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

MCO 3058.1
PPO/PS/PSM
23 OCT 2014

MARINE CORPS ORDER 3058.1

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS MISSION ASSURANCE

Ref: (a) National Security Strategy, May 2010
(b) The National Military Strategy of the United States of America, February 8, 2011
(c) DoD Mission Assurance Strategy, May 7, 2012
(d) Marine Corps Service Campaign Plan (MCSCP), 2012-2020
(e) Marine Corps Doctrinal Publication 1, "Warfighting," June 20, 1997
(f) Mission Assurance Assessment (MAA) Benchmarks, current edition
(g) Commandant of the Marine Corps Policy Memorandum 1-11, "Advocacy," February 23, 2011
(h) United States Marine Corps (USMC) Protection Advocate Charter, June 10, 2013
(i) Mission Assurance Operational Advisory Group (MA OAG) Charter, April 2012
(j) Marine Corps Mission Assurance-Enterprise (MCMA-E) Road Map, Annex C, Appendix 11, MCSCP, January 6, 2012
(k) MCO 11000.11
(l) MCO 3501.36A
(m) MCO 3302.1E
(n) MCO 3440.9
(o) MCO 3440.8
(p) MCO 3030.1
(q) MCO 5239.2A
(r) MCO 3850.1J
(s) MCO 5580.2B
(t) MCO 6220.1
(u) MCO 5311.6
(v) Secretary of Defense Memorandum, "Final Recommendations of the Ft. Hood Follow-On Review," August 18, 2010
(w) 5 U.S.C. 552a
(x) SECNAVINST 5211.5E

Encl: (1) Mission Assurance Risk Management Methodology
(2) Acronyms and Definitions

1. Situation

a. Purpose. To publish MA policy and establish a process to align and synchronize the management of protection-related risk across the Marine Corps.

b. Background

(1) Per references (a) and (b), the Marine Corps operates in a hostile and uncertain environment shaped by a complex array of manmade and naturally occurring threats and hazards. The Marine Corps faces a growing number of potential adversaries with the ability to asymmetrically cripple vital force projection, warfighting, and sustainment capabilities by targeting critical military and civilian resources that support global operations. Additional challenges include catastrophic natural disasters and technological failures capable of producing high-impact second and third order effects that can disrupt Marine Corps missions. Per references (c) and (d), the Department of Defense (DoD) and the Marine Corps are addressing the challenges to mission execution in the current risk environment, while retaining the flexibility and agility necessary to plan for and respond to future protection needs.

(2) Per reference (c), MA is both a process and an integrative framework to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD Mission Essential Functions in any operating environment or condition. The MA 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 and the range of military operations.

(3) Per references (c) and (d), MA is both an effective and efficient means to protect the force and manage risk to missions the Marine Corps supports. Previously, the DoD and the Marine Corps regarded MA as the aggregation of independent protection-focused programs. This characterization did not support a comprehensive, integrated approach to Risk Management (RM) and has resulted in a lack of synergy, unnecessary duplication, and inefficiencies across programs. Efforts are underway to remedy this situation. Per reference (e), Marine Expeditionary Force (MEF) units and Supporting Establishment (SE) bases and stations must assess and develop plans to manage risk as an integrated part of the Marine Corps planning

process. Per reference (f), the Marine Corps MA Benchmarks document the standards used to provide a uniform approach to assess and assist in the management of risk across protection programs at the installation and command levels Service-wide. This Order builds upon these efforts, recognizing the need for a comprehensive, integrated MA framework and supporting process to protect the force, systematically manage enterprise risk, synchronize complementary protection-related programs and activities, and enable the prioritization of investments to ensure mission performance in a constrained fiscal environment.

(4) To better protect the force and manage mission risk, the MA process will leverage existing protection and resilience programs, including but not limited to the following: Antiterrorism (AT); Installation Chemical, Biological, Radiological, Nuclear, and High-yield Explosive (CBRNE) Protection; Counterintelligence; Marine Corps Critical Infrastructure Protection (MCCIP); Continuity of Operations(COOP); Fire and Emergency Services (F&ES); Cyber Security; Installation Emergency Management (IEM); Law Enforcement (LE); and Physical Security (PS). Although these programs operate under existing directives and other authorities, they shall adhere to the overarching guidance and processes established in this Order, and shall be more closely coordinated and integrated through the MA process established by the Deputy Commandant, Plans, Policies, and Operations (DC, PP&O). This MA process shall adhere to the governance structure established in references (g), (h), and (i) and include the Protection Advocate (PA), Protection Executive Steering Group (P-ESG), and MA Operational Advisory Group.

2. Mission. This Order establishes a Service-wide MA policy and assigns specific responsibilities for implementing a comprehensive, integrated, all-threats/all-hazards RM process across protection-related programs, functions, and operational capabilities enterprise-wide. This RM process shall be synchronized within the Marine Corps, and externally with other Services, DoD agencies, and civilian government and private sector organizations, as appropriate.

3. Execution

a. Commander’s Intent and Concept of Operations

(1) Commander’s Intent

(a) Purpose. Align, synchronize, and integrate multiple protection-focused policies, plans, programs, and activities which enable protection of the force and mission execution

through a comprehensive RM process. This process shall provide commanders at all levels with risk-based information that supports their ability to execute assigned missions, maintain required capabilities, and manage risk. This process will inform Service-level decision making and resource allocation at the Marine Requirements Oversight Council (MROC) level as part of the Program Objective Memorandum (POM) cycle, as well as current year budget execution by commanders across the Marine Corps.

(b) End State

1. Mission analysis and RA activities are aligned, synchronized, and uniformly implemented across protection-related programs and activities Service-wide.

2. Inputs from a unified assessment process inform decision making, resource prioritization, and RM actions at various levels across the Marine Corps, based on impacts to mission and capability execution and protect-the-force considerations.

3. Coordination and synchronization are enhanced between existing Service-level protection related programs, as well as with those of key external partners.

(c) Concept of Operations

1. MA is intended to achieve a consistent, enterprise approach to RM and synchronize protection-related programs to adequately protect personnel, facilities, installations, equipment, information and information systems, supporting infrastructure, and logistic chains. It also preserves the capability to generate, project, and sustain combat power per reference (b).

2. Using this approach, plans are developed, trade-offs are weighed, and resources are invested based on a common risk picture and risk-informed decisions made by leaders at all levels across the Marine Corps. Additional benefits shall be derived by eliminating or modifying duplicative or inefficient activities within specific programs that may create exploitable seams, expose the mission to undue risk, and/or inefficiently or unnecessarily expend scarce resources.

3. Consistent with the DoD Mission Assurance Strategy, reference (c), the Marine Corps' approach to MA implementation is based upon the following strategic pillars:

a. Increase Collaboration and Synchronize Policies, Tools, Information Sharing Mechanisms, and Investments across Protection-Related Programs. This pillar emphasizes closer coordination and enhanced information sharing between "mission owners" and "asset owners," as well as increased synchronization and integration of protection-related programs. To facilitate this coordination, MA advocacy forums such as MA Executive Committees (MAEC) and/or MA Working Groups (MAWG) shall be established enterprise-wide starting at the local command level. These forums shall comprise a diverse mix of asset owners, mission owners, protection program subject matter experts, non-DoD supporting infrastructure and service providers, and civilian first responder organizations, as appropriate. This advocacy structure shall provide both local commanders and Marine Corps senior leaders the opportunity to assess and make informed decisions regarding risk, capabilities, gaps, supporting programs, and resource priorities.

b. Implement a Comprehensive, Integrated All-Threats/All-Hazards MA RM Methodology and Process. A comprehensive, integrated, and well-understood RM methodology and process is essential to protecting the force, effectively executing Marine Corps missions, and achieving efficiencies across individual protection programs and activities. Enclosure (1) outlines the methodology and process that will unify the Service-wide approach to RM, including standardized assessment benchmarks and terminology. Use of this methodology and process will enable the examination of risk from an enterprise perspective and help identify risk trends and issues that individual commanders may not recognize or be able to manage adequately at their level. It will also facilitate the sharing of best practices and integrated approaches to RM across functional domains, programs, and asset types, and encourage continuous innovation as threats and vulnerabilities change over time.

c. Risk-Informed Decision Making through an Enterprise MA Framework and Supporting Processes

(1) An integrated, multi-level MA framework and supporting processes shall be established to enable the comprehensive assessment of risk; inform policy, plans, and resource allocation; and drive actions to manage risk effectively. Within this construct, many risk decisions will remain decentralized at the local command level. Strategically, however, the MA framework and supporting processes will: enable the management of risks that affect Service-wide mission performance; help determine Service priorities and economy-of-scale protection solutions; and provide risk-based inputs into the Service POM process.

(2) The key Headquarters Marine Corps (HQMC) elements that provide governance over the MA framework and processes include the designation of DC, PP&O as the Protection Advocate, per references (g) and (u), and the establishment of a P-ESG and an MA OAG, per references (h) and (i).

(3) MA advocacy forums (MAECs and MAWGs), comprised of asset owner and mission owner organizations and functional program representatives, shall be established across the enterprise. These forums shall be responsible for integrating outputs from the RA and gap analysis processes at their respective levels. They shall also provide recommendations regarding protection capabilities, gaps, and priorities across individual program elements through their chain of command to the Protection Advocate and, as necessary, in coordination with the Installation's Advocate to ensure mission success.

d. Partner with External Entities to Further Identify, Assess, and Manage Risk to Marine Corps Missions. MA implementation will require extensive collaboration between the Marine Corps and other DoD components, civilian government agencies, and private sector infrastructure operators and service providers. These external partners have key authorities, capabilities, and resources that are essential to the Marine Corps mission, both directly and indirectly. Hence, the Marine Corps shall seek greater collaboration with these entities regarding joint risk and interdependencies analysis, information sharing, scenario-based contingency and continuity of operations planning, all-hazards exercises, risk mitigation, and technological innovation. The Marine Corps shall also encourage those industries and service providers on whom it depends for mission support to design and use systems and processes that can withstand disruption and address single points of failure and supply chain vulnerabilities.

b. Tasks

(1) DC, PP&O shall:

(a) Oversee the implementation of the MCMA-E Roadmap, reference (j), and provide updates to the MCSCP, reference (d), and other relevant policy and strategy documents, as needed.

(b) Per references (g),(h), and (u), serve as the responsible authority for the development, coordination, integration, and/or synchronization of MA guidance, policies, strategies, concepts, doctrine, orders, specific programs, and

performance metrics. In addition, ensure senior leader awareness on cross-domain and cross-functional, Service-wide protection and MA process issues.

(c) Develop, implement, and oversee a Marine Corps-wide MA framework supporting processes and RM Methodology; and provide governance to the MA process via Protection Advocacy, and through the P-ESG and MA OAG.

(d) Oversee and lead a Service-wide MAA process and Mission Assurance Assessment Team (MAAT) Program that includes a standardized RM methodology, mission analysis, all hazards threat assessments, capability assessments, and assessment benchmarks applicable across protection-related programs per enclosure (1).

(e) Represent the protection community in interaction with the Marine Requirements Board and the MROC; coordinate resourcing issues through the appropriate Program Evaluation Boards (PEBs), POM Working Groups, and other Service POM enterprise bodies.

(f) Coordinate the identification of protection-related capabilities and capability gaps through the Protection Advocate Capabilities List and the Protection Advocate Gap List processes.

(g) Provide policy oversight, in conjunction with other Deputy Commandants, as required, on all protection-related programs in order to ensure Marine Corps MA and protection policies, processes, and activities are consistent with guidance provided by the Office of the Secretary of Defense (OSD) and the Office of the Joint Chiefs of Staff.

(h) Assist Commanding Generals, Marine Corps Combat Development Command (MCCDC), and Training and Education Command, in the development of MA- and protection-focused training and education standards and programs.

(i) Facilitate the integration of MA and protection considerations into existing and future Marine Corps training, education, and exercise programs and other activities.

(j) Recommend and/or advocate for updates to MA- and protection-related tasks in the Marine Corps Task List (MCTL) and the Inspector General Marine Corps (IGMC) functional areas checklists under the Functional Area Checklist Management and Processing System (FACMAPS).

(k) Coordinate the exchange of MA- and protection-related information and best practices across the Marine Corps, and in conjunction with other organizational elements of DoD and external entities, as appropriate.

(l) Review SE and Operating Forces (OPFOR) change requests submitted through the MA OAG and provide recommended modifications to the Table of Organization/Table of Equipment for MA- and protection-related force structure and equipment.

(m) Develop and integrate processes, coordinating structures, and activities to link protection-related program metrics to the Defense Readiness Reporting System - Marine Corps (DRRS-MC).

(n) Periodically review Marine Corps Orders corresponding to the programs that fall within the MA purview (references (k) through (t)). Coordinate with and make recommendations to their offices of primary responsibility (OPR) and other stakeholders to align and/or synchronize standardized RA and RM processes outlined in enclosure (1), as well as training, program reviews, exercises, and other considerations in accordance with this Order.

(2) Deputy Commandants, Separate Division Directors, Advocates, and Proponents shall:

(a) Support the overarching MA framework and supporting processes overseen by DC, PP&O.

(b) Support DC, PP&O in the development, coordination, integration, and synchronization of guidance, policies, strategies, concepts, doctrine, orders, specific programs, and performance metrics related to cross-domain and cross-functional, Service-wide protection-related program and MA process execution.

(c) Establish mechanisms and processes to support DC, PP&O in the development and implementation of a Service-wide MA framework to:

1. Comprehensively and consistently identify and assess risk to Marine Corps missions.

2. Identify protection-related capabilities and gaps and provide prioritized recommendations and funding assessments to inform Service resource planning, capabilities development, and acquisition processes following programming and force development guidance.

3. Develop and integrate processes, coordinating structures, and activities to link protection-related metrics to the DRRS-MC.

(d) Implement the Critical Asset Identification Process (CAIP), per reference (l), to identify critical assets associated with the Deputy Commandants'/Separate Division Directors'/Advocates' and Proponents' assigned functions and tasks.

(e) Assign personnel to participate in MA forums (including the MA OAG, MAECs, and MAWGs) to identify and prioritize protection-related capabilities, gaps, and RM courses of action.

(f) Review Marine Corps Orders corresponding to the programs that fall within their purview and coordinate with DC, PP&O to integrate and/or synchronize RA, RM, training, program reviews, exercises, and other considerations in accordance with this Order.

(g) Publish and maintain supporting orders/policies that implement the guidance and policy outlined in this Order.

(3) Deputy Commandant, Installations and Logistics. In addition to the requirements outlined in Section 3b(2), shall establish a process and procedure to ensure outputs from the MA RM Methodology and MA Assessment Reports are included in all aspects of the facilities engineering planning process to include the prioritization of funds for military construction and Facilities, Sustainment, Restoration, and Modernization protection- related projects.

(4) Commanders, Marine Forces; MCCDC; Marine Corps Installations Command (MCICOM); and Marine Corps Recruiting Command shall:

(a) Support and participate in the overarching MA forums overseen by DC, PP&O.

(b) Support DC, PP&O in the development, coordination, integration, and synchronization of guidance, policies, strategies, concepts, doctrine, orders, specific programs, and performance metrics related to cross-domain and cross-functional, Service-wide MA and protection issues.

(c) Support DC, PP&O in the implementation of a Service-wide RM process to:

1. Identify and assess risk to Marine Corps missions per the guidance provided in enclosure (1).

2. Identify protection-related capabilities and gaps that impact the ability to execute Marine Corps missions, core capabilities, and functions, and provide prioritized recommendations and funding assessments to inform Service resource planning, capabilities development, and acquisition processes in accordance with relevant programming and force development guidance.

3. Ensure coordination, synchronization, and integration of individual protection-related programs, including, but not limited to: AT, CI, MCCIP, COOP, IEM, Cyber Security, Installation CBRNE Protection, PS, LE, and F&ES.

4. Implement processes, coordinating structures, and activities to link protection metrics to DRRS-MC.

(d) Establish, maintain, and assign personnel to participate in cross-functional MA advisory forums (including MAECs and MAWGs) that bring together the OPFOR and SE, tenant organizations, and functional area program representatives to identify, synchronize, and implement RA and RM activities.

(e) Assist in the prioritization of capabilities, gaps, and resource requirements supporting the Marine Corps Force Development System (MCFDS); DoD Planning, Programming, Budgeting, and Execution (PPBE) process; and other decision support processes, in coordination with external entities as appropriate.

(f) Implement MA at all levels within their commands (including MEF and MCICOM subordinate headquarters), including, but not limited to, the following key activities:

1. Designate a Mission Assurance Officer to ensure application of the MA process and RM Methodology across all protection-related programs at the command and installation levels.

2. Establish, maintain, and assign personnel to participate in cross-functional advisory forums (including MAECs and MAWGs) that bring together OPFOR, SE, tenant organizations, and functional program representatives to identify, synchronize, and implement RA and RM activities.

3. Assist in the prioritization of capabilities, gaps, and resource requirements supporting the MCFDS, PPBE, and other decision support processes, in coordination with external entities as appropriate.

4. Develop and implement plans to address and manage identified risk as part of the Marine Corps Air Ground Task Force (MAGTF), command, and installation planning process.

5. Conduct or participate in annual all-threats/all-hazards protection exercises to ensure the integration of various protection-related requirements at the command and installation levels.

6. Conduct annual program reviews of all Major Subordinate Commands (MSCs) with an on-site review conducted triennially to ensure compliance with program standards contained in the MA benchmarks, per reference (f), and provide corrective action assistance as necessary.

7. Conduct annual self-assessments and ensure the scheduling of triennial MAAs on all subordinate bases, stations, and installations and maintain the capability to provide follow-up assistance for all assessed commands.

8. Implement the CAIP to identify critical assets associated with missions, capabilities, and functions.

9. Ensure use of the Marine Corps Critical Asset Management System (Next Generation) (MC-CAMS NG) for documentation of all RA and RM plans.

10. Ensure coordination with all tenant commands and among all individual protection program elements in the development of installation protection capabilities, identification of protection gaps, and implementation of RM activities.

11. Establish Memoranda of Understanding/ Agreement with external entities as required to support MA and protection requirements.

12. Publish and maintain supporting orders, policies, and plans that implement the guidance and policy outlined in this Order.

(5) Commanding General, MCCDC, shall:

(a) Develop and maintain MA training standards to support individual and unit training in accordance with this Order.

(b) Integrate MA and protection considerations into the MCTL, and identify the specific sub-tasks that are aligned with the MA process.

(6) Commanding Generals of Service Components of Geographic Combatant Commands, in addition to the requirements outlined in paragraph 3b(4) above, shall: Conduct annual MA program reviews in accordance with the higher headquarters (HHQ) MA program review

benchmarks (enclosure 1) of all SE Commands, with an on-site review conducted triennially.

(7) Commanding General, Marine Corps Forces Cyber Command, in addition to the requirements outlined in paragraph 3b(4) above shall:

(a) Support DC, PP&O in the development, coordination, integration, and synchronization of guidance, policies, strategies, concepts, doctrine, orders, and performance metrics related to Marine Corps MA and protection issues.

(b) Identify and assess risk to Marine Corps cyber capabilities, functions, and missions.

(c) Identify cyber-focused protection capabilities and gaps and provide prioritized recommendations for reducing those gaps, along with funding assessments to inform Service resource planning, capabilities development, and acquisition processes in accordance with programming and force development guidance.

(d) Assist DC, PP&O in establishing requirements for, synchronizing, and coordinating the exchange of cyber-focused protection information and best practices across the Marine Corps, and in conjunction with other organizational elements of DoD and other key external entities.

(e) Publish and maintain supporting orders/policies that implement the guidance and policy outlined in this Order.

(8) Inspector General of the Marine Corps (IGMC). Coordinate with the Assistant Deputy Commandant PP&O PS (Security Division) regarding integration of the provisions of this Order into the FACMAPS discrepancy listing.

(9) Marine Corps Tenant Activities

(a) Participate in the host installation's MA forums and supporting processes, as appropriate.

(b) Coordinate and participate in RA and RM activities sponsored by the host installation.

(c) Support and participate in host installation exercise activities, as appropriate.

(d) Execute the CAIP and enter Baseline Elements of Information (BEI) into MC-CAMS NG.

(e) Provide CAIP information to HHQ and the host installation to support the installation-level RA process and other HQMC requirements.

(f) Participate and support installation commanders in the execution of their Continuous Evaluation Program and access control policies to include contractor vetting via the MAWG and other related forums.

c. Coordinating Instructions

(1) The MA framework and supporting processes discussed above are designed to interface with other advocates at HQMC, as well as support the Service's existing PPBE process, with a focus on managing protection-related risk across the USMC enterprise.

(2) MC-CAMS NG is the primary MA support tool for managing mission and asset data and for RM and RA activities. This system also provides the means to share information throughout the enterprise, horizontally and vertically.

(3) The Command, Control, Communications, Computers, and Intelligence (C4I) Suite shall be used to report events for shared situational awareness, while omitting detailed personal information, or information that is considered sensitive. The C4I Suite, when used in conjunction with the established tactical systems currently employed, will provide the capability to communicate across all levels of the chain of command and share real time threat information across the Service, as directed by reference (v).

(4) Commanders with off-installation facilities or Stand Alone Facilities (SAF) shall conduct RM activities as part of their annual MA process and supporting activities. Marine Corps tenants aboard SAF shall coordinate with and support the host facility's MA forums and associated RM activities. Under the joint basing concept, other service/agency tenants will coordinate with and support the host facility's MA and RM processes.

4. Administration & Logistics

a. DC, PP&O is the OPR for this Order. HQMC PP&O Security Division is the point of contact for correspondence related to this Order.

b. Recommendations for changes to this Order should be submitted to DC, PP&O via the appropriate chain-of-command.

c. The generation, collection or distribution of personally identifiable information (PII) and management of privacy sensitive information shall be in accordance with the Privacy Act of 1974, as amended, per references (w) and (x). Any unauthorized review, use, disclosure or distribution is prohibited.

5. Command and Signal

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

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

R. L. BAILEY
Deputy Commandant
Plans, Policies, and Operations

DISTRIBUTION: PCN 10203061000

Mission Assurance Risk Management Methodology

1. General. MA uses a risk-based framework to create synergies in implementing a standardized process for managing risk to the OPFOR and SE in the execution of their assigned missions, core functions, and related capabilities. MA also integrates and synchronizes numerous protection programs and other activities across the enterprise. This enclosure provides policy and procedures for a uniform, mission-focused, RM process to be employed Marine Corps wide.

a. Goal. To identify and implement a uniform process for identifying and managing risk to assets that support the execution of Marine Corps missions and core functions/ capabilities Service-wide. This mission-based approach also allows alignment and prioritization of effort across protection-related programs.

b. RM Responsibilities. RM enables prioritization of protection capabilities and capability gaps, informs decision making, and provides for more focused resource allocation.

(1) Marine Corps Installations. Commanders shall execute RM as part of their annual MA process and supporting activities. Marine Corps tenant commands shall coordinate with and support the host installation's MA forums, supporting processes, and associated RM activities. Under the joint basing concept, other service/agency tenants should coordinate with and support the host installation's MA and RM processes.

(2) OPFOR. Commanders shall execute RM as part of their operational planning per reference (d). RM principles are integrated into mission planning, preparation, and execution in all areas of operation. When OPFOR units are tenants aboard USMC installations, other service installations, or joint bases, OPFOR commanders shall coordinate with and support their host installation's RM process.

(3) Marine Corps SAFs. SAFs shall conduct RM activities annually as part of the MA process.

(4) Assessments. Both HHQ and annual local assessments shall utilize the most current Marine Corps Mission Assurance Assessment (MCMAA) benchmarks, reference (f), and other approved directives/guidance when performing OPFOR, installation, facility, and asset assessments.

(a) HHQ RAs. All Marine Corps installations and OPFOR units that are tenants on installations shall be subject to a MAA triennially. These assessments shall focus on installation and tenant missions and associated critical assets, as well as applicable

protection-related programs. Each assessment will evaluate the assessed command's RM execution, provide recommendations, and help advocate for improvement of the command's overall protection posture and those programs that support it.

(b) Annual Self-Assessment. MEF MSCs and installation commanders shall conduct RAs annually, or more frequently, if the hazard/threat environment or mission requirements dictate. Commanders shall also conduct RAs for any event or activity deemed as a special event or which involves a gathering of 300 or more DoD personnel. DoD facility directives also require that a detailed RA be performed annually on utility systems. This self-assessment can be used to fulfill the annual requirement for utility systems identified as Supporting Infrastructure Critical Assets (SICA) within the RA.

2. Risk Management (RM). RM involves the application of a standardized process to identify, assess, and manage risk and enable decision making that balances risk and cost with mission benefits. RM allows the commander to decide how best to employ allocated resources to reduce risk, or, where circumstances warrant, acknowledge risk. RM consists of two core activities: RA and risk planning.

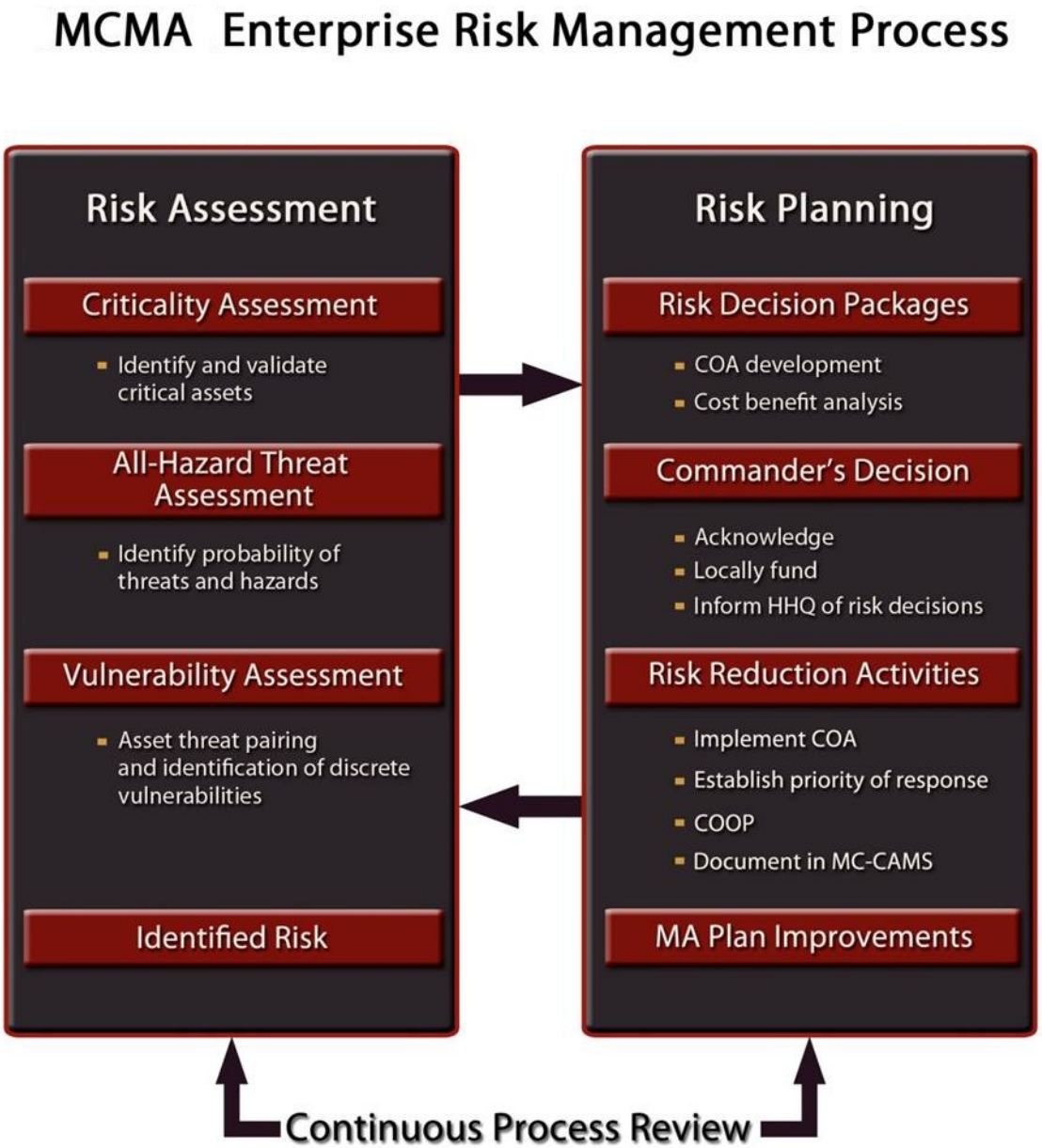

Figure 1.--MCMA-Enterprise Risk Management Process

a. Risk Assessment (RA). An RA involves the collection and evaluation of data concerning asset criticality based on mission impacts, probable threats and hazards, and degree of vulnerability to determine the overall risk posture of the asset. An RA involves a systematic, rational, and defensible process for identifying, quantifying, and prioritizing risks. A RA involves the collection and evaluation of data in three core areas:

(1) Criticality Assessment (CA). A CA involves assessing the total impact (failure or severe degradation) on the execution of missions or functions supported by an asset, should that asset be

unavailable for any reason. The CA identifies assets whose degradation or destruction impacts the command's ability to execute its assigned mission or functions. Commanders are required to conduct an annual CA utilizing the following process: 1) identify missions, functions, and associated standards and conditions for mission/function execution; 2) identify assets whose loss or unavailability will result in mission failure or severe degradation (mission impact).

(a) Mission Analysis. Mission Analysis provides the core foundation for conducting the CA. The overall objective of mission analysis is to gain an understanding of the missions executed by a command, as well as how they are 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 must involve close coordination between tenant commands and host installations.

(b) Commander's Guidance. Commander's guidance is utilized to develop 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, 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, or functions. Assets can include personnel, equipment, facilities, information and information systems, infrastructure, and supply chains which support the execution of the command's mission and associated critical functions. The DoD CAIP shall 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. These could include assets such as theaters, commissaries, base exchanges, etc., that present significant issues related to force protection.

(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 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 SICAs. The third involves the analysis of each SICA to identify any further SICAs, going at least one node beyond

the facility. During this analysis, BEI must be collected for each asset and entered into MC-CAMS NG. 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, regardless of whether the asset is owned by the Marine Corps, other DoD components, other governmental entities, or the private sector.

(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 Marine Corps Asset Prioritization Methodology (MC-APM) tool, or MC-CAMS NG when mission and mission impact data is populated in these tools (See paragraph 2, RM Process and Tools, for a discussion of tools and supporting metrics). This asset criticality rating is also used as the CA rating in the Marine Corps Asset RA (MC-ARA) methodology and tool. Along with Threat/Hazard (T/H) 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 based on an assessment of the threat and hazard environment in which Marine Corps forces and installations operate and 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. An AHTA shall be executed annually, tailored to the local environment and ensuring all threat and hazard information is integrated to meet the command's effort to manage risk to missions, personnel, and assets. The AHTA also supports a consistent view of the threat/hazard environment to support AT, CBRNE, CIP, IEM, LE, F&ES, 911 dispatch, PS, and COOP planning. A collaborative effort among the membership of the MAECs and MAWGs representing the various protection-related programs (CBRNE, IEM, CIP, AT, PS, and LE) will be required to develop the AHTA. The AHTA is also based on the fusion of information (strategic, operational, and local/tactical) derived from liaisons between civil and military LE; public safety agencies and departments; and meteorological, environmental, public health, and medical syndromic surveillance sources. 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 (See Figure 2 - Individual Threat/Hazard Analysis Data Matrix).

(a) T/H Analysis. Analysis must be conducted to identify a T/H baseline that could adversely impact command assets[1] (See Figure 2 – Individual T/H Analysis Data Matrix). The results of this annual AHTA analysis shall be integrated into all aspects of the RM process.

[1] When discussing execution of VAs below, the assessor must align one or more identified threats/hazards to one or more vulnerabilities of assets or the installation that could be exploited by the threat or hazard.

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. 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; DIA 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
	EMP	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 2-1.--Individual Threat/Hazard Analysis Data Matrix

(b) T/H Probability Ratings and Definitions. Once a T/H baseline 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 T/H probability ratings can be found in the MC-ARA stand-alone tool, located on the HQMC PS Division SharePoint Portal:

https://ehqmc.usmc.mil/org/ppo/PS/PSM/MAAT/Shared%20Documents/Forms/AllItems.aspx.

They are also embedded in MC-CAMS NG tool. 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 -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) T/H Categories

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

2. Hazards are broken down into two categories: Natural Hazards and Accidental Events. Each of these sub-areas is further described below.

a. Natural Hazards: The Natural Hazards category includes Geological, Meteorological, and Biological hazards. The Geological category includes volcanos, tsunamis, earthquakes, and landslides. The Meteorological category includes: hurricanes; tornados; drought; winter weather; fire; extreme heat; lightning; hail; wind; rain; and flooding. The Biological category includes diseases that impact humans or animals such as plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (also known as SARS), pandemic disease, bovine spongiform encephalopathy, etc.

b. Accidental 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, from events that result from human error (man-made) to those accidental events that are caused by technology or technological failures. Incidence ranges and frequency must align with the Hazard probability definitions (Low, Medium, High, and Critical) to determine the overall probability rating. Examples of various types of Accidental Events include, but are not limited to:

(1) Man-made accidental events such as construction accidents (e.g., a back-hoe that unintentionally cuts a power, water, fuel, or communications line) or inadvertent hazardous materials spills.

(2) Wildlife-induced accidental events, such as wildlife accessing and damaging assets (e.g., wildlife shorting out electrical transformers).

(3) Technologically-caused accidental events such as aging assets and infrastructure that are past their normal life cycles and fail in some way; equipment failure caused by power surges or "dirty" power; equipment overheating (e.g., servers when the 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 data bases.

(e) Sources of Threat Assessment Data. The MCMAA Program has established a detailed list of authoritative sources that support the development of the AHTA. The AHTA Methodology can be found on the HQMC Mission Assurance Assessment SharePoint Portal: https://ehqmc.usmc.mil/org/ppo/PS/PSM/MAAT/Shared%20%20Documents/Forms/AllItems.aspx.

(3) Vulnerability Assessment (VA). The VA process 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. A VA is a systematic examination of the characteristics of an installation's system, asset, application, or its dependencies to identify vulnerabilities that could be susceptible to the effects

of any number of threats or hazards. VAs shall be conducted by teams of subject matter experts with backgrounds in different functional areas such as PS, AT, CIP, CI, and installation integrated protection. VAs will be conducted as follows:

(a) Identify and assess all vulnerabilities to the installation, facilities, and assets, specifically including all identified critical assets. Vulnerability is defined as a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard effects. Vulnerabilities can result from a wide variety of factors such as design and construction flaws, environmental factors, proximity to other structures or systems, factors influencing accessibility, personal behaviors of individuals 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 installation access or perimeter control may lead to an adversary gaining access to the installation, and ultimately to an asset located somewhere on site.

(b) Align specific T/Hs to asset vulnerabilities. Threat-vulnerability pairing is conducted to link likely threats and hazards to specific asset vulnerabilities that may be susceptible to a specific T/H. This process is crucial because individual assets may have a greater degree of vulnerability to different threats or hazards. Threat-vulnerability pairing, in turn, will support the preparation of effective risk reduction plans designed to lower overall risk by incorporating and addressing both T/H and VA in those plans.

(c) Identify degrees of vulnerability. When assessing and identifying vulnerabilities, the assessor needs to make a judgment as to the significance or degree of an identified vulnerability. For example, lack of appropriate standoff around a high population building may be identified as a vulnerability, based on Unified Facility Criteria (UFC) requiring 25 meters of standoff distance with an actual standoff distance of 24 meters. 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 Vehicle Borne Improvised Explosive Device (VBIED) that the UFC requirement was designed to address. Identifying 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 MC-ARA tool and MC-CAMS NG.

(d) Vulnerability Ratings Definitions

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

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

3. High (.51 to .75): Indicates some effective countermeasures in place, but multiple known weaknesses exist through which adversaries, natural hazards, or accidental disruptions would be capable of causing loss of or disruption to asset.

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

(4) Risk Rating. A risk rating is established based on the values produced from the CA, AHTA, and VA. Risk is determined by the following equation: criticality rating x T/H rating x vulnerability rating = risk rating. MC-CAMS NG provides an integrated set of metrics to establish a risk rating. The risk rating is produced for each specific T/H and vulnerability/asset data pairing.

b. Risk Planning. The objective of the RM methodology is to enable the management of risk based on a holistic approach that cuts across individual programs and capabilities such as AT, CIP, PS, IEM, LE, Installation CBRNE Protection, 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. The RA process seeks to evaluate and identify asset risk of loss based on an asset's criticality (mission impact), the probability of the occurrence of specific threats and hazards, and associated degrees of vulnerability. Risk planning is the process of determining options or courses of action to reduce the risk of loss to the asset, and, thus, reduce impact to mission execution. To support the development of risk reduction plans, commands can leverage elements of the MA process such as the MAECs and/or MAWGs, or establish a risk reduction planning team consisting of experienced personnel with necessary expertise. Risk reduction planning and associated decision-making involve a number of specific considerations and steps, including:

(1) Risk Reduction Planning. Commanders shall implement effective and efficient risk reduction courses of action whenever possible. Examples include, but are not limited to: PS measures; personal protection measures; cyber security measures; building redundancy in assets critical to mission execution; etc. Risk reduction planning courses of action can involve efforts to implement risk reduction measures both 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 Packages (RDPs). RDPs represent one or more courses of action designed to address and reduce identified risk to assets and missions. RDPs are developed to assist commanders in risk decision making. RDPs shall be documented in MC-CAMS NG for all Tier I-III critical assets, at a minimum. The following elements shall 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 estimated reduction in risk anticipated.

(b) Cost Benefit Analysis. Proposed risk reduction courses of action identified as part of any risk reduction plan should include a cost-benefit analysis. The following shall be considered as part of this analysis:

1. Doctrine: policy, procedures, guidance, and agreements with internal and external tenant commands/agencies.

2. Organization: structure and location.

3. Training: formal, informal, and situational.

4. Material: physical, cyber, financial resources, and redundancy.

5. Leadership: education, knowledge, and experience.

6. Facilities: physical, access, security, and resilience.

7. Cost comparison: the cost of risk reduction versus the cost of mission disruption if risk reduction measures are not implemented.

(c) Analyze Options and Determine the Best Approach. This step focuses on analysis of one or more courses of action to determine the option that represents the most "bang for the buck." Use of the MC-ARA tool or MC-CAMS NG 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 reduce risk.

(d) Develop and Coordinate the Risk Reduction Plan. This step involves development of a Plan of Action and Milestones (POA&M) 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 shall include details concerning the asset; specific T/Hs to which the asset is vulnerable; information concerning the command's decision to reduce risk; and resource requirements needed to execute the plan.

(e) Implement the Risk Reduction Plan. This step follows plan approval and involves the tracking of the milestones developed

in the above POA&M and the measurement of success in reducing risk previously identified. Plan effectiveness is assessed through the command's annual exercise program or through a HHQ RAs, such as a MCMAA.

(f) Acknowledgement of Risk. Commanders have several options in weighing risk. Risk can be acknowledged, locally funded, or reduced by implementing remediation measures to reduce the risk, or the risk element can be forwarded to HHQ for funding or other consideration. Unless prohibited by a higher authority, a command may decide to "acknowledge risk" to assets where appropriate, rather than dedicating resources to reduce identified risk. Risk may be acknowledged by the command 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. The command also may acknowledge risk temporarily where resources are not currently available to support desired risk reduction courses of action. In these cases, documenting acknowledgement of risk in MC-CAMS NG is also the first step to be undertaken to identify such risk up the chain of command.

(g) HHQ Risk-Informed Decision Making. Commanders shall prioritize proposed risk reduction courses of actions that cannot be implemented at their level for current year or POM funding solutions. When effective and efficient countermeasures cannot be implemented immediately, commanders shall prioritize any remaining risks to compete for funding solutions. 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 current year funding or via the PPBE process or the MA process. People at all levels within the Marine Corps continuously update their RAs to alert the commander to emerging threats and associated vulnerabilities which need to be addressed. At the installation level, typical factors to consider in the development of risk reduction plans include, but are not limited to: PS and access control; cyber security; personnel security; facility design; critical asset and infrastructure resilience and redundancy; emergency response planning and resourcing; and training and exercises (See Figure 1 for an outline of the MCMA-E RM process).

(h) 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 by intentional conduct or by a natural or unintentional manmade disaster or hazard. All installations shall conduct capability assessments and consider contingency planning activities. Planners shall 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. MC-ARA and/or MC-CAMS NG shall be used to prioritize risk to assets, as well as to prioritize impact of critical assets on all the missions supported by the asset. These tools and processes generate priority values for impact to missions and the identification of risk. Risk reduction efforts will focus on obtaining optimal risk reduction and the most effective/efficient use of resources.

(i) Required Risk Reduction Plans. Risk reduction planning includes the development of the following plans which are typically implemented during or after an event, or upon receipt of warning of an impending event:[2]

1. Installation Emergency Response Priority Plan. This plan establishes first responder and other emergency response priorities with a focus on mission continuity once life-saving activities are executed.

2. Utility Restoration Priorities. This plan identifies the priority for restoring utility infrastructure (e.g., electricity, water). Priority of restoration shall take into account restoration of utilities supporting critical asset operations.

[2] All risk reduction plans must be documented in MC-CAMS NG.

Priority restoration plans shall be identified and integrated for critical assets supporting both installation and tenant commands.

3. Installation Security Response Priorities. These plans address actions taken in concert with threat/hazard indications and warnings which necessitate an escalation in security response capability and/or security measures. Examples of these plans include: the Security Force Augmentation Plan, Random AT Measures Implementation Plan, and FP Condition Action Sets Plan. Security response and protection measure priorities shall be identified for locations housing critical assets, including those critical assets owned by tenant commands, within the overall host installation security response priority planning.

4. Continuity of Operations Plans. These plans integrate Marine Corps COOP requirements with existing protection policies and programs focused on the protection of critical resources and infrastructure and continuation of Mission Essential Functions.

5. Reconstitution Plans. These plans are developed in advance of an event to address the loss of critical assets that support installation and tenant command missions, tasks, and essential functions.

(2) Process Review. Assessing risk and conducting risk reduction planning is part of a continuous cycle. Although commands are required to assess risk annually, a command's missions, threats/hazards, and vulnerabilities can change at any time. Risk shall be re-evaluated as these changes occur.

(a) Updating Critical Asset Risk Profile/Rating. Update critical asset risk profiles/ratings annually or when changes in the criticality, threats/hazards, or vulnerability occur. Significant increases in risk profiles/ratings may require changes in risk reduction plans or strategies and resource priorities.

(b) Program Review. Once the annual RM process is complete, it is essential to conduct a thorough review of the overall process. This is typically accomplished as part of the annual program review.

(c) Refine RM Plan. The RM process is executed in a cycle. Revisions to plans shall be accomplished and documented to enable plan improvement.

(d) Coordinate with Stakeholders. Commanders shall ensure that stakeholders in the military and local civilian communities are involved in the process review. This collaboration will ensure that supporting plans align with the RM process. Local community stakeholders can also help identify strengths and weaknesses, focusing on collaboration between military and civilian agencies. Complex operating environments magnify the importance of coordinating with OPFOR and SE installations. In order for commanders to effectively manage risk, those with protection responsibilities should possess a solid understanding of the local customs, culture, and society in which they operate. Interfacing and coordinating preventive and/or response measures with local stakeholders will help 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 involves the exercising of risk reduction plans that have been implemented during annual exercises, and making adjustments as needed.

3. Risk Management Processes and Tools. The following is a list of processes and tools required to be used in the execution of MCMA-E RM process.

a. MC-CAMS NG. MC-CAMS NG is a mission and asset RM-focused data management system which is designed to provide operational and contingency planning support for multiple MA and RM tasks and requirements. MC-CAMS NG is used to enter RM data, including RA and risk reduction planning results and information. MC-CAMS NG incorporates both the MC-APM and the MC-ARA Methodology. Where appropriate, MC-CAMS NG will automate the sharing of RM data with other DoD Components and data management systems.

b. MC-APM. The MC-APM is a standardized, mission-focused methodology that supports prioritization of Marine Corps assets and

infrastructures – both critical and non-critical. Prioritization is based solely on the following metrics related to the mission and its execution:

(1) Level of Task, Function or Capability (e.g., tactical level to strategic level).

(2) Mission Impact (Failure, Severe Degradation, or No Significant Impact).

(3) Time to Mission Impact (time from asset unavailability to the time mission is impacted).

(4) Time to Restore the Asset or its capability provided to the mission (assume asset is completely destroyed).

(5) Elements (1)-(4) are captured for every mission, task, and function that the asset supports.

Each of these data elements must be captured and entered into MC-CAMS NG to enable the prioritization of assets. All identified assets will have their asset priority score determined by use of the MC-APM.[3]

c. MC-ARA. This stand-alone tool provides an integrated set of metrics and definitions that support a standardized process for the identification and analysis of criticality, T/H, and VA functions resulting in the production of a risk rating. These same RA metrics and methodology are also imbedded in MC-CAMS NG. Each of the RA data elements (mission impact, threats, and vulnerabilities) must be captured and entered into MC-CAMS NG.

[3] Asset priority value is also the impact value or score that is utilized in the MC-ARA methodology and tool to support the determination of risk of loss to the critical asset.

Acronyms and Definitions

Part I: Acronyms

AHTA	All Hazards Threat Assessment
AT	Antiterrorism
BEI	Baseline Elements of Information
CA	Criticality Assessment
CAIP	Critical Asset Identification Process
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-yield Explosive
C4I	Command, Control, Computers, and Intelligence
CI	Counterintelligence
CMC	Commandant of the Marine Corps
COOP	Continuity of Operations
DC, PP&O	Deputy Commandant, Plans, Policies, and Operations
DCA	Defense Critical Asset
DoD	Department of Defense
DRRS-MC	Defense Readiness Reporting System - Marine Corps
F&ES	Fire and Emergency Services
FACMAPS	Functional Area Checklist Management and Processing System
FP	Force Protection
FSRM	Facilities Sustainment, Restoration, and Modernization
HHQ	Higher Headquarters
HHQ RA	Higher Headquarters Risk Assessment
HQMC	Headquarters Marine Corps
HVAC	Heating, Ventilation, and Air Conditioning
IAW	In Accordance With
IEM	Installation Emergency Management
IGMC	Inspector General Marine Corps
LE	Law Enforcement
MA	Mission Assurance
MA OAG	Mission Assurance Operational Advisory Group
MAA	Mission Assurance Assessment
MAEC	Mission Assurance Executive Committee
MAGTF	Marine Corps Air Ground Task Force
MAWG	Mission Assurance Working Group
MC-APM	Marine Corps Asset Prioritization Methodology

MC-ARA	Marine Corps Asset Risk Assessment
MC-CAMS NG	Marine Corps Critical Asset Management System (Next Generation)
MCCDC	Marine Corps Combat Development Command
MCCIP	Marine Corps Critical Infrastructure Protection
MCDP	Marine Corps Doctrinal Publication
MCFDS	Marine Corps Force Development System
MCICOM	Marine Corps Installations Command
MCMAA	Marine Corps Mission Assurance Assessment
MCMA-E	Marine Corps Mission Assurance-Enterprise
MCO	Marine Corps Order
MCSCP	Marine Corps Service Campaign Plan
MCTL	Marine Corps Task List
MEF	Marine Expeditionary Force
MET	Mission Essential Task
MILCON	Military Construction
MROC	Marine Requirements Oversight Council
MSC	Major Subordinate Command
OPFOR	Operating Forces
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
PEB	Program Evaluation Board
P-ESG	Protection Executive Steering Group
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PS	Physical Security
RA	Risk Assessment
RDP	Risk Decision Package
RM	Risk Management
SAF	Stand Alone Facility
SARS	Severe Acute Respiratory Syndrome
SE	Supporting Establishment
SECDEF	Secretary of Defense
SICA	Supporting Infrastructure Critical Asset
T/H	Threat/Hazard
TCA	Task Critical Asset
TECOM	Training and Education Command
UFC	Unified Facility Criteria
USMC	United States Marine Corps

VA	Vulnerability Assessment
VBIED	Vehicle Borne Improvised Explosive Device

Part II: Definitions

Advocate Capabilities List (ACL). Marine Corps capabilities comprised of functional tasks, applicable conditions, and required standards.

Advocate Gap List (AGL). An assessment of the ability of the programmed force to provide the capabilities called for in the ACL.

All-Hazards and Threats. Any incident, natural or manmade, including those defined in DoDI 6055.07, which warrants action to protect the life, property, health, and safety of military members, dependents, and civilians at risk, and minimize any disruptions of installation operations. Also referred to as All-Threats/All-Hazards. (DoDI 6055.17)

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. (JP 1-02)

Asset. A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40)

Chemical, Biological, Radiological, Nuclear and High Yield Explosive (CBRNE). An emergency resulting from the deliberate or unintentional release of nuclear, biological, radiological, or toxic or poisonous chemical materials, or the detonation of a high-yield explosive. (MCO 3440.8)

Common Operating Picture (COP). A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 3-0)

Continuity of Operations (COOP). An organization’s ability to continue its Mission Essential Functions with little or no interruption during, and in the aftermath of an emergency. (MCO 3030.1)

Counterterrorism (CT). Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Also called CT. (JP 1-02)

Critical Asset Identification Process (CAIP). Provides a standardized methodology for identifying assets that are critical to the execution of a command's missions, functions and/or core capabilities. Used to conduct the criticality assessment portion of the Marine Corps RA process across all mission areas and programs. (JP 3-07.2 / DoDM 3020.45 (Vol. 1)

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a serious, debilitating effect on the ability of the DoD to fulfill its missions. (DoDD 3020.40)

Defense Critical Infrastructure Program (DCIP). A program that takes action to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc. Also called CIP. (DoDD 3020.40)

Force Protection (FP). Actions taken to prevent or mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. (JP 1-02)

Installation Emergency Management (IEM). A program designed to provide the integrated planning, execution, and management of response efforts (designed or intended) to prepare for, respond to, and recover from the effects of an "all-hazard" incident, to include but not limited to, natural hazards, human-caused events, and technologically-caused events to protect the force and allow freedom of maneuver to meet National Military Strategic requirements. (MCO 3440.9)

Marine Corps Air Ground Task Force (MAGTF). A term used by the Marine Corps to describe the principal organization for all missions across the range of military operations. MAGTFs are a balanced air-ground, combined arms task organization of Marine Corps forces under a single commander that is structured to accomplish a specific mission.

Marine Corps Force Development System (MCFDS). A process used to develop future warfighting capabilities to meet national security objectives. The system guides the identification, development, and integration of warfighting and associated support and infrastructure capabilities for the MAGTF. (MCO 3900.15A)

Marine Requirements Oversight Council (MROC). Principal body advising the Commandant on policy matters related to concepts, force structure, and requirements validation.

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

Marine Corps Mission Assurance Enterprise Roadmap (MCMA-E). Provides the framework and Service-level direction to develop and integrate protection-related programs, activities, functions, and operational capabilities using a comprehensive, all-hazards approach. Specifically, this approach is structured to enhance the overall protection of the OPFOR and SE in order to ensure mission execution and accomplish the specified and implied tasks identified in the MCSCP. The MCMA-E aligns planning and resource activities; synchronizes policy, doctrine, and capabilities development; and integrates functional area management across the enterprise.

Mission Assurance (MA). Both an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets - including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains - critical to the performance of DoD MEFs in any operating environment or condition. (DoD Mission Assurance Strategy, May 2012)

Mission Assurance Assessment Team (MAAT). A group of subject matter experts established by the HQMC PP&O Security Division to conduct an all-threats/all-hazards RA to provide base and installation commanders with a clear understanding of risk exposure. These assessments integrate all aspects of protection, providing the commander with information necessary to support an integrated RM decision process. (CMC MSG DTG: 141427Z Apr 10)

Mission Assurance Operational Advisory Group (MA OAG). A forum chartered to make recommendations on how the USMC should organize, man, train, and equip USMC OPFOR and the SE to protect and sustain MEFs, personnel, and resources. The MA OAG recommends protection program priorities and provides direct interaction among the Deputy Commandants, other HQMC Departments, and the SE, as well as other representatives concerned with issues involving protection programs.

Mission Assurance Executive Council (MAEC). An installation- or command-level executive body that assesses, integrates, and synchronizes protection-focused capabilities, programs, and resource investments - including existing, planned, and emergent requirements for identifying risks, and informing and prioritizing protection courses of action to the commander for decision so that finite resources can be better allocated. The MAEC provides a single, multi-disciplinary entity to review all-threats/ all-hazards protection and MA issues, recommend changes, recommend resource priorities, and monitor the implementation of MA policy.

Mission Assurance Working Group (MAWG). A body comprised of a diverse mix of asset owners, mission owners, program managers, and non-DoD support or civilian community-focused entities at the command and installation level. The MAWG facilitates the interdisciplinary coordination between subject matter experts designed to assist with the MA advocacy process.

National Military Strategy (NMS). A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain National Security Strategy and National Defense Strategy objectives. **(**JP 3-0)

Physical Security (PS). Active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, material, and documents, and to safeguard them against sabotage, damage, and theft.

Planning, Programming, Budgeting, Execution (PPBE). Process used to allocate resources within the Department of Defense. The PPBE is a cyclic process that provides the mechanisms for decision making and provides the opportunity to reexamine prior decisions in light of changes in the environment.

Program Evaluation Board (PEB). Establishes the funding priorities for the next POM submission. The Seven PEBs consist of: Warfighting, Training, Manning, Operating Forces, Installations, Sustainment, and Headquarters & Support.

Program Objective Memorandum (POM). An annual memorandum in prescribed format submitted to the Secretary of Defense (SECDEF) by the DoD Component heads, which recommends the total resource requirements and programs within the parameters of SECDEF’s fiscal guidance. The POM is a major document in the PPBE process, and the basis for the component budget estimates.

Protection. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 1-02).

Protection Executive Steering Group (P-ESG). Provides senior-level strategic guidance and oversight for the MA OAG, and serves as the Protection Advocate's senior forum for strategic interaction with various POM/MCFDS enterprise bodies and processes. The P-ESG also reviews/approves MA OAG recommendations; provides guidance on issues forwarded by the MA OAG; and, in turn, endorses, settles, or provides recommendations for issue resolution to the Protection Advocate. The P-ESG also ensures that protection-related issues and requirements are fully coordinated with other advocates and POM/EFDS enterprise bodies, as appropriate.

Risk. Probability and severity of loss linked to threats or hazards. (JP 3-07.2)

Risk Management (RM). A continual process or cycle where risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to measure performance, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and risk avoidance. (DoDI 6055.17)

Task Critical Asset (TCA). An asset of such extraordinary importance that its incapacitation or destruction would have a serious and debilitating effect on the ability to execute the MET, Mission Essential Function, or capability it supports. A TCA is an asset that is utilized to directly execute an essential business function or operational task/mission (e.g., a satellite used for a surveillance task).

Stand Alone Facility (SAF). A facility that resides off a DoD installation. SAFs are embedded in communities. While some have barriers that define an operational area, most are an integral part of the environment where they reside and have no organic security or emergency response capabilities. Most SAFs are dependent upon external community or military agencies for security and intelligence analysis. Each requires careful consideration of protective measures and application of resources specifically tailored to the existing threat.

Supporting Establishment (SE). Includes Headquarters Marine Corps, MCRC, and other non-MAGTF organizational elements that primarily

serve in the capacity as advocate or proponent for training, manpower, headquarters, acquisition, logistics, and installations. (MARADMIN 422-07, MARADMIN 597-12)

Supporting Infrastructure Critical Asset (SICA). An asset that supports the functioning or operation of a TCA such that the asset's loss, degradation, or denial will result in the inability of the TCA to function or operate as intended in the execution of its associated task/MET or function. In other words, a TCA cannot operate or function without an SICA being available and functioning properly.