioritized (based on risk to mission execution) list of TCAs and present RDPs for the highest priority TCAs for decision by the commanders and/or the FPEC. Coordinate with the host installation for the following support and information:

(1) AHTA

(2) NCIS support

(3) Support from local, state, and federal agencies

e. Coordinate with the host installation for the identification of TCAs and SICAs necessary to facilitate integrated RM and response planning.

(1) Identify, and share with host installations, the I MEF METs and core functions, and the I MEF TCAs, that are critical to the execution of those METs and core functions.

(2) Coordinate with host installations/host nations to identify base support agreements for SICAs that support I MEF TCAs and ensure their availability and protection through installation security and protection priority plans and agreements.

(3) Participate in the MCI-W/MCB CAMPEN CIPWG/MAWG.

(4) Coordinate I MEF participation in each installation CIPWG/MAWG by the senior I MEF tenant at each host installation.

f. Coordinate, and integrate, CIP security plans with COCOM CIP points of contact (POC), when deployed OCONUS. Coordinate and collaborate with the appropriate COCOM(s) CIP POC in order to identify supporting infrastructure networks, and supporting material and services, within the AOR, required to support MEF TCAs.

g. Enter and update I MEF CIP data pertaining to the execution of all CIP areas/activities into MCCAMS. The I MEF CIP Officer shall support and facilitate CIP-related data entry for the MSCs, in order to ensure standardization and continuity.

h. Complete all requirements for the area/activity of monitoring and reporting. Implement the Marine Corps Common Operating Picture-C4I Suite within the I MEF COC in order to facilitate FP situational awareness and information sharing during routine operations and crisis action events, or as directed. Until that time, coordinate closely with the host installation for C4I Suite information sharing.

i. Execute the planning, training, and exercise activities, as discussed in this section. Coordinate closely with the host installation to integrate the following:

(1) Formal training opportunities provided by external agencies and the conduct and monitoring of CIP training for MSCs.

(2) Response plans and emergency response priorities, to include the determination of personnel augmentation support to installations relative to changes in Force Protection Conditions.

(3) Planning and execution of annual CIP inject exercises in conjunction with the host installation annual MA/CIP exercise, and the consolidation of after-action items with the host installation's final After Action Report, in order to develop and execute a plan to rectify discrepancies or problem areas determined from the CIP inject exercise.

(4) The conduct of MA/CIP program reviews and higher headquarters MA assessments on installations where I MEF commands are tenants.

j. Submit a prioritized list of CIP risk response requirements (mitigation, remediation), via the AC/S G-3 and FPEC, to support the resource identification and application activity discussed in this section. Ensure this data is entered in the "projects" sub-folder, contained in the RM folder, within MCCAMS.

k. Monitor and update the operational status of I MEF TCAs affecting COCOM missions, and Marine Corps core capabilities and functions, in MCCAMS. Absent extreme circumstances, an update to changes in operational status of Tier I and II TCAs is required within 24 hours of a change in status. Incorporate procedures to report operational status changes to Tier I and II TCAs in existing OPREP reporting formats.

Resource Application

1. General. Generating resource requirements and acquiring additional resources to mitigate/remediate identified vulnerabilities is a key step in reducing risk. The limited availability of resources requires proper planning and justification of requirements. A realistic and affordable FY budget and procurement strategy must be developed that captures total life-cycle costs (staffing needs, training costs, logistics/maintenance, and replacement costs). FP requirements must be well defined, formally documented, and prioritized. The FY budget and procurement strategy should be derived from an analysis of asset prioritization, based on risk to mission and cost benefit analysis of courses of action, in order to reduce risk to an acceptable level, as developed during Risk Decision Planning. Several funding avenues are addressed in this Enclosure, and should be considered when developing budget and FP funding requests.

2. Determining Resource Requirements

a. The use of an asset prioritized list, based on risk-to-mission, is intended to help the FP Officer identify program needs so that funding can effectively address the most serious shortfalls.

b. Once FP requirements are documented and prioritized, the FP officer and Comptroller should work together to formulate a budget that addresses requirements, and identifies the specific resources needed, and the fiscal codes used, to program funding and track budget execution.

c. The FPWG/TWG shall analyze the asset-prioritized list, based on risk to mission produced during the RM process, to determine resource requirements. The FPWG/TWG shall consider all TTPs that may mitigate risks while understanding that the cost of mitigation measures must be fiscally achievable. Given limited resources and budgetary constraints, the FPWG/TWG shall provide commanders with alternatives for timely, cost-effective FP resources that still permit the successful execution of the plan. On-hand resources and mitigation measures must meet the minimum security requirements for baseline FPCONs.

3. Cost-Benefit Analysis. FP officers employ cost-benefit analysis twice in the risk and resource management processes: first, during consideration of executable mitigation measures with available resources; and second, in prioritizing resource requirements in a FPWG/TWG forum, along with other Program Managers. Cost-benefit analysis is an analytical tool used to weigh the total expected costs against the total expected benefits of one or more actions, in order to choose the most effective option. The cost should include more than monetary and resource expenses; it should also incorporate the reduction of risk from implementing the measure in the near term and the long term through the PPBE cycle. The residual risk from one measure should be compared to the residual risk of other potential mitigation measures to help determine which measures will provide the greatest impact. Employing a comprehensive cost-benefit analysis of each potential mitigation measure will assist the commander with managing risk and prioritizing funding requests.

4. Prioritizing Resource Requirements. Once requirements have been determined, the FPWG/TWG shall analyze the justification data (threat/hazard, vulnerabilities, asset criticality, FP program effectiveness and commander's risk), and prioritize requirements based on the most critical and important

needs. Resources required to mitigate a major or high-risk situation shall be given priority. Emphasis should be placed on acquiring resources that deter, detect, and defend against threats to areas of significant importance. Additionally, priority should be given to resource requirements needed to meet minimal security standards and to adhere to HHQ directives, standards, instructions, and regulations. While prioritizing resource requirements, the FPWG/TWG shall place each requirement in one of the four priority categories: Critical, High, Medium or Low.

a. A critical-priority resource requirement should include the majority of these criteria: a serious threat; an asset that is critical to the continuity of essential military missions; major vulnerabilities; and a lack of resources to execute baseline FPCON measures. A critical-priority resource requirement addresses an unacceptable risk in the top 20% of the commander's funding priorities.

b. A high-priority resource requirement should include the majority of these criteria: a serious threat; an asset that is critical to the mission; major vulnerabilities; and a lack of resources to execute baseline FPCON measures. A high-priority resource requirement addresses an unacceptable risk in the top 21-40% of funding priorities.

c. A medium-priority resource requirement should include the majority of these criteria: a moderate to high threat; an asset that is moderately critical to the mission; moderate vulnerabilities; and resources that may be needed to execute elevated FPCON measures. A medium-priority resource requirement addresses a considerable risk.

d. A low-priority resource requirement should include the majority of these criteria: all threat levels; an asset that is important to the mission; less significant vulnerabilities; and resources that would enhance/improve an FP program. A low-priority resource requirement usually addresses a low risk.

5. Documenting Resource Requirements. The requirements shall be formally documented, using FP/MA Assessment Benchmark requirements as justification to initiate the funding process. Resource requirements that address vulnerabilities are classified and cannot be listed in funding requests. Formally, clearly, and continuously documenting resource requirements, and maintaining records of the requirements at every level of command, is crucial to successfully compete for FP funding, and to leverage supplemental funding, should it become available on short notice.

6. Funding Sources. Once resource requirements are generated, prioritized, and documented, a realistic and affordable budget and procurement strategy shall be developed. Budget planning shall capture all life-cycle costs, including staffing needs, logistics, maintenance, and replacement costs. If the commander determines that the resource requirements cannot be funded locally, a funding request shall then be submitted to HHQs.

a. Planning, Programming, Budgeting, and Execution (PPBE) process. The PPBE process is the business cycle of allocating resources within the DoD. The PPBE process is cyclic and provides the mechanisms for decision-making and the opportunity to reexamine previous decisions in light of changes in the environment (e.g., evolving threat, changing economic conditions). The ultimate objective of the PPBE is to provide commanders with capabilities that include the best mix of forces, equipment, and support, attainable within established fiscal constraints, to accomplish their mission. Resource planning and programming is accomplished through the Program Objective Memorandum or (POM) process, and budgeting and execution is accomplished during the execution of the Five Year Defense Plan (FYDP). It is important for FP officers to be aware of the budget and data call timelines, during the PPBE process, to ensure critical information is provided at the appropriate time, to the appropriate agencies, for both programming future funding and executing the budget. Figure 5 is a sample budget/data call timeline.

FISCAL YEAR											
OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP
Continuing Resolution Authority or Current Year Budget Distribution			Current Year Mid-Year Review			Results of Mid-Year Review		Close-Out and Year-End Sweep			
Deficiencies are updated monthly during current year											
Unfunded Program List (Current Year + 1)			Initial Review of next FY Baseline			Supplemental Data Call			Deficiencies		
Program Objective Memorandum / Program Review (Future Years)											

Figure 5. Sample Budget/Data Call Timeline

b. Program Objective Memorandum (POM) Process. The POM process is the primary method of programming resources. The POM process does not address the current year funding; rather, it addresses the programming of funding execution two years in advance of the current year. For example, planning and submission for POM 18 is done in FY16. POM submissions are evaluated by Program Evaluation Boards (PEB) for each type of appropriation and Marine Corps Programming Codes (MCPC), such as MCPC 630104, Security. POM nominations are submitted by the MARFOR level G8 and or the appropriate HQMC Program Manager.

c. Universal Needs Statements (UNS). The UNS identifies operational enhancement opportunities and deficiencies in capabilities. Opportunities include new capabilities, improvements to existing capabilities, and elimination of redundant or unneeded capabilities. There are generally two types: Deliberate Universal Needs Statement (D-UNS) and an Urgent Universal Needs Statement (U-UNS).

(1) A D-UNS is a mechanism to communicate future desired capabilities (equipment fielding within 3-5 years of submission) to HQMC for consideration and possible entry into the Expeditionary Force Development System (EFDS), and other deliberate requirements planning and resourcing processes. The D-UNS attempts to identify capability gaps, recommended solutions or operational enhancement opportunities, which include new capabilities, improvements to existing capabilities, and elimination of redundant or

unneeded capabilities to capture both current and future needs of the Marine Corps, that are immediately required to support ongoing contingency operations.

(2) The U-UNS process is to provide rapid acquisition of a capability to meet an urgent requirement (equipment fielding within one year of submission) in support of combat and contingency operations that threaten mission accomplishment or are life-threatening.

f. Combatant Commander Initiative Fund (CCIF). The primary focus of the CCIF is to support unforeseen requirements critical to COCOMs' joint warfighting readiness and national security interests. The strongest candidates for approval are initiatives that support COCOM activities and functions, enhance interoperability, and yield high benefits at a low cost. The funds do not subsidize ongoing projects, supplement budget shortfalls, or support routine activities. Initiatives submitted for funding under CCIF must fall under one of the following authorized activities: joint exercises and force training; contingencies and selected operations; civil and humanitarian assistance; command and control; military education and training; or personnel expense of defense personnel for bilateral or regional cooperation programs.

7. Types of Appropriations

a. Operations and Maintenance (O&M). O&M appropriation provides funding resources for Marine Corps missions, functions, activities, and facilities. This appropriation also finances the OPFOR sustainment requirements; depot maintenance; base operating support costs; training and education requirements; Marine Corps headquarters administration and Service-wide support requirements; and defense commissary operations. The Marine Corps is authorized to use annual O&M funds for construction projects costing less than $750,000 ($1.5 million to correct a life-threatening condition or for new construction and $3 million for maintenance and repair of existing facilities).

b. Procurement. Procurement is a three-year appropriation that finances the purchase of tactical equipment, combat vehicles, communications and electronic equipment. Procurements made with non-appropriated funds should aid in obtaining products and services through purchasing and contracting operations.

c. Military Construction (MILCON). MILCON funds are obtained through a formal process using DD Form 1391, FY Military Construction Project Data, and must be approved by Congress under applicable procedures. These funds are used to pay for expenses related to the construction of buildings, locks, dams, and roadways.

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

8. Resource Application Support. Throughout the resource application process, FP Officers shall work closely with special staff offices.

a. Comptroller. Comptrollers acquire, control, and certify funds in accordance with fiscal law. As FP Officers work to articulate and justify the requirements, the Comptroller is responsible for identifying the correct appropriation and funding amounts, and submitting the funding requirement at the appropriate time to the organization responsible for funding the requirement.

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

c. Contracting. Competing requirements make demands on limited resources. A shortage of resources generally results in a need for some form of contracting to meet a mission and fulfill necessary requirements. The joint mission of resource management and contracting is to ensure the proper allocation of scarce resources across a theater of operations. With command approval, resource management allocates funds to contracting, enabling it to obtain those supplies, services, and construction that a unit does not currently possess but must have to perform its mission. The I MEF Operational Contracting Support (OCS) Office will establish the appropriate review boards to ensure all requirements are properly developed, coordinated, reviewed, prioritized and routed through the contracting process.

Physical Security (PhySec)

1. PhySec Program

a. PhySec is the utilization of active and passive security measures and management protocol that are designed to prevent unauthorized access to personnel, equipment, material, documents and safeguard against espionage, sabotage, acts of terrorism, damage and theft. PhySec is an integral component of Force Protection.

b. PhySec is a primary command responsibility. All commanders are required to establish and issue regulations for the security of personnel, equipment and locations under their charge. Commanders shall ensure PhySec considerations are included in all plans, operations, and daily activities. PhySec Programs shall follow an all-hazards approach, be proactive in nature, and be coordinated and synchronized throughout appropriate commands, down to the battalion/squadron level.

c. Commanders shall ensure PhySec programs are coordinated and synchronized with this plan and/or host installation AT plans. Deployed units shall ensure PhySec plans comply with the supported command's PhySec plan and Force Protection requirements.

d. The development and maintenance of the PhySec program elements should be ongoing and continuously refined to ensure the relevance and viability of all PhySec measures employed, in order to employ a holistic security system to counter terrorist and criminal activities.

e. PhySec Program Elements

(1) Access Control

(2) Material Control

(3) Personnel

(4) Restricted Areas

(5) Electronic Security Systems (ESS)

(6) Security Forces

(7) Barrier Plan

2. PhySec Officer. Commanders shall appoint a Security Officer, in writing, down to the Battalion/Squadron level. Security Officers shall:

a. Plan, manage, implement and direct the organization's physical security program.

b. Establish physical security requirements for the command with assistance from the installation provost marshal, public works officer and facilities engineer as appropriate.

c. Develop, implement and maintain an organizational physical security plan that supports the unit and installation AT plan.

d. Develop and maintain a security education program.

e. Identify assets (property and structures) requiring protection by priority and location. Particular attention will be paid to areas housing personnel and property.

f. Identify in writing, all designated restricted areas within the command and provide this information to the installation commander via the provost marshal's office physical security section.

g. Determine and identify resources or resource shortfalls (e.g., personnel, materials, funds, etc.) required to implement physical security measures.

h. Assist the commanding officer in specifying facility, training, construction, and equipment requirements necessary to comply with this Order.

i. Program and budget fiscal resources necessary to support physical security requirements and correct deficiencies.

j. Serve as the organization point of contact for all command physical security and loss prevention matters.

k. Coordinate all physical security matters with the installation provost marshal.

l. Attend quarterly FP, PS, AT, and other working groups as required.

m. Ensure physical security programs support the installation security effort.

n. Maintain and implement the organizational physical security barrier plan.

o. Coordinate all physical security matters and requirements through the installations provost marshal's office physical security section.

3. PhySec Planning. Security planning is a continuous process carried out in advance of, and concurrent with, security operations. Each organization (battalion/ squadron and above) will develop and publish a PhySec Plan as part of its AT Plan. The plan will reflect the detailed implementation of Marine Corps policy.

a. Risk Management (RM). The RM process outlined in Reference (m) and Enclosure 2 of this order shall be applied in all aspects of the Physical Security program implementation and planning to include; operational plans and decisions, development of risk mitigation measures, and the prioritization and allocation of resources. Risk will be quantified using the methodology; Risk = Threat X Criticality X Vulnerability.

b. PhySec Coordination. Commanders shall coordinate their physical security program and plan requirements with the host installation/separate facility commander, or civilian equivalent director. I MEF tenant units shall participate fully in installation physical security programs. I MEF units coordinate physical security programs by:

(1) Ensuring physical security plans support the next higher level of command, host installation or supported commander.

(2) Participating in training, exercises, and working groups.

(3) Coordinating for resources and support.

c. Access Control. Establish procedures governing access control for:

(1) Individual personnel. This is not limited to

(2) Vehicle

(3) Restricted and non-restricted

d. Material control. Establish procedures governing material control for:

(1) Inbound

(a) Admission of material and supplies

(b) Search/ inspection of material

(c) Special controls for deliveries to restricted areas.

(d) Establish controlled holding areas for classified, AA&E and hazardous material.

(2) Outbound

(a) Required documentation

(b) Transfer areas for controlled, classified, AA&E and Hazardous materials.

e. Restricted Areas. Areas will be designated as either restricted areas or non-restricted areas. Different areas and tasks require varying degrees of security interest and importance. The degree of security is dependent upon the area mission, nature of work performed within and assets/ material within the area. All restricted area must be designated in writing by the commanding officer. There are three types of designation for restricted areas: Level One, Level Two and Level Three.

(1) Level One. The least secure type of restricted areas, it contains a security interests that if lost, stolen, compromised or sabotaged would cause damage to the command mission and national security.

(2) Level Two. The second most secure type of restricted area and contain interests that if lost, stolen, compromised or sabotaged would cause serious damage to the command mission and national security.

(3) Level Three. The most secure type of restricted area and contains a security interests that if lost, stolen, compromised or sabotaged would cause grave damage to the command mission and national security.

(4) Decisions regarding the designation of restricted areas and their levels are at the discretion of the commanding officer however, the following areas will be designated as specified below, at a minimum.

(a) Level One

1. Motor Pools.

2. Tank ramps, tank compounds and tank housing facilities.

3. Fuel issue points and storage tanks (500-999 Gallons)

4. Funds and negotiable instrument storage areas.

(b) Level Two

1. Aircraft, aircraft hangers, ramp, parking, flight line and runways.

2. Aircraft rework areas.

3. Research, development, test and evaluation (RDT&E) centers.

4. AA&E RDT&E facilities, storage facilities and processing areas (including ammunition supply points, production buildings and temporary storage in ready service magazines and lockers).

5. Fuel depots and bulk storage tanks (1000 gallons or more).

6. Critical communications, computer facilities and antenna sites.

7. Critical assets power stations, transformers, master valve and switch spaces.

8. Military Working Dog (MWD) facilities.

(c) Level Three

1. Nuclear, biological, chemical, special weapons research, testing, storage and maintenance facilities.

2. Sensitive Compartmented Information Facilities (SCIF).

3. Special Access Program Facilities (SAPF).

4. Assets and equipment in direct support of the Presidential Mission.

f. Electronic Security Systems. Electronic Security Systems (ESS) are an essential element to any in-depth physical security program. ESS is designed to detect a predetermined anomaly, provide real-time assessment and timely notification to the commander; however it does not prevent actual or attempted penetrations. The design, implantation and operation of ESS must contribute to the overall physical security poster.

(1) ESS determination factors. For facilities requiring ESS the following factors must be addressed to determine the necessity for installation of ESS outside of regulatory guidance.

(a) Mission.

(b) Criticality.

(c) Threat.

(d) Geographic location and location of facilities to be protected within each activity.

(e) Accessibility/vulnerability to intruders.

(f) Other means of protection.

(g) Construction of the facility.

(h) Hours of operation.

(i) Security Forces and expected response time to alarm activation.

g. Security Forces. During periods of elevated Force Protection Conditions (FPCON), other emergency/ increased threat situations or special events, installations may require additional security forces to perform additional security duties.

(1) The Security Augmentation Force (SAF) should possess the capability to full augment Installation posts required in FPCON BRAVO, CHARLIE and DELTA, with the ability to sustain operations for a minimum of 30 days or until the relief forces can be identified and deployed. Regardless of the type of personnel employed, security force functions fall into four general categories:

(a) Prevent/deter theft and other losses caused by fire damage, accident, trespass, sabotage, espionage, criminal activity, etc.

(b) Protect life, property, and the rights of individuals.

(c) Enforce rules, regulations, and applicable statutes.

(d) Detect, deter, and defeat terrorism.

(2) The size and complexity of the installation, critical assets an d the number of personal required to man additional security posts to protect mission essential assets during increased FPCO's should be considered when determining SAF size and capabilities. Reference (bb) outlines the I MEF/ MCIWEST SAF policy and implementation timeline. The size of the security force is dependent upon several factors;

(a) Size and location of the installation/site.

(b) Geographic characteristics of the installation/site.

(c) Mission.

(d) Number, type, and size of restricted areas.

(e) Use and effectiveness of physical security equipment.

(f) Availability of non-organic, LE, camp guard, or other security forces.

(g) Installation population and composition.

(h) Criticality of assets being protected.

Training and Exercises

1. General. Commanders shall ensure:

a. AT training and exercises are integrated with overall physical security, and afforded the same emphasis as combat task training. AT based exercises should be executed with the intent to identify shortfalls affecting the protection of personnel and assets against terrorist attack and subsequent terrorism consequence management efforts.

b. AT training, particularly pre-deployment training, is supported by measurable standards, including credible deterrence and response standards; deterrence-specific tactics, techniques, and procedures (TTP); and lessons learned. AT training shall also be incorporated into unit-level training plans and pre-deployment exercises. Pre-deployment training shall also include terrorist scenarios and hostile intent decision-making.

2. Training Mandates. Commanders shall implement AT training and ensure AT training identifies shortfalls that affect the protection of personnel and assets against terrorist attack and subsequent terrorism consequence management efforts. Ensure AT training is supported by measurable standards, including credible deterrence and response standards, deterrence-specific TTPs, and lessons learned. AT training shall be incorporated into unit-level training plans and exercises. A process shall be developed to collect and report information on personnel received within the command who have not completed required training. The following AT training shall be completed, as required:

a. Level I AT Awareness Training

(1) The primary means of accomplishing Level I AT awareness training shall be via MarineNet: https://www.marinenet.usmc.mil. Personnel who do not have access to MarineNet may complete the training via this website: https://atlevel1.dtic.mil/at or through a Level II-trained ATO.

(2) Level I AT awareness training for DoD contractors, as required by Defense Federal Acquisition Regulation Supplement, and as specified in the contract.

(3) Level I AT awareness training for dependent family members ages 14 years and older (or younger at the discretion of the DoD sponsor) traveling OCONUS on official business (e.g., on an accompanied permanent change of station move).

b. AOR-Specific AT Awareness Training

(1) AOR-specific AT Awareness Training and Education programs shall be developed to orient all DoD personnel (including family members ages 14 years and older) assigned permanently or temporarily, transiting through, or performing exercises or training in the AOR.

(2) DoD personnel (including family members ages 14 years and older) departing to another COCOM's AOR shall complete the gaining COCOM's AOR-specific AT education requirements within three months prior to a permanent change of station.

(3) Commanders shall ensure AOR-specific requirements for deployments are entered in the Aircraft and Personnel Automated Clearance System (APACS), as appropriate.

(4) Commanders shall ensure all personnel subject to deployment in theater have completed other training or actions required by that theater COCOM (e.g., survive, evade, resist, or escape training; isolated personnel report) and are qualified within the AOR designated time frame.

3. Training Exercises. When OPFOR are in garrison, unit AT exercise requirements shall be integrated with the host installation annual MA exercise. There is no requirement for OPFOR to have a separate AT exercise. Deploying forces should conduct an in-transit security exercise. Exercise documentation shall be maintained for three years.

a. Annual AT exercises encompass all aspects of AT and PHYSEC plans; the current baseline FPCON, through FPCON Charlie measures, shall be exercised.

b. Physical security, terrorist incident response, and terrorist consequence management measures are assessed, to include CIP and CBRN.

c. Remediation and mitigation planning is included.

d. Exercises include first/local responders, tenants, and host installation coordination to ensure synchronization of related plans.

e. Exercise scenarios are based on the AHTA and include multi-disciplinary and multi-jurisdictional incidents.

f. Exercises assess and validate proficiency levels; clarify and familiarize personnel with roles and responsibilities; improve interagency coordination and communication; highlight capability gaps; and identify opportunities for improvement.

g. Exercises include participation of appropriate leaders and decision makers representing each of the emergency response functions, and whenever possible, local, State, other Service(s), private sector, and nongovernmental organization partners, as appropriate.

4. Types of Exercises. AT exercises are similar in planning, preparation, execution, and evaluation to other command training events and exercises. They include functional exercises, tabletop exercises, and full-scale exercises.

a. Functional Exercise. Functional exercises are collective training events that focus on selected functions, procedures, or portions of a plan. For example, portions of a plan that can be exercised to achieve limited objectives are command post exercises, notification drills, first responder drills, or evacuation drills. Drills are scenario-driven events usually limited to specific organizations or functions to test, assess, and validate specific portions of a plan.

b. Tabletop Exercise. This type of exercise involves the key leaders and staff of an organization. It is a scenario-driven discussion, led by a facilitator, and can be used to exercise the entire plan or specific portions of the plan.

c. Full-Scale Exercises (FSE). A full-scale exercise is the most complex exercise, and likely involves the entire installation or site. A FSE will likely impact day-to-day functions and operations. To ensure success of a FSE, careful coordination, planning, tabletop exercises and drills are required prior to conducting the FSE.

5. Exercise Evaluations. Commanders shall ensure exercises include a thorough and objective exercise evaluation process. At the conclusion of each exercise, units shall conduct formal reviews among exercise participants and observers of actions performed successfully, outcomes achieved, lessons learned, and areas for improvement, derived from the exercise.

6. After Action Review. Commanders shall ensure exercise AARs are completed, and submitted to the next higher level of command, within 30 days following completion of the exercise. II MEF and its MSCs shall enter AARs into MC-CAMS NG. AARs shall also be submitted to the Marine Corps Center for Lessons Learned (MCCLL) database, via the below websites:

a. NIPRNET - http://www.mccll.usmc.mil

b. SIPRNET - http://www.mccll.usmc.smil.mil

U.S. Marine Corps Operational Forces
Higher HQ Protection Program Review -
Mission Assurance Benchmarks
14 June 2016

Protection is comprised of measures taken to preserve the forces potential so that it can be applied at the appropriate time and place. It includes those measures the force takes to remain viable by protecting itself from the effects of natural and man-made threats. Protection safeguards friendly centers of gravity and protects, conceals, reduces, mitigates, and/or eliminates critical vulnerabilities. (MCDP 1-0, MCWP 5-1, JP 3-07.2, JP 3-10 (primary), JP 3-11, JP 3-27)

Core Programs: Operational Forces (OPFOR) Protection, Antiterrorism (AT), Critical Infrastructure Protection (CIP), Physical Security (PS), Chemical, Biological, Radiological, Nuclear Defense (CBRN), Military Police (MP), and Personnel Recovery (PR).

OPFOR Protection Program Assessment Architecture:

1. Higher Headquarters Program Review Benchmarks.
2. Functional area checklists.
3. MEB/MEU benchmarks and deployment checklists.
4. *Note 1. The USMC expeditionary benchmarks only apply to the MARFOREUR and MARFORAF, Cooperative Security Locations (CSLs).
5. * Note 2. The Mission Assurance Assessment Team (MAAT) Benchmarks apply to MCICOM installations.

The U.S. Marine Corps, Operational Forces, Higher Headquarters Protection Program Review Benchmarks apply to Marine Expeditionary Forces (MEF) Command Element (CE), Marine Division (MARDIV), Marine Air Wing (MAW), and Marine Logistics Group (MLG). The protection benchmarks serve as the framework to ensure continued functions and resilience of capabilities critical to the operating forces. U.S. Marine Corps Operational Forces will utilize these benchmarks in order to outline requirements; to include the determination for the organization, staffing, equipment, training, planning, management, and execution, of the core protection programs.

The OPFOR protection program benchmarks detail:

1) The enduring core protection program requirements as outlined in DoD, Combatant Command, and Service doctrine.

2) Those protection program requirements the OPFOR commander must ensure are accomplished under his/her role as a tenant command supporting the host installation protection program. The protection program Functional Area Inspection checklists within the Inspector General framework apply to those units

subordinate to the MEF Headquarters Groups (MHG), as well as subordinate units below the MARDIV, MAW, and MLG. MEB/MEU protection program requirements will be assessed as part of pre-deployment certification.

Benchmark	Applicability	Doctrine	Requirements
OPFOR- FP-01; OPFOR Protection Program: The OPFOR Protection program integrates the protection related risks and capability gaps, prioritizes, and advocates for proposed solutions and mitigation strategies to protect or ensure the continued function and resilience of capabilities and assets critical to the performance of Mission Essential Functions in any operating environment or condition. The OPFOR Protection approach accounts for the full range of threats and hazards to the capabilities and supporting assets upon which our fighting forces depend, and ensures all protection efforts are coordinated across the enterprise	MEF CE MARDIV MAW MLG	Marine Corps Mission Assurance-Enterprise Road Map, Annex C, Appendix 11. MCO 3058.1, Marine Corps Mission Assurance. MCDP X-X, Marine Corps Protection, *in development.	**Program** ▪ Has the command published Protection policy outlining the command's Protection process? (MCO 3058.1 and MCDP MC Protection) ▪ Is a person appointed in writing assigned to perform OPFOR Protection activities? (MCO 3058.1 and MCDP MC Protection) ▪ Does the program integrate all the protection programs to ensure all risk management efforts are coordinated across the enterprise and the range of military operations? (MCO 3058.1 and MCDP MC Protection) ▪ Does the program document and track Force Protection related workgroup minutes (highlights, issues, tasks, and due outs). (MCO 3058.1) **Protection Risk Planning Activities** ▪ Does the program outline the process for the identification and consolidation of protection-related risk, and capabilities gaps? (MCO 3058.1 and MCDP MC Protection)

Benchmark	Applicability	Doctrine	Requirements
and the range of military operations.			**Protection Risk Prioritization** ▪ Does the Command have a methodology to prioritize protection risk and capability gaps? (MCO 3058.1 and MCDP MC Protection) **Protection Risk Mitigation** ▪ Does the program facilitate the Command's participation and advocate proposed solutions and mitigation strategy of protection risk? (MCO 3058.1 and MCDP MC Protection) ▪ Do the Protection risk and capability gaps inform other Command programming processes; DRRS, CCIF, IPL, JCDS, POM, MILCON, UNS, etc. (MCO 3058.1 and MCDP MC Protection) ▪ Does the program provide prioritized proposed solutions and mitigation strategy for resource requirements? (MCO 3058.1 and MCDP MC Protection) ▪ Does the program track the status of proposed solutions and mitigation strategies of force protection risk / capability gaps? (MCO 3058.1 and MCDP MC Protection)
OPFOR-FP-02; Antiterrorism Program: Each command shall execute a comprehensive Antiterrorism program	MEF CE MARDIV MAW MLG	DODI 2000.16 MCO 3302.1E	**Intelligence Support to AT** ▪ Does the command gather, analyze and circulate terrorism threat information in step 1 of the Marine Corps Planning Process (MCPP)? (DODI 2000.16 STD 2)

Benchmark	Applicability	Doctrine	Requirements
designed to protect personnel, equipment, and capabilities for which they have Tactical Control for Force Protection. Each command will provide AT policy and guidance to subordinates.			▪ Do the command's Priority Intelligence Requirements and Commander's Critical Information Requirements focus AT collection and analysis efforts? (DODI 2000.16 STD 2) ▪ Do the command's operations orders, LOIs, etc. reflect adequate analysis of terrorist threats in the SITUATION paragraph? (DODI 2000.16 STD 2) **AT Risk Management** ▪ Are risk mitigation actions developed based on thorough analysis of Threat, Vulnerability, Criticality, and Risk Assessments? (DODI 2000.16 STD 3) ▪ Are risk mitigation actions developed for steps 2-4 of the MCPP? (DODI 2000.16 STD 3) **Threat Assessment** ▪ Are Terrorist Threat Assessments (TTAs) completed for exercises, deployments and special events (300 or more DoD personnel)? (DODI 2000.16 STD 4) ▪ Does the command ensure a TTA is completed at least annually for bases/stations/installations/garrisons (300+ daily populations)? (DODI 2000.16 STD 4)

Benchmark	Applicability	Doctrine	Requirements
			Criticality Assessment ▪ Are Criticality Assessments completed for exercises, deployments and special events (300+ DoD personnel)? (DODI 2000.16 STD 5) **Vulnerability Assessment** ▪ Are Vulnerability Assessments completed for exercises, deployments and special events (300+ DoD participants)? (DODI 2000.16 STD 6) **Antiterrorism Plan** ▪ Are AT plans developed for all operational deployments, training exercises and special events (300 or more DoD personnel)? (DODI 2000.16 STD 7; MCO 3302.1E para 4.c.(11)(b)) ▪ Are terrorist threats fully analyzed in the SITUATION paragraph of the OPORD and considered through steps 2-4 of the MCPP? (DODI 2000.16 STD 7; MCO 3302.1E para 4.c.(11)(b)) **Antiterrorism Program Coordination** ▪ Do ATOs consistently coordinate with higher, adjacent (e.g., Installation ATOs, local law enforcement, host nation Law Enforcement, U.S. Embassy force protection/security experts) and subordinate commands? (DODI 2000.16 STD 8)

U.S. Marine Corps Operational Forces
Higher HQ Protection Program Review -
Mission Assurance Benchmarks
14 June 2016

Benchmark	Applicability	Doctrine	Requirements
			Antiterrorism Officer (ATO) ▪ Has the command assigned an AT Level II-trained ATO in writing? (DODI 2000.16 STD 9; MCO 3302.1E para 4.c.(11)(a)) ▪ Do smaller units or detachments of more than 300 pax assign an ATO in writing when deploying without HQ? (DODI 2000.16 STD 9; MCO 3302.1E para 4.c.(11)(a)) ▪ Has MARFOR established a full-time AT staff? (DODI 2000.16 STD 9; MCO 3302.1E para 4.c.(11)(a)) ▪ Do MEFs maintain a current list of all MSC ATOs? (MCO 3302.1E para 4.c.(11)(h)) **Antiterrorism Working Group (ATWG)** ▪ Does the command conduct quarterly ATWGs? (MCO 3302.1E para 4.c.(11)(d); MCO 3302.1E para 4.c.(12)(d)) ▪ Do commands attend their host installation ATWGs? (DODI 2000.16 STD 10) ▪ Do commands attend HHQ ATWGs? **Threat Working Group (TWG)** ▪ Do commands attend their host installation TWGs? (DODI 2000.16 STD 11) ▪ Does the command conduct quarterly TWGs?

Benchmark	Applicability	Doctrine	Requirements
			(MCO 3302.1E para 4.c.(11)(c)) ▪ Do MEFs coordinate and implement an effective process to integrate and fuse all sources of threat info to MSCs? (MCO 3302.1E para 4.c.(12)(c)) ▪ Does MARFOR gather, analyze, disseminate and report terrorist threat info? (MCO 3302.1E para 4.c.(12)(c)) **Antiterrorism Executive Committee (ATEC)** ▪ Do commands conduct and/or attend their host installation ATECs? (DODI 2000.16 STD 12) **Random Antiterrorism Measures (RAMs)** ▪ Has the command developed and implemented a RAM program in coordination with the installation? (MCO 3302.1E para 4.c.(12)(g)) **Antiterrorism Measures for Off-Installation Facilities, Housing and Activities** ▪ Has the command coordinated with the installation to develop specific mitigation actions for off-installation housing, transportation, daycare or other mass-gathering areas? Minimal: emergency notification, recall procedures, guidance for selection, shelter-in-place, relocation and evacuation? (DODI 2000.16 STD 15)

Benchmark	Applicability	Doctrine	Requirements
			Antiterrorism Construction and Building Considerations ▪ Has the command developed a prioritized list of AT measures to be used by site selection teams? (DODI 2000.16 STD) **Antiterrorism Measures for Logistics and Contracting** ▪ Do ATOs work with contracting officers to ensure vendors are submitted for appropriate background checks and employee vetting? (DODI 2000.16 STD 18) ▪ Do contracts require employee information to be provided for vetting purposes? (DODI 2000.16 STD 18) ▪ Do contracts allow for cancellation in the event of non-compliance with AT vetting requirements or concerns? (DODI 2000.16 STD 18) **FPCON Measures** ▪ Has the command set policies and procedures for setting FPCON levels? (DODI 2000.16 STD 22; MCO 3302.1E para 4.c.(11)(h)) ▪ Has the command established review mechanisms to lower FPCCON levels as threat environment permits? (DODI 2000.16 STD 22; MCO 3302.1E para 4.c.(11)(h))

U.S. Marine Corps Operational Forces
Higher HQ Protection Program Review -
Mission Assurance Benchmarks
14 June 2016

Benchmark	Applicability	Doctrine	Requirements
			▪ Has the command developed site-specific FPCON measures in garrison and at forward-deployed locations? Are they coordinated with the installation FPCON plan? (DODI 2000.16 STD 22; MCO 3302.1E para 4.c.(11)(h)) ▪ Does MARFOR acknowledge receipt of FPCON changes and report implementation within one hour? (DODI 2000.16 STD 22; MCO 3302.1E para 4.c.(11)(h)) **Antiterrorism Training and Exercises** ▪ Does the command execute pre-deployment AT training?...and maintain records for 2 years? (DODI 2000.16 STD 23) ▪ Are AT plans exercised at least annually? (DODI 2000.16 STD 23) **Antiterrorism Level I Awareness Training** ▪ Do all individuals complete AT level I training annually? (DODI 2000.16 STD 25) **Antiterrorism Level II ATO Training** ▪ Do all BN+ units have an AT level II certified ATO?...initial or refresher training current within 3 years? (DODI 2000.16 STD 26)

Benchmark	Applicability	Doctrine	Requirements
			Antiterrorism Level III Pre-Command Training ▪ Do O-5/6 commanders receive AT level III training before assuming command? (DODI 2000.16 STD 27) **Antiterrorism Level IV Executive Seminar** ▪ Does O-6 thru O-8s receive AT level IV training? (DODI 2000.16 STD 28) **AOR-Specific Training** ▪ Do all applicable personnel receive AOR-specific threat information covering transit routes and sites that will be visited? (DODI 2000.16 STD 29) **AT Resource Application** ▪ Does the command submit validated, prioritized AT resource requests? (DODI 2000.16 STD 30) ▪ Does MARFOR advocate for AT resources to HQMC? (DODI 2000.16 STD 30) ▪ Does MARFOR keep COCOM informed of significant PPBE issues related to AT? (DODI 2000.16 STD 30) **Comprehensive AT Program Review** ▪ Does the command perform HHQ assessments of its MSCs at least every 3 years? (DODI 2000.16 STD 31; MCO 3302.1E para

Benchmark	Applicability	Doctrine	Requirements
			4.c.(11)(g)) ▪ Does the command perform self-assessments in every year a HHQ review does not occur? ▪ Does the command perform pre-deployment program reviews? ▪ Do commands ensure travelers comply with TT/IATP entry requirements of this message? (MFP Msg 271950Z APR11) **Risk Management** ▪ Do MARFORs ensure procedures are in place to closely monitor risk management decisions to closure? (DODI 2000.16; MCO 3302.1E)
OPFOR-FP-03; Critical Infrastructure Protection (CIP) Program: Commanders shall ensure that task critical assets and supporting infrastructure are identified, prioritized, risk is assessed and managed. The focus of an Operational Force CIP Program is to identify, protect, and ensure the availability of	MEF CE MARDIV MAW MLG	DODI 3020.45 SECNAVINST 3501.1B NAVMC 3500.63 MCO 3501.36A MCO 3058.1 MFPO 3020.1B MFCO 3501.1	**Program** ▪ Has the command published CIP policy? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the Command Identified an office of primary responsibility for matters pertaining to the identification, prioritization, and management of risk of mission critical assets? (MFPO 3020.1B and MFCO 3501.1) ▪ Appointed a person in writing to execute the CIP program? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the appointed person received annual

Benchmark	Applicability	Doctrine	Requirements
infrastructures, assets, and capabilities deemed critical to the operating forces in accomplishing their war-fighting mission and to accept prudent risk where necessary. Additionally, the CIP Program must concentrate on developing a plan to mitigate the effects of the potential loss or disruption of these critical infrastructures, assets, and capabilities. To maintain operational and tactical readiness, commanders and forces must understand the importance of their assets, perform continuous threat and vulnerability assessments of mission critical assets, and effectively manage their risk of loss or degradation.			CIP training, formal or informal, per the references? (MFPO 3020.1B and MFCO 3501.1) **Identify Task Critical Assets (TCA)** ▪ Does the Command use the Critical Asset Identification Process (CAIP) to identify TCAs? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the Command identified, and approved its Task Critical Assets annually? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the Command identified Supporting Infrastructure Critical Assets (SICAs) which an asset directly uses to support the functioning or operation of a TCA. (MFPO 3020.1B and MFCO 3501.1) ▪ Does the Command maintain Mission, TCA/SICAs, Risk Assessments data in Marine Corps Critical Asset Management System (MC-CAMS)? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the Command shared its list of TCAs with other stakeholders (i.e. host installation, other service counterparts, etc.)? (MFPO 3020.1B and MFCO 3501.1) **Assess, Prioritize and Manage Risk** ▪ Does the Command have a risk assessment strategy to prioritize and manage the risk to mission produced by the TCAs? (MFPO 3020.1B and MFCO 3501.1) ▪ Does the Command have a system to monitor

Benchmark	Applicability	Doctrine	Requirements
			and report changes in operational status of TCAs and SICAs within 24 hours using the MC-CAMS, and OPREP-3 format? (MFPO 3020.1B and MFCO 3501.1) ▪ Has the Command accounted for and integrated TCAs into their planning processes for operational plans, orders, and exercises to manage their risk to mission. (MFPO 3020.1B and MFCO 3501.1) ▪ Is the status of Risk reduction actions and mitigations of prioritized TCAs tracked? (MFPO 3020.1B and MFCO 3501.1)
OPFOR-FP-04; PHYSICAL SECURITY: Each higher headquarters shall apply the principles of the Physical Security Program and fully integrate them into Protection Plans to ensure employment of a holistic security system to counter terrorist and criminal activities to protect personnel and equipment.	MEF CE MARDIV MAW MLG	DODI 2000.16 DODD 5200.8-R MARADMIN 039/16 MCO 5530.14A	**Expeditionary:** ▪ Are commands requesting Physical Security support from PMO/LEBN if not organic to the unit? (MCO 5530.14A) ▪ Are commands ensuring surveys are conducted at designated MEVA sites; AA&E storage sites, aviation assets, piers/ports, POL facilities, ECP's/ACP's, critical assets, and motor pools? (MCO 5530.14A)Are decisions to accept/reduce risk based on a risk assessment? (Risk = Threat x Criticality x Vulnerability) (MCO 5530.14A) ▪ Are commands requesting exceptions and waivers IAW the Marine Corps Physical Security Waiver/Exception Policy? (MCO 5530.14A)

Benchmark	Applicability	Doctrine	Requirements
			Garrison: ▪ Are tenant commands coordinating and integrating unit security plans and measures into the installation AT Plan? (MCO 5530.14A) ▪ Are Physical security plans signed, published, and incorporated into the Installation FP/AT plan? (MCO 5530.14A) ▪ Are commanders appointing Physical security officers in writing? Bn and Squadron level? (MCO 5530.14A) ▪ Are commands designating restricted areas in writing and providing them to PMO for implementation into the installation AT plan? Completed annually? (MCO 5530.14A) ▪ Are Physical security plans reviewed annually in conjunction with the AT Plan? (MCO 5530.14A)Are commands coordinating with host installation for specific technology (e.g., barriers, access control systems, etc.) to mitigate identified vulnerabilities and if so, how is this information disseminated / enforced at the subordinate level? (MCO 5530.14A) ▪ Are AA&E protective measures coordinated with the host installation? (MCO 5530.14A) ▪ Are commands requesting exceptions and waivers IAW the Marine Corps Physical Security Waiver/Exception Policy? (MCO 5530.14A)

Benchmark	Applicability	Doctrine	Requirements
OPFOR-FP-05 Chemical, Biological, Radiological, Nuclear Defense (CBRND): CBRND, functions, objectives, and capabilities occurring in peace, crisis, and war. It also describes how CBRND is integrated into MAGTF operations and supports operational and tactical level expeditionary activities.	MEF CE MARDIV MAW MLG	DODI 2000 .16 DODI 3020.52 National Response Framework (NRF) MCO 3440.8 NAVMC 3500.78 MCO 3400.3G MCO 3302.1E JP 3-07.2 DoDI 3020.45 DoDD 3020.40 NAVMC 3500.103 MCWP 5-1 MCWP 3-34.1 MCO 5580.2B JP 3-11 JP 3-40 JP 3-41	▪ Does the command maintain awareness of CBRN Defense equipment availability within the Consolidated Storage Facility (CSF)? (JP 3-11, 3-40, 3-41) ▪ Does the command have a CBRN Defense equipment distribution plan? (JP 3-11, 3-40, 3-41) Note: Comprehensive CBRN Defense planning shall be integrated in the supporting relationship with the installation. Note: Installation/Base Commanders should take the lead in garrison, but the tenants have equities and their participation and coordination is an integral part of a successful CBRN Defense capability. ▪ Does the OPFOR coordinate/plan with Garrison/Host installation in support of CBRN capabilities? (JP 3-11, 3-40, 3-41) ▪ Is the Command using "Plan, Prepare, Respond, and Recover" integrated/incorporated into CBRN Defense planning? (DODI 6055.17, Encl. 5, 5.a) Note: OPFOR shall assist Base Commander in developing relevant support agreements. These support agreements include, but are not limited to MOAs, MOUs, inter-Service support agreements, SOFAs, and/or other support contracts. Command legal counsel should assist in the preparations and perform a legal review of all support agreements before execution.

Benchmark	Applicability	Doctrine	Requirements
			▪ Have MOU/MOAs been established with Garrison/Host installation to ensure detection/identification/mitigation and CBRN response capabilities. (JP 3-11, 3-40, 3-41) ▪ Are the MOU/MOAs integrated into IEM, AT, CBRN, LE, and Medical Response Plan? (JP 3-11, 3-40, 3-41) Note: These can include utility restoration planning, priority of response and critical asset security. ▪ Are MOU/MOA's reviewed at least annually and modified as appropriate? (JP 3-11, 3-40, 3-41) ▪ Is there a POC who maintains and tracks all CBRN Defense related MOU/MOAs? (JP 3-11, 3-40, 3-41) ▪ Are protection programs (e.g. CBRN) adequately considered in COA Development? (JP 3-11, 3-40, 3-41) ▪ Do CBRN Defense plans include notification, mitigation, evacuation, search and shelter in place procedures? (JP 3-11, 3-40, 3-41) ▪ Is CBRND planning considered in MARFOR/MEF/MSC and MAGTF CBRND with other Services and/or HNs? (JP 3-11, 3-40, 3-41) ▪ Is CBRND capabilities planning integrated into operational plans and exercise

Benchmark	Applicability	Doctrine	Requirements
			planning? (JP 3-11, 3-40, 3-41) ▪ Is Command conducting Threat Analysis of AOR OPORDS / OPLANS / CONPLANS? (JP 3-11, 3-40, 3-41) ▪ Does Command staff conduct Operational Integration of CBRND considerations for all operations? (JP 3-11, 3-40, 3-41) ▪ Does Command/Organization CBRND attend MAWG which meets at least quarterly, or more often if necessary, and is a compilation of security related programs on the installation. Note: These security related programs include, but are not limited to; Antiterrorism, Physical Security, CBRND, Law Enforcement, IEM, CIP, Personnel Recovery and Force Protection. (JP 3-11, 3-40, 3-41)
OPFOR-FP-06; Military Police: MP tasks, functions, objectives, and capabilities occurring in peace, crisis, and war. It also describes how military police integrate into operations and support operational and tactical level expeditionary activities. The MP program plans, prepares,	MEF CE MARDIV MAW MLG	MCWP 3-34.1	▪ Does the MP program support policing operations; criminal investigations requiring CID & MP investigative support, conduct Police Intelligence Operations, and establishes linkages to local police agencies and other international/interagency law enforcement agencies? (MCWP 3-34.1) ▪ Does the section coordinate for MP and/or CID Division/EAD/EAC augmentation forces, Military Working Dogs (Explosives/Narcotics /Patrol), LE BNs. (MCWP 3-34.1)

Benchmark	Applicability	Doctrine	Requirements
provides staff supervision of the execution and assesses MP support of all MP core functions: maneuver and mobility support, area security, law enforcement, and detention operations throughout the supported AOR.			▪ Does the program provide supervision and policy compliance concerning the collection, processing, evacuation and internment of EPW/CI/Detained persons reporting and data submission? (MCWP 3-34.1) ▪ Does the program coordinate with allied forces, host nation military territorial organizations, and civilian police authorities concerning policing operations to theater support area operations? (MCWP 3-34.1) ▪ Does the program provide guidance on escalation of force from non-lethal to lethal tactics, weapons, munitions, effects and systems? (MCWP 3-34.1) ▪ Does it coordinate police advising, training, and partnering requirements for training exercises within the AO? (MCWP 3-34.1) ▪ Does the program coordinate contingency operations; writes the MP portion of detailed plans, orders, and estimates; coordinates staff with other Cells, nodes, and functional groupings internal and external? (MCWP 3-34.1) ▪ Does the program coordinate Detention Operations, coordinate Internment and Resettlement (I/R) operations of EPWs, and civilian internee handling? (MCWP 3-34.1) ▪ Does the program provides support for

Benchmark	Applicability	Doctrine	Requirements
			civil disturbances (DHS [FEMA], support to federal agencies in immigration emergencies (DHS [Citizenship & Immigration Services]), and law and order (investigation of crimes, apprehension of offenders, and incarceration of offenders) for the entire AO? (MCWP 3-34.1) ▪ Does the program provide theater law enforcement and criminal investigation data management within the AO? (MCWP 3-34.1)
OPFOR-FP-07; Personnel Recovery: Commanders will develop policies and procedures, in accordance with applicable combatant command regulations and all applicable references, to accomplish the five PR execution tasks (report, locate, support, recover and reintegrate).	MEF CE MARDIV MAW MLG	JP 3-50, Personnel Recovery MCO 3460.3	▪ Has the Command Identified an office of primary responsibility for matters pertaining to PR? (MCO 3460.3). ▪ Do the operations (G-3) and intelligence (G-2) offices have personnel trained in Personnel Recovery Coordination Cell (PRCC) functions and assigned collateral duties? (MCO 3460.3). ▪ Have the appointed personnel received the required PR training, per the references? (JP 3-50, MCO 3460.3). ▪ Does the command have the capability to standup and execute the functions of a PRCC. When applicable, be prepared to execute and/or support the functions of a Joint Personnel Recovery Center (JPRC). (JP 3-50, MCO 3460.3). ▪ Has the Command integrated PR into their planning processes for operational plans, orders, and exercises? (MCO 3460.3).

U.S. Marine Corps Operational Forces
Higher HQ Protection Program Review -
Mission Assurance Benchmarks
14 June 2016

Benchmark	Applicability	Doctrine	Requirements
			▪ Does the Command ensure designated personnel receive appropriate PR requirements such as Survival, Evasion, Resistance, and Escape (SERE) and Isolated Personnel Report (ISOPREP) prior to deployments? (MCO 3460.3)
OPFOR-FP-08; OPFOR Support to Installation Protection: These benchmarks assess the OPFOR HHQ's responsibilities as a tenant supporting the host installation protection program. These benchmarks reinforce the installation requirements mentioned in each OPFOR protection program and also complement the installation MAAT results.	MEF CE MARDIV MAW MLG	Marine Corps Mission Assurance-Enterprise Road Map, Annex C, Appendix 11. MCO 3058.1, Marine Corps Mission Assurance. MCICOMO 3000-1 Installation Protection. MCDP X-X, Marine Corps Protection, *in development.	**Installation Protection Program Support** ▪ Do OPFOR commands coordinate with and support their host installation protection program? (MCO 3058.1 and MCDP MC Protection) ▪ Does the command integrate risk planning activities with the installation protection program? (MCO 3058.1 and MCDP MC Protection) ▪ Does the command support prioritization of protection risk with the host installations protection program? (MCO 3058.1 and MCDP MC Protection) ▪ Does the program support the proposed solutions and mitigation strategy of host installation protection risk? (MCO 3058.1 and MCDP MC Protection) ▪ Does the command support resource requirements for installation protection? (MCO 3058.1 and MCDP MC Protection)

JTF Protection Planning Considerations

1. Purpose. The protection function at the operational/Joint Task Force (JTF) level focuses on preserving the joint force's fighting potential in four primary ways;

a. Active Defensive Measures. Protect the joint force, information, bases, critical infrastructure and lines of communication (LOCs) from an adversaries attack or from other all-hazards based threats.

b. Passive Defensive Measures. Enhance the protective posture by making friendly forces, systems, and facilities difficult to locate, strike, and destroy.

c. Applying Technology. To enhance protection efforts and generate efficiencies leveraging capabilities such as electronic sensor arrays, intelligence/surveillance/reconnaissance (ISR) platforms, forensics, explosives and contraband detection, and information management.

d. Emergency Management and Incident Response. To minimize loss of personnel and capabilities in response to terrorist or criminal incidents, accidents, force health, and natural disasters.

2. Responsibilities

a. Commander, Joint Task Force (CJTF)

(1) As the CJTF's mission requires, the protection function extends beyond anti-terrorism & force protection (AT/FP) to encompass protection of US noncombatants; the forces, systems, and civil infrastructure of friendly nations; and organizational partners. Protection capabilities apply domestically in the context of homeland defense, defense support of civil authorities, and emergency preparedness.

(2) Provide air, space, and missile defense.

(3) Protect US civilians.

(4) Provide physical security for forces and means.

(5) Conduct defensive countermeasure operations to include: counter-deception, counter-propaganda, and counter-improvised explosive devices (C-IED).

(6) Provide chemical, biological, radiological, and nuclear (CBRN) defense.

(7) Conduct operations security (OPSEC), computer network defense (CND), information assurance (IA), defensive electronic attack (EA) and electronic protection activities.

(8) Secure and protect forces, bases, joint security areas (JSAs), and LOCs.

(9) Conduct personnel recovery (PR) operations.

(10) Mitigate the effects of CBRN threats and hazards through weapons of mass destruction consequence management.

(11) Establish antiterrorism programs.

(12) Establish capabilities and measures to prevent fratricide.

(13) Provide emergency management and response capabilities and services.

3. Tasks, Functions, and Procedures

a. Force Protection

(1) Take preventive measures to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, critical infrastructure, and information.

(2) Tailor selection and application of multilayered active and passive measures within the operational area, across the range of military operations to achieve acceptable levels of risk.

(3) Intelligence sources provide information regarding an adversary's capabilities against personnel and resources, as well as information regarding FP considerations.

(4) Foreign and domestic law enforcement agencies (LEAs) prevent, detect, respond to, and investigate crimes; and share information on criminal and terrorist organizations.

(5) In coordination with the combatant commander (CCDR), the CJTF maintains a cooperative police program involving domestic or host nation military and civilian LEAs.

(6) In coordination with the CCDR, determine the status, operations, and use of security contractors in the operational area.

(7) Implement OPSEC countermeasures to reduce the vulnerability of US personnel from successful adversary exploitation of critical information to ensure friendly capabilities that might be easily countered are not compromised.

b. Security of Forces and Means

(1) Identify and reduce the vulnerability of friendly forces to hostile acts, influence, or surprise; protect forces, LOCs, bases, and JSAs through security operations.

(2) Utilize physical security measures to reduce vulnerabilities to identified threats. Apply appropriate deterrent, control, and denial safeguarding techniques and measures, and respond to changing conditions and evolving threats.

(3) Physical security functions include security of facilities, law enforcement, guard and patrol operations, special land and maritime security areas, and other operations such as military working dogs, forensics/investigative, emergency, and disaster response support operations.

(4) Physical security measures include fencing and perimeter stand-off areas, land or maritime force patrols, lighting and sensors, vehicle barriers, facility hardening measures, blast protection/mitigation, intrusion detection systems, electronic surveillance, and access control devices and systems. These measures should be integrated, provide overlap in coverage, and be deployed in depth.

c. Defensive Counter-air. Detect, identify, intercept, and destroy or neutralize enemy forces attempting to penetrate or attack through friendly airspace.

(1) Active air and missile defense. Utilization of aircraft, integrated air and missile defense (IAMD) systems, electronic warfare (EW), and other available weapons as direct defensive actions taken to destroy, nullify, or reduce the effectiveness of air and missile threats against friendly forces and assets. This integration of systems should also allow for defense in depth.

(2) Passive air and missile defense. Utilization of all measures, other than active air and missile defense, to include; camouflage, concealment, deception, dispersion, reconstitution, redundancy, detection of warning systems, and the use of protective construction to minimize the effectiveness of hostile air and missile threats against friendly forces and assets.

d. Defensive use of information operations. Ensure access to timely, accurate, and relevant information while denying adversaries opportunities to exploit friendly information and information systems for their own purposes.

(1) Operations Security (OPSEC). OPSEC is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence systems, denies critical information to the enemy, determines if information obtained by the enemy could be useful to them, and then executes selected measures that eliminate or reduce enemy exploitation of friendly critical information. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities.

(2) Computer Network Defense (CND). CND includes actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks.

(3) Information Assurance (IA). IA encompasses measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. IA incorporates protection, detection, response, restoration, and reaction capabilities and processes to shield and preserve information and information systems. IA for DOD information and information systems requires a defense-in-depth that integrates the capabilities of people, operations, and technology to establish multilayer and multidimensional protection to ensure survivability and mission accomplishment. IA must account for the possibility that access to DOD information and information systems can be accessed by outside elements beyond DOD control. Note that IA and cyberspace are interrelated and rely on each other to support information operations.

(4) Electronic protection. Integrates components of EW to protect personnel, facilities, and equipment from any effects of friendly or enemy

use or manipulation of the electromagnetic spectrum (EMS) that can degrade, neutralize, or destroy friendly combat capability.

(5) Defensive Electronic Activities. Encompass activities that use the EMS to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and FP measures such as the use of expendables (e.g., flares and active decoys), protection jammers and lasers, towed or mobile decoys, and directed energy countermeasures systems.

e. Personnel Recovery (PR). Use military, diplomatic, and civil efforts to recover and reintegrate isolated personnel. Consider all available individual, component, joint, and interorganizational partner capabilities when planning and executing PR missions. There are five PR execution task;

(1) Report

(2) Locate

(3) Support

(4) Recover

(5) Reintegrate

f. CBRN Defense. Prepare for potential enemy use of CBRN weapons.

(1) Consider the strategic, operational, psychological, and political impacts of their use that may affect strategic objectives and campaign design.

(2) Provide defensive measures which ensure the capability to sustain operations in CBRN environments using the principles of contamination avoidance of CBRN hazards; protection of individuals, units and equipment from unavoidable CBRN hazards, and decontamination.

(3) Ensure effective CBRN preparedness and operational readiness to possibly deter enemy CBRN use by contributing to the survivability of US forces.

g. Anti-terrorism. Establish defensive measures that reduce the vulnerability of individuals and property to terrorist attacks.

(1) Employ sound personal protective measures.

(2) Use individual protective equipment.

(3) Use hardened vehicles and facilities if/as available.

(4) Employ dedicated/trained guard force personnel.

(5) Use duress alarms.

(6) Vary the installation/facility force protection posture through the use of a robust random anti-terrorism measures program.

h. Combat Identification (CID). Attain an accurate characterization of detected objects in the operational environment sufficient to support engagement decisions.

(1) Characterize CID depending on operational requirements (e.g., "friendly", "enemy", "neutral", or "unknown" or by class, type, nationality, and mission configuration) and apply rules of engagement (ROE) or rules for the use of force (RUF).

(2) Develop CID procedures early during planning. Ensure they are consistent with established ROE or RUF and do not adversely interfere with unit's or individual's abilities to engage enemy forces. Consider mission, capabilities, and limitations of all participants, including organizational partners.

(3) Integrate CID procedures across all command levels and among all participants involved in the operation by employing communications systems and available technology to enable accurate and timely decisions.

(4) Maintain constant coordination and conveyance to decision makers on situational awareness of friendly and neutral forces, restrained sites and structures, and identification of threat elements.

i. Force Health Protection (FHP). Measures to promote, improve, or conserve the behavioral and physical well-being of service members to enable a healthy and fit force, prevent injury and illness, and protect the force from health hazards.

(1) Ensure adequate capabilities are available to identify health threats (e.g., employment of CBRN capabilities; environmental, occupational, industrial, and meteorological conditions; endemic human and zoonotic diseases; and other medical considerations that can reduce the effectiveness of military forces) and implement appropriate FHP measures.

(2) In coordination with the combatant command surgeon, implement health surveillance to identify the population at risk; identify and assess hazardous exposures; employ specific countermeasures to eliminate or mitigate exposures; and monitor and report battle injury, disease, and non-battle injury trends and other health outcomes.

j. Critical Infrastructure Protection CIP. CIP programs support the identification and mitigation of vulnerabilities to defense critical infrastructure, which includes DOD and non-DOD domestic and foreign infrastructures essential to plan, mobilize, deploy, execute and sustain US military operations on a global basis. Coordination between DOD entities and other US Government departments and agencies, state, and local governments, the private sector, and equivalent foreign entities, is key in effective protection of critical assets controlled both by DOD and private entities. Vulnerabilities found in defense critical infrastructure shall be remediated and/or mitigated based on risk management decisions made by responsible authorities. These vulnerability mitigation decisions should be made using all available program areas, including anti-terrorism, military deception, OPSEC, and FP.

k. Counter-Improvised Explosive Device (C-IED) Operations. C-IED operations are the collective efforts, at all levels, to neutralize the IED threat to friendly forces and civilians. They are conducted as an integral part of the broader joint operation and include measures taken to neutralize the network supporting the production and employment of IEDs; technical exploitation (forensics) of the device to obtain information to support targeting and improve friendly FP measures; and the development of tactics, techniques, and procedures to counter the IED threat at the tactical level.

4. Additional Considerations

a. There are protection considerations that affect planning in every joint operation.

b. The greatest risk - and therefore the greatest need for protection - occurs during campaigns and major operations that involve large-scale combat against a capable enemy. These typically will require the full range of protection tasks, thereby complicating both planning and execution.

c. Although the operational areas and the joint force may be smaller for crisis response or limited contingency operations, the mission can still be complex and dangerous with a variety of protection considerations.

d. Permissive operating environments associated with civil-military and civil affairs operations, military engagement, security cooperation, and deterrence still require that planners consider protection measures commensurate with potential risks which may include a wide range of threats such as terrorism, criminal enterprises, environmental threats and hazards, and cyber.

5. Reference Publications ISO JTF Level Protection Planning

a. CJCSI 3125.01C, Defense Response to Chemical, Biological, Radiological, and Nuclear (CBRN) Incidents in the Homeland

b. CJCSI 3213.01D, Joint Operations Security

c. DODO 2000.12, DOD Anti-terrorism Handbook (FOUO)

d. DODD 3020.40, Defense Critical Infrastructure Program (DCIP)

e. DODI 2000.12, DOD Anti-terrorism (AT) Program

f. DODI 2000.16, DOD Anti-terrorism (AT) Standards

g. JP 3-0, Joint Operations

h. JP 3-01, Countering Air and Missile Threats

i. JP 3-07.2, Anti-terrorism

j. JP 3-10, Joint Security Operations in Theater

k. JP 3-11, Operations in CBRN Environments

l. JP 3-13.3, Operations Security

m. JP 3-13.4, Military Deception

n. JP 3-15.1, Counter-Improvised Explosive Device Operations (FOUO)

o. JP 3-34, Engineer Operations

p. JP 3-41, Chemical, Biological, Radiological, and Nuclear Consequence Management

q. JP 3-50, Personnel Recovery

r. JP 3-57, Civil-Military Operations

s. JP 3-68, Noncombatant Evacuation Operations

t. JP 4-02, Health Service Support

Acronyms

AC/S	Assistant Chief of Staff
AHTA	All Hazards Threat Assessment
AOR	Area of Responsibility
APACS	Aircraft and Personnel Automated Clearance System
ASM	Action Set Matrix
AT	Antiterrorism
ATO	Antiterrorism Officer
ATWG	Antiterrorism Working Group
BEI	Basic Elements of Information
C4I	Command Control Communications Computers Intelligence
CA	Criticality Assessment
CAIP	Critical Asset Identification Process
CAT	Crisis Action Team
CBIRF	Chemical Biological Incident Response Force
CBRN	Chemical Biological Radiological Nuclear
CCIF	Combatant Commander Initiative Fund
CCIR	Commander's Critical Information Requirements
CDO	Command Duty Officer
CE	Command Element
CI	Counterintelligence
CID	Combat Identification
C-IED	Counter - Improvised Explosive Devices
CIP	Critical Infrastructure Program
CIPWG	Critical Infrastructure Program Working Group
COA	Course of Action
COC	Chain of Command

COCOM	Combatant Commander
CONUS	Continental United States
COOP	Continuity of Operations
CWA	Chemical Warfare Agents
CWC	Chemical Weapons Convention
DC, PP&O	Deputy Commandant Plans Policy and Operations
DCA	Defense Critical Assets
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIWS	Defense Indications and Warning System
DOD	Department of Defense
DOS	Department of State
DRRS	Defense Readiness Reporting System
D-UNS	Deliberate Universal Needs Statement
EE	Eagle Eyes
FBI	Federal Bureau of Investigation
FHP	Force Health Protection
FPCON	Force Protection Condition
FSE	Full Scale Exercise
FY	Fiscal Year
FYDP	Future Years Defense Plan
GCC	Geographic Combatant Command
HHQ	Higher Headquarters
HQMC	Headquarters Marine Corps
HRP	High Risk Personnel
HVAC	Heating Ventilation and Air Conditioning
I&W	Indications and Warnings
IA	Information Assurance

IAMD	Integrated Air and Missile Defense
IAW	In Accordance With
IFC	Information Fusion Cell
I MHG	I MEF Headquarters Group
INFOCON	Information Operations Condition
MA	Mission Assurance
MAAT	Mission Assurance Assessment Team
MAEC	Mission Assurance Executive Committee
MAGTF	Marine Air-Ground Task Force
MAO	Mission Assurance Officer
MARDIV	Marine Division
MARFOR	Marine Forces
MARFORCOM	Marine Corps Forces Command
MARFORNORTH	Marine Corps Forces North
MARFORRES	Marine Corps Forces Reserve
MAW	Marine Aircraft Wing
MAWG	Mission Assurance Working Group
MCAPM	Marine Corps Asset Prioritization Methodology
MCARA	Marine Corps Asset Risk Assessment
MCCAMS	Marine Corps Critical Asset Management System
MCCLL	Marine Corps Centers for Lessons Learned
MCCSP	Marine Corps Cyber Security Program
MCFDS	Marine Corps Force Development System
MCI-W/MCBCAMPEN	Marine Corps Installations East/MCB Camp Lejeune
MCMAA	Marine Corps Mission Assurance Assessments
MCMA-E	Marine Corps Mission Assurance Enterprise
MCPC	Marine Corps Programming Code
MCPP	Marine Corps Planning Process

MCSAT	Marine Corps Suspicious Activity Tool
MCS/MSE	Major Subordinate Command/Major Subordinate Element
MCSFR	Marine Corps Security Force Regiment
MEF	Mission Essential Function
MET	Mission Essential Task
MEU	Marine Expeditionary Unit
MILCON	Military Construction
MIG	MEF Information Group
MLG	Marine Logistics Group
MTAC	Multiple Threat Alert Center
NCIS	Naval Criminal Investigative Service
NIPRNET	Non-Classified Internet Protocol Router Network
NTAS	National Terrorism Advisory System
O&M	Operations and Maintenance
OAG	Operational Advisory Group
OCONUS	Outside of Continental United States
OCS	Operational Contracting Support
OPFOR	Operating Force
OPLAN	Operations Plan
OPORD	Operations Order
OPR	Office of Primary Responsibility
OPREP-3	Operational Event/Incident Report-3
OPSEC	Operational Security
PAO	Public Affairs Officer
PEB	Program Evaluation Board
PHYSEC	Physical Security
PIR	Priority Intelligence Requirements
POA&M	Plan of Action and Milestones

POC	Point of Contact
POM	Program Objective Memorandum
PPBE	Planning Programming Budgeting Execution
PS DIV	Security Division (PP&O)
PSWG	Physical Security Working Group
RA	Risk Assessment
RAM	Random Antiterrorism Measure
RDD	Radiological Dispersion Device
RDP	Risk Decision Package
RED	Radiological Exposure Device
RM	Risk Management
RP	Risk Planning
SAF	Security Augmentation Force
SAR	Suspicious Activity Reporting
SICA	Supporting Infrastructure Critical Asset
SIPRNET	Secret Internet Protocol Router Network
SIR	Serious Incident Report
SJA	Staff Judge Advocate
SME	Subject Matter Expert
TCA	Task Critical Assets
TIC	Toxic Industrial Chemical
TIM	Toxic Industrial Material
TTL	Terrorism Threat Levels
TTP	Tactics Techniques and Procedures
TWG	Threat Working Group
TWR	Terrorism Warning Report
UFC	Unified Facilities Criteria
UNS	Universal Needs Statement

USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
U-UNS	Urgent Universal Needs Statement
VA	Vulnerability Assessment
VBIED	Vehicle Borne Improvised Explosive Device
WMD	Weapons of Mass Destruction