



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

MCO 3501.36B
PP&O (PS)
12 Feb 2021

MARINE CORPS ORDER 3501.36B

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS CRITICAL INFRASTRUCTURE PROGRAM

Ref: See Enclosure (1)

Encl: (1) References
(2) Baseline Elements of Information (BEI)
(3) Critical Asset Identification Process (CAIP)
(4) Restricted Area Definitions for Critical Assets
(5) Guidance for Resourcing Critical Asset Risk Reduction Plans

1. Situation. The ability to ensure execution of Department of Defense (DoD), Department of Navy (DON), and Marine Corps missions is highly dependent upon the employment of critical assets and infrastructures. This Order updates service-specific Critical Infrastructure Protection (CIP) policy and provides Marine Corps CIP program requirements for commands and staffs. Significant updates to this Order include provisions ensuring compliance with and integration of CIP-related activities detailed in reference (a) and the identification of Marine Corps Installations Command (MCICOM) roles and responsibilities for CIP program implementation. This Order is in accordance with references (a) through (s).

2. Cancellation. MCO 3501.36A

3. Mission. The Marine Corps shall identify, assess, manage, and monitor risk to infrastructure critical to the execution of Mission Essential Functions and assigned missions. This mission will be accomplished at all levels of command in accordance with reference (b).

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Nothing in this Order shall detract from or be construed to conflict with the inherent responsibility of military commanders to protect personnel and equipment under their commands.

(b) Marine Corps leaders must understand and execute integrated protection functions continuously regardless of location. Globalization and the evolution of information and technology have created critical mission-related dependencies for the Marine Corps including single points of failure that are vulnerable in an all-hazards, all-threats operating environment.

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

While the Marine Corps has a vast array of internal capabilities, systems, and processes, its missions depend heavily on other government and private-sector critical assets and infrastructure systems and networks outside of its ownership and control. Critical infrastructure protection is a key pillar of the protection framework which supports and ensures successful execution of Marine Corps missions.

(2) Concept of Operations. The Commander's intent shall be executed through a continuous risk management process, which, at a minimum, shall include the following annual requirements:

(a) Critical Asset Identification Process (CAIP). In the first quarter of each fiscal year and any time new missions are added, commands, activities, sector leads, and staff will use enclosure (3) to identify and validate assets and infrastructures critical to the execution of DON and Marine Corps missions, tasks, core functions, and capabilities. Missions and associated critical assets identified in the CAIP analysis shall be documented in the Marine Corps Critical Asset Management System (MC-CAMS), including all Baseline Elements of Information (BEI) defined in enclosure (2) that can be received by the system. MC-CAMS is the authoritative database for Marine Corps critical asset and infrastructure data, including CIP data and dependency mapping of Mission Relevant Terrain in Cyberspace (MRT-C), and will support sharing Marine Corps data with other DoD Components as required by references (b) and (c).

(b) Risk Management. Battalion-level and above commands shall conduct risk management activities assigned in this Order and manage CIP requirements for their subordinate commands. During the second and third quarters of the fiscal year, commands, activities, sector leads, and staff will use the Risk Management (RM) methodology in reference (a) to assess and identify risk to critical assets and infrastructure. Key risk management activities in support of CIP include:

1. Conducting a command risk assessment that includes criticality, threat/hazard, and vulnerability assessments as defined in reference (a) in order to identify, validate, assess, and prioritize risk to missions and supporting critical assets, infrastructures, and capabilities per references (a) through (e).

2. Utilizing the results of the risk assessment to identify and prioritize risk to missions and supporting critical assets and infrastructures.

3. Developing appropriate plans to reduce risk to identified critical assets and infrastructures. 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 of executing a risk reduction plan.

4. Identifying and prioritizing resources to reduce risk and associated protection gaps in critical assets and infrastructures.

5. Documenting and tracking critical asset risk reduction plans in MC-CAMS.

6. Comply with national and DoD CIP requirements, including coordination to identify and facilitate protection of non-DoD-owned assets

and infrastructures critical to DoD, DON, and Marine Corps missions, core functions, and capabilities.

(c) Resourcing and Executing Risk Reduction Plans. Commands execute resourcing and implementing approved critical asset risk reduction plans prior to the end of the fiscal year. The limited availability of resources requires proper planning, justification of requirements, and coordination with mission and asset stakeholders. For risk reduction plans to compete against other funding requirements, requirements must be well-defined by documenting the level of risk to mission execution as well as mission impact if not funded. Enclosure (5) outlines resourcing guidelines to consider when addressing risk reduction resource planning.

(d) Monitoring and Reporting/Indications and Warnings (I&W). The receipt of timely, accurate, and relevant intelligence by the commands in the field is vital to the protection of Task Critical Assets (TCAs) and Supporting Infrastructure Critical Assets (SICAs). The monitoring and reporting of TCA and SICA operational status is imperative to risk management. Critical infrastructure protection activities that will enhance our ability to receive timely I&W include the following tasks:

1. Share authoritative critical asset/infrastructure information with DoD, DON, and Marine Corps intelligence organizations to support a defined focus area for I&W support.
2. Support the development of Command Priority Intelligence Requirements (PIRs) and Critical Information Requirements (CIRs) specific to critical assets and infrastructures.
3. Report Tier 1 and 2 mission critical asset non-availability, destruction, or degradation to Higher Headquarters (HHQ) via Operational Report-3 (OPREP-3) Serious Incident Report procedures when a change in status occurs. Change of operational status of Tier 1 and 2 critical assets must be entered in MC-CAMS within 24 hours.

(e) Share Marine Corps authoritative CIP information with other DoD Components, including information on decisions made to acknowledge or manage risk to critical assets and infrastructures. Support the DoD and DON DCIP efforts to implement CIP information sharing through the Navy Critical Asset Management System and MC-CAMS. This is a net-centric environment to support DoD, DON, and Marine Corps operational and programmatic requirements and facilitate coordination with the U.S. Department of Homeland Security to address private sector infrastructure supporting Marine Corps missions.

(f) CIP Program Reviews. Program reviews regarding the implementation and execution of CIP requirements prescribed in this Order shall be conducted by all major subordinate commands and staff with responsibilities under this Order annually unless the command is undergoing an Inspector General inspection that assessed CIP during the same FY.

b. Tasks

(1) Deputy Commandant for Plans, Policies and Operations (DC PP&O). Responsible for ensuring Marine Corps compliance with DoD CIP policy. Day-to-day oversight and responsibility for the management and execution of the Marine Corps CIP program is delegated to the Assistant Deputy Commandant (ADC) (Security) for PP&O.

(a) ADC (Security) PP&O shall:

1. Provide oversight and maintain overall responsibility for the CIP program, including the establishment, implementation, and execution of a CIP policy, strategy, guidance, and supporting methodologies within the Marine Corps.

2. Provide representation to support DoD and DON CIP-related meetings and working groups, including DoD and DON CIP Councils, Executive Steering Groups, or other senior-level bodies.

3. Provide recommendations to the DON on CIP policy, strategy, and risk assessment methodology.

4. Oversee, manage, and direct the identification, validation, prioritization, and assessment of assets and infrastructures critical to the execution of Marine Corps missions, capabilities, core functions, and tasks annually, at a minimum.

5. Serve as the Office of Primary Responsibility (OPR) for resources to execute the Marine Corps CIP program and risk reduction plans. Support the identification and submission of Marine Corps CIP requirements through the annual Planning, Programming, Budgeting, and Execution (PPBE) process; military construction, sustainment, and modernization projects; and the Marine Corps Enterprise Integration Plan (MCEIP).

6. Develop and maintain Marine Corps CIP program review standards and benchmarks to identify, monitor, and track execution of DoD, DON, and Marine Corps CIP requirements, goals, and objectives.

7. Ensure Marine Corps CIP program activities are synchronized with and align to MA risk management requirements in accordance with reference (a).

8. In coordination with the DON, develop and implement CIP awareness, education, and training programs and curricula. Issue CIP training requirements annually.

9. Develop requirements for and oversee the implementation and management of MC-CAMS as the authoritative database for Marine Corps critical asset and infrastructure data in support of risk management.

10. Provide service-level integration, coordination, and sharing of CIP information and methodologies to include TCA reporting in accordance with reference (c).

11. Chair the Headquarters Marine Corps (HQMC) Critical Infrastructure Protection Working Group (CIPWG). The ADC may assign or delegate this responsibility as appropriate. The HQMC CIPWG shall be conducted annually, or more frequently as required.

12. In coordination with the Deputy Commandant for Installations and Logistics (DC I&L), support the conduct of protection-related reviews of plans and designs for the refurbishment, re-use, renovation, design, and/or construction of facilities that have a direct

mission linkage to TCAs via the appropriate service-level venues to document gaps in resiliency, capability, and security impacting mission execution.

13. Annually coordinate with the DON CIP Office of Primary Responsibility (OPR); Director, Naval Criminal Investigative Service; and the Marine Corps Intelligence Activity (MCIA) to request intelligence and counter-intelligence products to meet CIP threat monitoring and I&W responsibilities for Marine Corps-owned and supported critical assets per reference (g).

14. Develop processes to define, identify, document, and address risk to critical assets, infrastructures, Critical Program Information (CPI), and Defense Critical Assets owned or supported by the Marine Corps.

15. Annually, review the quality and completeness of MC-CAMS BEI data, and identify gaps and trends that need to be addressed service-wide.

16. Oversee the identification and development of policies and processes for the automated sharing of critical infrastructure program data in MC-CAMS with other DoD Component information systems.

17. Coordinate with the Defense Readiness Reporting System (DRRS) program office to share MC-CAMS critical asset operational status based on potential impacts to command-reportable mission essential tasks.

18. Coordinate with Deputy Commandant for Information (DC I) to establish data-sharing capabilities for information technology (IT) and operational technology (OT) risk from MC-CAMS for critical assets that are applications or systems that reside on the Marine Corps Enterprise Network (MCEN) with accreditation requirements in the Marine Corps Compliance and Authorization Support Tool (MCCAST).

19. Coordinate with DC I on requirements that pertain to information, communication, command and control, computers, intelligence, space, cyberspace, electronic warfare, and the electromagnetic spectrum.

20. In coordination with the Office of the Inspector General of the Marine Corps (IGMC), develop Marine Corps CIP program functional area checklists and benchmarks supporting the conduct of the IGMC.

21. Integrate the scheduling of Program Reviews with scheduled Commanding General's Inspections.

(b) Plans, Policies and Operations Director of Strategy and Plans, shall:

1. Designate, in writing, an OPR to manage execution of Space Sector CIP requirements in this Order.

2. Coordinate with U.S. Space Command, DC I, and the appropriate service component to ensure Marine Corps and DoD Space Sector CIP requirements are identified and addressed.

3. Utilize the CAIP to identify and validate critical Marine Corps Space Sector systems, assets, and infrastructures, and enter that information in MC-CAMS in accordance with reference (a).

4. Serve as a member of the HQMC CIPWG.

(2) Deputy Commandant for Manpower & Reserve Affairs (DC M&RA) shall:

(a) Designate, in writing, an OPR to serve as the sector lead to manage execution of M&RA CIP requirements in this Order.

(b) Utilizing the CAIP in enclosure (3), identify and prioritize critical Marine Corps-owned and managed M&RA systems, assets, and infrastructures, and enter that information into MC-CAMS in accordance with reference (a).

(c) Coordinate with the ADC (Security) PP&O, Marine Forces (MARFORs), and Marine Corps installations to assess M&RA systems, assets, and infrastructures.

(d) Manage and oversee the documentation and execution of plans for all sectors to reduce risk to identified assets and infrastructure to maintain minimum essential level of M&RA core functions in accordance with reference (a).

(e) Coordinate with the ADC (Security) PP&O and other CIP sector leads to identify and seek the required personnel structure and staffing to fully support Marine Corps CIP requirements.

(f) Coordinate with the Defense Human Resources Agency to ensure Marine Corps and DoD Personnel Sector CIP requirements are identified and coordinated.

(g) Serve as a member of the HQMC CIPWG.

(3) Deputy Commandant for Programs and Resources (DC P&R) Fiscal Director shall:

(a) Designate, in writing, an OPR to serve as the sector lead to manage execution of P&R CIP requirements in this Order.

(b) Coordinate with the DoD Finance sector lead agency, Defense Finance and Accounting Service, to ensure Marine Corps and DoD finance sector CIP requirements are identified, coordinated, and executed.

(c) Utilize the CAIP to identify and validate critical Marine Corps-owned and -managed financial management systems, assets, and infrastructures, and enter that information in MC-CAMS in accordance with reference (a).

(d) Ensure P&R CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(e) In accordance with the integrated framework identified in reference (a), oversee the development and execution of plans and projects for the reduction of risk to P&R critical systems and assets to ensure

minimum essential levels of financial core functions can be maintained and sustained. Enter risk reduction plans and projects in MC-CAMS.

(f) Serve as a member of the HQMC CIPWG.

(4) Deputy Commandant for Information (DC I) shall:

(a) Through the Director, Command, Control, Communications and Computers (DIR C4):

1. Designate, in writing, an OPR to serve as the sector lead to manage execution of DoD Information Network (DoDIN) CIP requirements in this Order and in reference (h).

2. Identify, approve, and maintain a repository of Impact Values (LOW, MODERATE, HIGH) and Security Objectives (Confidentiality, Integrity, and Availability (C, I, and A)) for all Marine Corps CIP-related systems.

3. Coordinate with ADC (Security) PP&O in the technical evaluation of MCEN compatibility with command and control (C2) systems and tools designed to provide near real-time CIP situational awareness, threat monitoring, and reporting.

4. In coordination with ADC (Security) PP&O, assist with the evaluation, accreditation, and implementation of the MC-CAMS and its associated support tools on the MCEN.

5. Support the DoD DoDIN sector lead agency, Joint Force Headquarters, to ensure Marine Corps and DoD DoDIN Sector CIP requirements are identified, coordinated, and executed.

6. Utilizing the CAIP in enclosure (3), identify and validate critical Marine Corps-owned and supported C4 systems, assets, and infrastructures, and enter that information in MC-CAMS in accordance with reference (a). Identify and document MRT-C that may impact Marine Corps missions in MC-CAMS.

7. Ensure C4 CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

8. Serve as a member of the HQMC CIPWG.

(b) Through the Director, Intelligence:

1. Designate, in writing, an OPR to serve as the sector lead to manage execution of Intelligence, Surveillance, and Reconnaissance (ISR) CIP requirements in this Order.

2. Support the DoD ISR lead agency, Defense Intelligence Agency, to ensure Marine Corps and DoD ISR Sector CIP requirements are identified, coordinated, and executed.

3. Utilizing the CAIP in enclosure (3), identify and validate critical Marine Corps ISR systems, assets, and infrastructures, and enter that information in MC-CAMS in accordance with reference (a).

4. In coordination with ADC (Security) PP&O and the DON CIP OPR, provide support to the development of the capability to identify, monitor, and report threats, including timely dissemination of I&W to Marine Corps installations and facilities where DoD or Marine Corps critical assets and infrastructures are located.

5. In coordination with ADC (Security) PP&O and MCIA, develop processes to define, identify, and document threats to critical assets and infrastructures.

6. Serve as a member of the HQMC CIPWG.

(c) Through the Director, Information Maneuver Division:

1. Coordinate space, cyberspace, electronic warfare, and associated spectrum requirements with the sector leads, and ensure CIP requirements are identified, validated, prioritized, and addressed.

2. Serve as a member of the HQMC CIPWG.

(d) In coordination with ADC (Security) PP&O, develop metrics to support MCCASt and MC-CAMS system-to-system data-sharing capabilities for IT and OT risk for critical assets that are applications or systems that reside on the MCEN with accreditation requirements.

(5) Deputy Commandant for Installations and Logistics (DC I&L) shall:

(a) Designate, in writing, Marine Corps sector leads for the Logistics, Public Works, and Transportation Sectors to manage execution of each Sector's respective CIP requirements.

(b) Support the DoD Logistics Sector (Defense Logistics Agency), Public Works Sector (Naval Facilities Engineering Command and U.S. Army Corps of Engineers), and Transportation Sector lead agencies to ensure Marine Corps and DoD Logistics, Public Works, and Transportation Sector CIP requirements are identified, coordinated, and executed.

(c) Utilizing the CAIP in enclosure (3), identify and validate critical Marine Corps logistics, public works, and transportation systems, assets and infrastructures and enter that information in MC-CAMS in accordance with reference (a). Oversee the execution of CAIP requirements for subordinate commands.

(d) In conjunction with Marine Corps Forces Cyber Command (MARFORCYBER) and DIR C4, develop and implement cybersecurity policies and guidance for the use, security, and protection of critical utility and facility-related control systems and Supervisory Control and Data Acquisition (SCADA) systems.

(e) In coordination with ADC (Security) PP&O, assess risk to critical logistics, public works, and transportation systems and assets, specifically including critical utility and facility related control systems and SCADA systems and assets, utilizing the risk assessment methodology identified in reference (a).

(f) Ensure the review of all new construction plans and Facilities Sustainment, Restoration, and Modernization projects for compliance with DoD and Marine Corps CIP requirements in order to appropriately incorporate the analysis of threats/hazards to facilities housing TCAs into the facility planning, design, construction, and renovation.

(g) Provide guidance and recommendations for the relocation of Marine Corps-owned TCAs from non-DoD, civilian-shared tenant spaces to Marine Corps installations or government facilities with appropriate physical and logical security measures required for protection of the TCAs.

(h) In coordination with ADC (Security) PP&O, synchronize GEOFidelis and CIP data to support unified visibility of critical infrastructure.

(i) Logistics, Public Works, and Transportation OPRs will identify representatives to serve as members of the HQMC CIPWG.

(6) Deputy Commandant for Aviation (DC AVN) shall:

(a) In coordination with DC I&L and the Logistics sector lead, designate a POC in writing to manage execution of aviation logistics CIP requirements in this Order.

(b) In coordination with Naval Aviation Systems Command OPR, utilize the CAIP to identify and validate critical aviation assets and supporting infrastructures per enclosure (3), to include sole source aviation supply chains, management systems, and infrastructures provided by commercial suppliers from the Defense Industrial Base (DIB) and document those critical assets in MC-CAMS in accordance with reference (a).

(c) Ensure AVN CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(d) Provide a representative to serve as a member of the HQMC CIPWG.

(7) Director, Health Services (HS) shall:

(a) Designate, in writing, an OPR to serve as the Marine Corps sector lead for Health Services.

(b) Coordinate with the DoD Health Affairs sector lead agency, Office of Assistant Secretary of Defense, Health Affairs and Department of Navy Bureau of Medicine and Surgery (BUMED) to ensure Marine Corps, Navy, and DoD Health Affairs Sector CIP requirements are coordinated, identified, and executed.

(c) Coordinate with BUMED to obtain and share information on the identification, validation, and prioritization of BUMED assets and systems critical to supporting Marine Corps health care services, systems, and assets.

(d) Utilize the CAIP in enclosure (3) to identify and validate critical health/medical assets and supporting infrastructures. Coordinate

with ADC (Security) PP&O to enter critical health/medical assets, systems, and infrastructures impacting the Marine Corps into MC-CAMS in accordance with reference (a).

(e) Ensure HS CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(f) Serve as a member of the HQMC CIPWG.

(8) Inspector General of the Marine Corps (IGMC) shall coordinate with the ADC (Security) PP&O regarding IGMC functional area checklist Marine Corps CIP requirements.

(9) Staff Judge Advocate (SJA) to the Commandant of the Marine Corps shall:

(a) Conduct legal reviews of CIP plans, operations, exercises for compliance with domestic and international law, and provide legal advice on the establishment of joint military-civilian efforts to protect both critical military and commercial assets upon which military operations are dependent, and on the development of joint mutual aid and assistance agreements for joint military-civilian emergency response activities.

(b) Support ADC (Security) PP&O in the review of policy provisions or other guidelines pertaining to the release of CIP-related information.

(c) Provide legal advice on the control of critical infrastructure-related information, to include security information focusing on open source handling of installation/facility critical facility and asset diagrams, over-flight permissions, and critical asset Geographic Information Systems data, pictures, and maps.

(d) Upon request, make legal counsel available to support the HQMC CIPWG.

(10) Commander, Marine Corps Systems Command (COMMMARCORSYSCOM) shall:

(a) Designate, in writing, an OPR to serve as the Marine Corps sector lead for the DIB.

(b) Support the DoD DIB sector lead agency, Defense Contract Management Agency, to ensure Marine Corps and DoD DIB Sector CIP requirements are identified, coordinated, and executed.

(c) Identify, validate, and prioritize mission-critical Marine Corps DIB assets per enclosure (3) based on the following minimum criteria:

1. Manufacturers or suppliers that are prime or subcontractor single or sole source suppliers with unique technology or industrial capability that could significantly impact warfighter capabilities due to non-availability of material or product for the Marine Corps.

2. Manufacturers or suppliers that are single source subcontractors with long re-qualification times that support numerous programs and products across the Marine Corps.

(d) Document identified Marine Corps critical DIB assets, systems, and/or manufacturers in MC-CAMS.

(e) Identify DIB related MRT-C that may impact Marine Corps missions and record this data in MC-CAMS.

(f) Ensure DIB-related CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(g) Support and coordinate with ADC (Security) PP&O to identify and protect CPI by:

1. Identifying an OPR for the identification, management, and protection of CPI.

2. Annually documenting assets and infrastructure that support and secure CPI.

3. Sharing the CPI list of programs and systems with the ADC (Security) PP&O protection programs.

(h) Upon request, serve as a member of the HQMC CIPWG.

(11) Deputy Commandant, Combat Development and Integration (DC CD&I) shall:

(a) Utilize the CAIP per enclosure (3) to identify and validate assets and supporting infrastructures critical to MCCDC missions and essential functions, and document those critical assets in MC-CAMS in accordance with reference (a).

(b) In coordination with ADC (Security) PP&O, develop and validate CIP doctrinal and training requirements, procedures, and/or guidance for the identification, prioritization, assessment, and management of risk to critical assets and infrastructures.

(c) In coordination with the ADC (Security) PP&O, support the development and integration of CIP tasks into the Marine Corps Task List.

(d) In coordination with ADC (Security) PP&O, develop and validate CIP doctrine and training requirements, procedures, and/or guidance for the identification, prioritization, assessment, and management of risk to critical assets and infrastructures.

(e) In coordination with appropriate DCs and ADC (Security) PP&O, assist in the identification and prioritization of Marine Corps CIP capabilities, and gaps, and coordinate with appropriate stakeholders to address those gaps in annual MCEIP processes.

(f) Serve as a member of the HQMC CIPWG.

(12) Commanding General, Training and Education Command (CG, TECOM)
shall:

(a) Designate, in writing, an OPR to serve as the TECOM sector lead for executing Marine Corps CIP program requirements identified in this Order.

(b) In coordination with MCICOM, provide oversight and recommendations for CIP requirements to be executed at Service Level Training Installations. Coordinate with MCICOM to identify and prioritize CIP-related resource requirements for program execution and resources for risk reduction plans for critical assets and infrastructures.

(c) Implement CIP education for Marine Corps formal schools and other professional military education venues. Support the implementation of CIP training and readiness requirements across the Marine Corps.

(d) Utilize the CAIP in enclosure (3) to identify and validate critical Marine Corps training and education systems, assets, and infrastructures and document the information in MC-CAMS in accordance with reference (a).

(e) Ensure TECOM CIP activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(f) Serve as a member of the HQMC CIPWG.

(13) Commanding General, Marine Corps Recruiting Command (CG, MCRC)
shall:

(a) Designate, in writing, an OPR to serve as the sector lead to manage execution of MCRC CIP requirements in this Order.

(b) Utilizing the CAIP in enclosure (3), identify and validate critical Marine Corps Recruiting Command critical assets and infrastructures and document the information in MC-CAMS in accordance with reference (a).

(c) Ensure MCRC CIP program activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(d) Upon request, serve as a member of the HQMC CIPWG.

(14) Commander, Marine Forces Cyber (COMMARFORCYBER), subject to the direction of Commander U.S. Cyber Command, shall:

(a) Designate, in writing, an OPR to serve as the sector lead to manage execution of CIP requirements in this Order pertaining to MARFORCYBER missions and operations.

(b) Utilizing the CAIP per enclosure (3), identify and validate critical MCEN systems, assets, and infrastructures in accordance with reference (a), to include critical cyber terrain and MRT-C per the requirements in reference (h), and enter that information in MC-CAMS. Share the authoritative MRT-C data with the Mission Assurance Decision Support System 2.0 or higher version to ensure data integrity.

(c) Coordinate with DC PP&O and DC I to meet requirements that pertain to the DoDIN and/or MCEN systems, assets, infrastructures, and critical cyber terrain.

(d) Serve as a member of the HQMC CIPWG as required.

(15) Commanding General, Marine Corps Installations Command (CG, MCICOM) shall:

(a) Oversee, manage, and direct implementation of all CIP requirements for subordinate commands and installations.

(b) Direct and oversee the annual execution of the CAIP process per enclosure (3) during the first quarter of the FY at all installations to identify assets and supporting infrastructures critical to installation missions, functions, and tasks in accordance with reference (a).

(c) Oversee the execution of the installation critical asset validation process and serve as the final validation authority for critical assets and infrastructures identified by the installations that support their essential tasks, functions, and capabilities. Direct all installations to document Command approval and validation of critical assets in MC-CAMS.

(d) Manage and oversee the documentation and execution of plans to reduce risk for installation critical assets and infrastructures in accordance with reference (a).

(e) Oversee and direct that installation annual protection-related exercises shall include at least one CIP-related inject to test critical infrastructure mission support, critical asset availability, response, and/or recovery. At the commander's discretion, CIP-related exercise injects may be conducted in tabletop or seminar format to prevent disruption to exercise timelines and objectives.

(f) Annually, review the quality and completeness of MC-CAMS BEI data, and identify gaps and trends across supporting establishment commands.

(g) Advocate for funding in appropriate PPBE forums in order to address CIP shortfalls requiring funding for mitigation.

(h) Designate an OPR to plan, manage, and execute the Marine Corps CIP program for Marine Corps Installations Command.

(i) Ensure TCA status and availability is included in Commanders' CIRs and PIRs.

(j) Ensure that Force Protection Condition action sets are developed for implementation when required for the protection of TCAs when the probability of threats increases.

(k) Address critical assets in:

1. Operational Planning Teams and Integrated Planning Teams as appropriate.

2. Operational Plans, Concept Plans, Installation Protection Plans, Base Defense Plans, and Emergency Action/Response plans as appropriate.

3. Installation Emergency Management planning, to include developing an integrated emergency/first responder set of response priorities incorporating the priority of missions associated with installation facilities and critical assets and infrastructures per reference (i).

4. Capability assessments and planning, specifically including the identification of assets critical to providing installation capabilities responding to emergency events.

5. Continuity of Operations (COOP) Plans per reference (j), specifically identifying critical assets and infrastructures that support installation essential functions and developing plans to restore essential functions of or supported by critical assets within 12 hours.

6. Mutual aid, assistance, and support agreements for joint military-civilian emergency response activities at bases, stations, and facilities within their areas of responsibility, including utility restoration priority plans.

(l) Serve as a member of the annual HQMC CIPWG.

(m) Implement CIP awareness, education, and training.

(16) Installation Commanders shall:

(a) Appoint a CIP officer, in writing, at every installation and regional command, to facilitate CIP coordination and execution of the requirements of this Order throughout the chain of command. The CIP officer shall execute the following CIP management requirements:

1. Annually, or as new mission and risk data are identified, enter and update MC-CAMS data pertaining to the identification, validation, prioritization, assessment, and management of risk to critical assets and supporting infrastructures per reference (a) and enclosure (3).

2. Use MC-CAMS to monitor, update, and inform HHQ of any changes in Tier 1 and 2 asset operational readiness or status within 24 hours as well as OPREP-3 reporting procedures.

3. Coordinate the integration of and access to CIP data in command Emergency Operations Centers and crisis action centers to support response to real-world events and operations.

4. Annually, support the identification, prioritization and submission of resource requirements for the development and execution of plans to reduce identified risk to Tier 1 and 2 critical assets as soon as those risks are identified.

5. Collaborate with appropriate Operations Security Officers to ensure critical asset information is included in the commander's Critical Information List.

(b) Ensure command personnel responsible for executing CIP requirements and activities complete annual training to remain current on program requirements and Marine Corps risk management processes in accordance with annual requirements distributed by ADC (Security) PP&O.

(c) Establish and periodically convene a Command CIPWG to facilitate coordination with Marine Corps Commands that are tenants on Marine Corps installations and ensure alignment with Marine Corps risk management processes in accordance with reference (a).

(d) Coordinate with operational units and all tenant activities stationed on installations to support the development and execution of joint CIP exercise injects.

(e) Conduct physical security surveys in accordance with enclosure (4) of this Order and reference (m) to assign an appropriate level of restricted area protection to critical assets. Designate critical assets as restricted areas as appropriate.

(17) MARFOR Commanders shall:

(a) Designate, in writing, an OPR to serve as the sector lead to manage execution of MARFOR CIP requirements in this Order.

(b) Execute the CAIP in accordance with reference (a) and enclosure (3) of this Order to perform and/or update mission decomposition and identify critical assets and infrastructures associated with those mission areas, including applicable MRT-C, operational plans, and concept plans.

(c) Ensure MARFOR CIP activities are synchronized with and align to Mission Assurance risk management requirements in accordance with reference (a).

(d) Develop Command CIRs and PIRs for information pertaining to threats/hazards to Command critical assets and infrastructures.

(e) Annually, review the quality and completeness of MC-CAMS BEI data, and identify gaps and trends across the commands.

(f) Develop and implement plans and projects to reduce and manage identified risk to assets and infrastructures critical to the execution of the command's missions, essential functions, and capabilities. Document plans and projects to reduce risk or decisions to acknowledge risk in MC-CAMS per enclosure (5).

(g) Advocate for funding and resources in appropriate PPBE forums to reduce unacceptable risk to command critical assets and associated missions.

(h) Use MC-CAMS to monitor, update, and inform HHQ of any changes in Tier 1 and 2 asset operational readiness or status within 24 hours as well as OPREP-3 reporting procedures.

(i) Direct and oversee execution of CIP requirements of all major subordinate commands.

(j) Coordinate the transfer of deploying MARFOR TCAs to gaining MARFOR in the execution of all CIP requirements. Ensure TCA management is addressed in all deployment plans.

(k) Serve as a member of the annual HQMC CIPWG.

c. Coordinating Instructions

(1) Marine Corps commands shall utilize MC-CAMS to identify, validate, document, and manage mission critical asset data including Mission Relevant Terrain of all types and other risk management information; support security, protection, and response activities; synchronize data across protection-related programs and activities; and support command prioritization of critical infrastructure protection gaps.

(2) BEI are attached and incorporated into this Order as enclosure (2).

(3) The CAIP is the Marine Corps methodology to: conduct a mission decomposition and analysis of commands' and activities' missions, tasks, functions, and/or capabilities; identify critical assets and infrastructure dependencies, and; identify impacts to mission execution. The CAIP methodology is attached and incorporated into this Order as enclosure (3).

(4) To support uniform application of security measures for Marine Corps critical assets and infrastructures, critical assets shall be assigned minimum levels of protection per references (l) and (m). Specific guidance is attached and incorporated into this Order as enclosure (4).

(5) Guidance to support resourcing critical asset and infrastructure risk reduction plans is attached and incorporated into this Order as enclosure (5). This guidance is intended to assist commands and activities who own, manage, and/or are responsible for the protection and security of critical assets and infrastructures to identify, prioritize, and procure resources to implement risk reduction plans for those critical assets and infrastructures.

(6) The unit/command Mission Essential Task List (METL) contained in DRRS should be used to guide the mission decomposition process. Command METLs should be obtained from the Marine Corps Training Information Management System (MCTIMS) by entering the Training and Readiness Module - Taskmaster. The MCTIMS website is <https://mctims.usmc.mil>, and personnel registration is required.

(7) Reference (n) provides guidance for the classification of critical asset and infrastructure information in general, and for the handling of critical asset information specifically, and shall be used by all commands and activities in executing the requirements of this Order.

5. Administration and Logistics

a. Recommendations. Recommendations for changes to this Order should be submitted to ADC (Security) PP&O via the appropriate chain of command.

b. Records Management. Records created as a result of this directive shall be managed according to National Archives and Records Administration (NARA)-approved dispositions per SECNAV M-5210.1 CH-1 to ensure proper

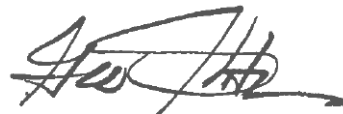
maintenance, use, accessibility and preservation, regardless of format or medium. Records disposition schedules are located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at:

<https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx>. Refer to MCO 5210.11F for Marine Corps records management policy and procedures.

c. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a) and implemented per SECNAVINST 5211.5F.

6. Command and Signal

- a. Command. This Order is applicable to the Marine Corps Total Force.
- b. Signal. This Order is effective the date signed.



G. W. SMITH, Jr.
Deputy Commandant for
Plans, Policies, and Operations

DISTRIBUTION: PCN 10203363200

References

- (a) MCO 3058.1
- (b) DoDD 3020.40 CH 1, "Mission Assurance (MA)," September 11, 2018
- (c) DoDI 3020.45, "Mission Assurance Construct," August 14, 2018
- (d) SECNAVINST 3501.1D
- (e) OPNAVINST 3502.8
- (f) MCO 5040.6J
- (g) SECNAVINST 5430.107A
- (h) Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", February 12, 2013
- (i) DoDI 6055.17 CH-3, Department of Defense Emergency Management (EM) Program, June 12, 2019
- (j) MCO 3030.1A
- (k) DoDI 5240.19 CH-2, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP), November 6, 2020
- (l) MCO 3302.1F
- (m) MCO 5530.14A
- (n) Defense Critical Infrastructure (DCI) Line of Effort (LOE) Security Classification Guide, July 27, 2018
- (o) Unified Facilities Criteria 4-010-01, DoD Minimum Antiterrorism Standards for Buildings, December 12, 2018
- (p) SECNAVINST M-5210.1
- (q) MCO 5210.11F
- (r) 5 U.S.C. 552a
- (s) SECNAVINST 5211.5F

CIP Program Basic Elements of Information (BEI)

BEI Area	BEI Name	BEI Description
CIP Database Requirements	System ID	Identifier of DCIP entity originating the data record
	Asset ID	Database-unique identifier for asset
	Last Update	Date Time Group of last update to asset record (ZULU)
Asset Data	Asset Name	Name of asset (as determined by asset owner records)
	Asset Description	Description of the asset, which typically includes the function and capability that the asset can perform
	Asset Owner - Organization	Name of the Organization that owns the asset. Ownership is usually denoted by the organization responsible for the procurement and maintenance of the asset
	Asset Owner - POC	Name of the person that is responsible for the day-to-day management and/or operation of the asset. POC Data will also include POC Non-classified Internet Protocol Router (NIPR)/ Secret Internet Protocol Router (SIPR) email and work phone number.
	Asset Location: Street Address (1)	Street address of physical location of asset
	Asset Location: Street Address (2)	Further physical address information for asset (e.g., Bldg. or Facility #, Room or Suite #, Pier #)
	Asset Location: City	City corresponding to physical address of asset
	Asset Location: Installation	DoD component installation corresponding to the physical address of the asset, if applicable
	Asset Installation Association	Supported installations
	Asset Location: State	State abbreviation corresponding to physical address of asset, if in United States
Asset Data	Asset Location: Zip Code	ZIP Code corresponding to physical address of asset, if in United States

BEI Area	BEI Name	BEI Description
	Asset Location: Country Code	International Standards Organization 3166 Country Code (3-character tri-graph) indicating country in which the asset is physically located or homebased or home-ported
	Asset Location: Latitude	Latitude coordinates of asset in decimal degrees (minimum precision of 4 decimal places, e.g., 37.4008); negative for south of equator
	Asset Location: Longitude	Longitude coordinates of asset in decimal degrees (minimum precision of 4 decimal places, e.g., -85.6302); negative for south of the equator
	Asset Location: Latitude/Longitude Source	Method used to obtain latitude-longitude coordinates (e.g., geocode/address match, global positioning system, map/imagery interpretation, feature extraction or Service Geospatial Database)
	Asset Type: (Choice of three types)	<p>Asset Type 1: Fixed (Asset is fixed, or built-in to other infrastructure. Cannot be moved)</p> <p>Asset Type 2: Moveable. An asset that can be moved, and is intended to be moved from time to time (e.g., an asset that is deployable with a unit or operational force)</p> <p>Asset Type 3: Mobile. An asset that is constantly in motion (e.g., a satellite).</p>
	Asset: Operational Status	<p>Identify current operational status of the asset based on the following picklist categories:</p> <ol style="list-style-type: none"> 1. Functioning normally 2. Degraded - down for maintenance 3. Degraded - emergency (unplanned) 4. Destroyed
	Asset: Sector Type	A picklist of the 10 DoD Sectors. Select one or more sector(s) associated with the functional capability of the asset (e.g., if the asset function support utilities, associate the asset with the Public Works Sector.

BEI Area	BEI Name	BEI Description
	Asset: Time to Restore	Time it would take to restore a destroyed critical asset or infrastructure node, or the capability it represents. (minutes, hours, days, weeks or months)
Facility/ Building Data	Facility: Real Property Index #	The real property inventory number associated with the facility (land, building, structure, linear structure, utility or relocatable) that is documented in the internet Navy Facilities Asset Data Store (iNFADS) real property inventory database. This identifier typically begins with "NFA..." under the Real Property Unique Identifier category.
	Facility/Asset Category: (Multi-Select)	A facility or asset can be categorized in one or more categories. Below is a list of categories and related BEI for each. A facility or asset may be one, two, all or none of these categories. The categories are: RA: Restricted Area / Controlled Access AT: Antiterrorism CA: Covered Asset under Section 130i WS: Weapon System, Program or Platform CS: Control Systems MRT-C: Mission Relevant Terrain - Cyberspace
	Facility Peak Load	Total daily peak energy load
	Facility/Asset: Restricted Area	Document existence and location of assets or areas that qualify as restricted areas. This includes documenting the Designation Letter, Physical Security Survey, Access Control, Security Lighting, Fencing, and Signage. Select one per asset or facility. Restricted areas (RA) will be broken down into four choices: -Controlled Access Area - Command designated controlled area usually for a special event or temporary requirement. -Level I Restricted Area -Level II Restricted Area* -Level III Restricted Area*

BEI Area	BEI Name	BEI Description
	Facility/Asset: Restricted Area	If a facility or asset is a Level II RA, then it may also have an additional identifier as Special Access Program (SAP) / Special Access Required (SAR). This will be an additional selectable field after Level II RA is chosen for the facility or asset.
	Facility/Asset: Restricted Area (RA)	If a facility or asset is a Level III RA, then it may also have one of two additional identifiers: either Sensitive Information / Sensitive Compartmented Information or SAP/SAR. This will be an additional selectable field after Level III RA is chosen for the facility or asset.
	Facility/Asset: AT	Under AT there are two selectable options for a facility or asset: High Risk Area (HRA) and High Value Target (HVT). An HRA is a facility or area with a high population or aggregation point. Document the number of occupants and the associated days and times of occupancy. An HVT is a facility that hosts a high value mission set or capability.
	Facility/Asset: CA Type	A picklist of the covered mission areas under U.S. Code Title 10 Section 130i. Select one or more associated with the functional capability of the facility/asset.
	Facility/Asset: Weapon System (WS)	Document the supported Joint Capability Area(s) (JCA) of a facility/asset at the Tier 2 JCA level. For example, a utility grid is nominally supporting JCA 4.7 Installation Support.
	Facility/Asset: WS	Document the Program Element Code, Marine Corps Program Code, Program Short Title, Resource Sponsor and Office of Primary Responsibility.

BEI Area	BEI Name	BEI Description
	Facility/Asset: Control System (CS)	Document the existence of CS nodes that operate out of a specific facility/asset. A control system will be categorized by drop-down menus starting with: BCS: Building Control System ICS: Industrial Control System UCS: Utility Control System An additional selection box will be for Facility Related Control Systems (FRCS) portfolio categorization. Not all control systems are within the FRCS portfolio. The relationship of the CS to its hosted facility will be documented as either Direct Support (required for normal operations) or General Support (not required for normal operations).
	Facility/Asset: Building Control System (BCS)	Document through drop-down table the type of BCS a CS is. BCS are defined as supporting a specific facility function such as access control, elevators, physical security, fire protection, CCTV, etc.
	Facility/Asset: Industrial Control System (ICS)	Document through drop-down table the type of ICS a CS is. ICS are defined as supporting a specific machine or industrial function such as Weapons System IT/OT, Airfield IT, Utility Generation Systems, Training Systems, Maintenance Systems, Logistics Systems, pneumatics, etc.
	Facility/Asset: Utility Control System (UCS)	Document through drop-down table the type of UCS a CS is. UCS are defined as supporting utility distribution functions such as for Power, Water, Wastewater, Natural Gas, Telecommunications and Steam. Systems such as Fuels, POL and High/Low pressure gases are utility-like and are considered ICS.
	Facility/Asset: MRT-C	Mission Relevant Terrain - Cyberspace will be categorized by the following: Select one: System, Node, or Pathway.

BEI Area	BEI Name	BEI Description
	Facility/Asset: MRT-C Systems	<p>MRT-C Systems are defined by drop-down menu as either Command and Control (C2), Non-Command and Control (Non-C2), or Defense Business System (DBS). Select one only.</p> <p>C2 is a network node defined as SIPR, NIPR, Defense Video Services, Joint Worldwide Intelligence Communications System, Defense Switched Network, or RDT&E. Some nodes may have more than one selection.</p> <p>Non-C2 is for non-service specific, non-DoD owned, common use, or commercial services that are relevant to a critical mission.</p> <p>DBS is a specific node for a given program that is typically hosted by a C2 network like Marine On-Line, MC-CAMS, MyPay, TFMSS, iNFADS, etc.</p>
	Facility/Asset: MRT-C Nodes	<p>MRT-C Nodes are defined by drop-down menu as either Hosting or Distribution Facility. Select one only. This is for a physical location of a relevant MRT-C system or the physical distribution through a campus area. Hosting nodes are typically data centers or central offices. Distribution nodes are typically cable huts, area distribution nodes, transmission facilities or antenna towers.</p>
	Facility/Asset: MRT-C Pathway	<p>MRT-C Pathway is defined by drop-down menu as either Facility (Physical path) or Circuit (Logical path). Select one only. Physical path includes defining wirelines (Fiber/Copper/Coaxial) and wireless (Radio Frequency, Wi-Fi, Satellite) means and service providers. Logical path includes bandwidth, TPS/WPS, Circuit Designation and service providers.</p>
	Facility Mission Dependency Index (MDI) Score	<p>MDI is a numerical valuation that takes into account all the missions being executed in a facility. MDI will be generated automatically by MC-CAMS when a facility - or asset in a facility is linked to one or more missions (tasks, function or capability). MDI is <u>not</u> the equivalent of the Critical Asset Priority score.</p>

BEI Area	BEI Name	BEI Description
Mission Type: Tasks	Task Name and Number	Task name and number from authorized, published tasks lists such as the Universal Joint Task List and Marine Corps Task List, etc. Pull task from various task picklists in MC-CAMS (USMC, Navy, Army, Air Force, Coast Guard)
	Task Description	The description of the scope of the task published by the authoritative task lists
	Task Standard	Task Standards derived from authoritative OSD and/or Service-level DRRS reporting
	Task Conditions	Task Conditions associated with each Standard from authoritative OSD and/or Service-level DRRS task reporting.
Mission Type: DoD/Marine Corps Functions	DoD Sector Function: Name	Picklist of the functions associated with each of the 10 DoD sectors. These functions are supported by the Marine Corps.
	DoD Sector Function: Description	Authoritative descriptions for each sector function published by DoD Sector Lead Agency.
	DoD Sector Function: Scope	Describes the scope of the sector functions supported by an associated asset. Four categories of scope of function: Strategic, Theater, Operational and Tactical.
Mission Type: DoD Mission Essential Functions (MEFs)	DoD MEF: Name	Picklist of the DoD MEFs. These functions are supported by the Marine Corps, who may have assets associated with the execution of one or more DoD MEFs.
	DoD MEF: Description	DoD mission essential function description from authoritative sources.
Mission Type: Service Mission Essential Functions	Service MEF: Name	Picklist of the Service MEFs. These functions are developed by the Marine Corps, who may have assets associated with the execution of one or more Service-level MEFs.
	Service MEF: Description	Service-level mission essential function description from authoritative sources.

BEI Area	BEI Name	BEI Description
Mission Type: Operations Plans (OPLAN) / Contingency Plans (CONPLANS)	OPLAN: Name and Number	OPLAN names and numbers (e.g., OPLAN 2020) captured and entered into MC-CAMS as a picklist. Individual component tasks and functions can be linked to support for execution of an OPLAN.
	OPLAN: Description	Authoritative, abbreviated description associated with each OPLAN name and number
	CONPLAN: Name and Number	CONPLAN names and numbers (e.g., CONPLAN 3000) captured and entered into MC-CAMS as a picklist. Individual component tasks and functions can be linked to support for execution of an OPLAN
	CONPLAN: Description	Authoritative, abbreviated description associated with each CONPLAN name and number
Mission Types: Mission Impact Data	Mission Impact	There are three types of mission impacts caused by the loss of an asset tied to the execution of a task, function, or capability. Mission impact types are in a picklist in MC-CAMS, and are: <ul style="list-style-type: none"> 1. Failure 2. Severe Degradation 3. No Significant Impact
Mission Types: Mission Impact Data	Mission Impact Description	Detailed description of how the task, function, or capability execution is impacted by the unavailability or loss of the asset supporting execution of the task function or capability.
	Time to Mission Impact	Time to mission impact describes the time from the loss of an asset that supports a task, function or capability to the time there is demonstrated impact (failure, severe degradation) on the execution of the task, function or capability. Time to impact is captured through entry of the following discrete data: months, weeks, days, hours and minutes.

BEI Area	BEI Name	BEI Description
	Critical Asset Prioritization Score	The critical Asset prioritization score is developed from the underlying methodology in MC-CAMS. The Critical Asset Priority Score provides a cumulative rating of a critical asset for all missions supported and mission impacts incurred, whether based on tasks or functions). MC-CAMS database automatically calculates the score.
Mission Owner Data	Mission Owner: Name	This field identifies the organization that has responsibility to directly execute the task, function or capability. The broad category of mission owners can include Combatant Commands, Military Departments, Services or components; and Defense agencies, but NOT sectors. MC-CAMS will have a picklist of DoD component organizations to select from when associated a task, function or capability to the organization that will directly execute that task, function or capability.
	Mission Owner: Nominating POC	The individual POC for the organization that is listed as the mission owner. POC information must include work phone, NIPR and SIPR email addresses. This is the POC responsible for nominating the asset as critical to the Mission Owners' mission, task, or function.
Risk Management Data	Assessment: Type	A picklist of the names of assessments conducted within DoD (e.g., Joint Service Integrated Vulnerability Assessment, USMC Mission Assurance Assessment (MAA), Joint Staff MAA, etc.)
OI	Assessment: Name	Name of the specific assessment report that is typically tied to an Installation (e.g., MCB Camp Lejeune MAA).
	Assessment: Date	Start date and end date of the period covered by the assessment.
	Assessment: Report Date	Date of the final, published assessment report.
	Assessment: Location	Location of the assessment (usually an installation).

BEI Area	BEI Name	BEI Description
	Assessment: Sponsoring Organization	Usually the installation command being assessed.
	Assessment: Executing Organization	Usually a HHQ assessment team (HQMC MAA, Defense Threat Reduction Agency Balanced Survivability Assessment Team, etc.).
	Threat: Name	Select from a standardized threat name picklist in MC-CAMS.
	Threat: Description	Standardized threat description picklist associated with each threat name.
	Threat: Probability Rating	Four threat probability rating categories: Critical, High, Medium and Low.
	Threat: Intent Data	Free form data field to capture data pertaining to <i>intent</i> to execute a particular threat.
	Threat: Capability Data	Free form data field to capture data pertaining to the <i>capability</i> of actors to deliver a specific threat.
	Threat: History Data	Free form data field to capture data pertaining to the <i>history</i> of actors of executing on prior similar threats.
	Hazard: Name	Select from a standardized hazard name picklist in MC-CAMS.
Risk Management Data	Hazard: Description	Standardized hazard description picklist associated with each threat name.
	Hazard: Probability Rating	Four hazard probability rating categories: Critical, High, Medium and Low.
	Vulnerability: Name	Select from a standardized vulnerability name picklist in MC-CAMS.
	Vulnerability: Description	Standardized vulnerability descriptions associated with each vulnerability name.
	Vulnerability: Degree of Vulnerability	Four vulnerability rating categories: Critical, High, Medium and Low.
	Risk Rating	MC-CAMS to produce a risk rating based on the input and integration of asset criticality data, threat/hazard rating, and vulnerability rating.

BEI Area	BEI Name	BEI Description
	Revised Risk Rating	MC-CAMS to produce a revised rating to account for reductions in asset vulnerability ratings caused by the execution of risk reduction plans and courses of action.
	Risk Response: Type	<p>Risk response types identifies three basic decision areas in addressing identified risk to assets and their associated missions. The three types of risk response are:</p> <ol style="list-style-type: none"> 1. Remediation Plans: focus on reducing vulnerabilities and risk <u>before</u> a threat or hazard occurs that could exploit identified vulnerabilities; 2. Mitigation Plans: focus on executing response plans and measures after a threat/hazard occurs that aids in securing, protecting or restoring assets and supported missions; and, 3. Risk Acknowledgement: At the commander's discretion - and where appropriate based on the documentation of level of risk and impacts to mission - a decision to acknowledge risk may be appropriate. These decisions are generally made where proposed risk reduction plans do not substantially change the risk profile of the asset of concern.
Risk Management Data	Risk Reduction: Plan Type	The field has a drop-down picklist that includes various categories for plans that are meant to reduce risk either before, or after a threat/hazard event has occurred. Includes the following specific plan types: Asset Risk Reduction Plan; AT Plan; Chemical, Biological, Radiological, Nuclear, Explosive Plan; COOP; Critical Asset Reconstitution Plan; Emergency Response Plan; and IT Disaster Recovery Plan.
	Risk Reduction Plan: Name	Capture the name of a specific risk reduction plan.
	Risk Reduction Plan: Date	Capture date of risk reduction plan.

BEI Area	BEI Name	BEI Description
	Risk Reduction Plan: Course of Action Name	Capture one or more detailed courses of action (COA) to reduce vulnerabilities to an asset.
	Risk Reduction Plan: COA Date	Capture date for when the COA was prepared.
	Risk Reduction Plan: COA Description	Free form data field that will capture a detailed description of the COA being recommended.
	Risk Reduction Plan: COA Assets	Identify the specific assets that are addressed in the COA.
	Risk Reduction Plan: COA Vulnerabilities	Identify the specific vulnerabilities for the asset to be addressed by the COA.
	Risk Reduction Plan: COA Cost	Document an estimated cost to implement the recommended COA.
	Risk Reduction Plan: COA Funding	Document whether the recommended COA is: 1. Funded 2. Not Funded 3. Pending Funding Decision
	Risk Reduction Plan: COA Decision	Capture the command's decision on risk reduction plans and COAs. MC-CAMS will support a picklist for possible decisions: 1. Command Approved 2. Not Approved 3. Decision Deferred
	Risk Reduction Plan: Project COA Start Date	A Command-approved COA is tracked to execution through the capture of a project start date.
	Risk Reduction Plan: Project COA End Date	A Command-approved COA is tracked to the end of execution through the capture of a project end date.

Marine Corps Critical Asset Identification Process

1. Critical Asset Identification Process (CAIP)

a. The CAIP provides a standardized process for Marine Corps commands and staffs to identify Task Assets (TA), Task Critical Assets (TCA), Supporting Infrastructure Assets (SIA) and Supporting Infrastructure Critical Assets (SICA) required to execute Marine Corps Mission Essential Tasks (MET), Mission Essential Functions (MEF), and capabilities. The CAIP ensures the Marine Corps is able to meet DoD requirements in references (b) and (c).

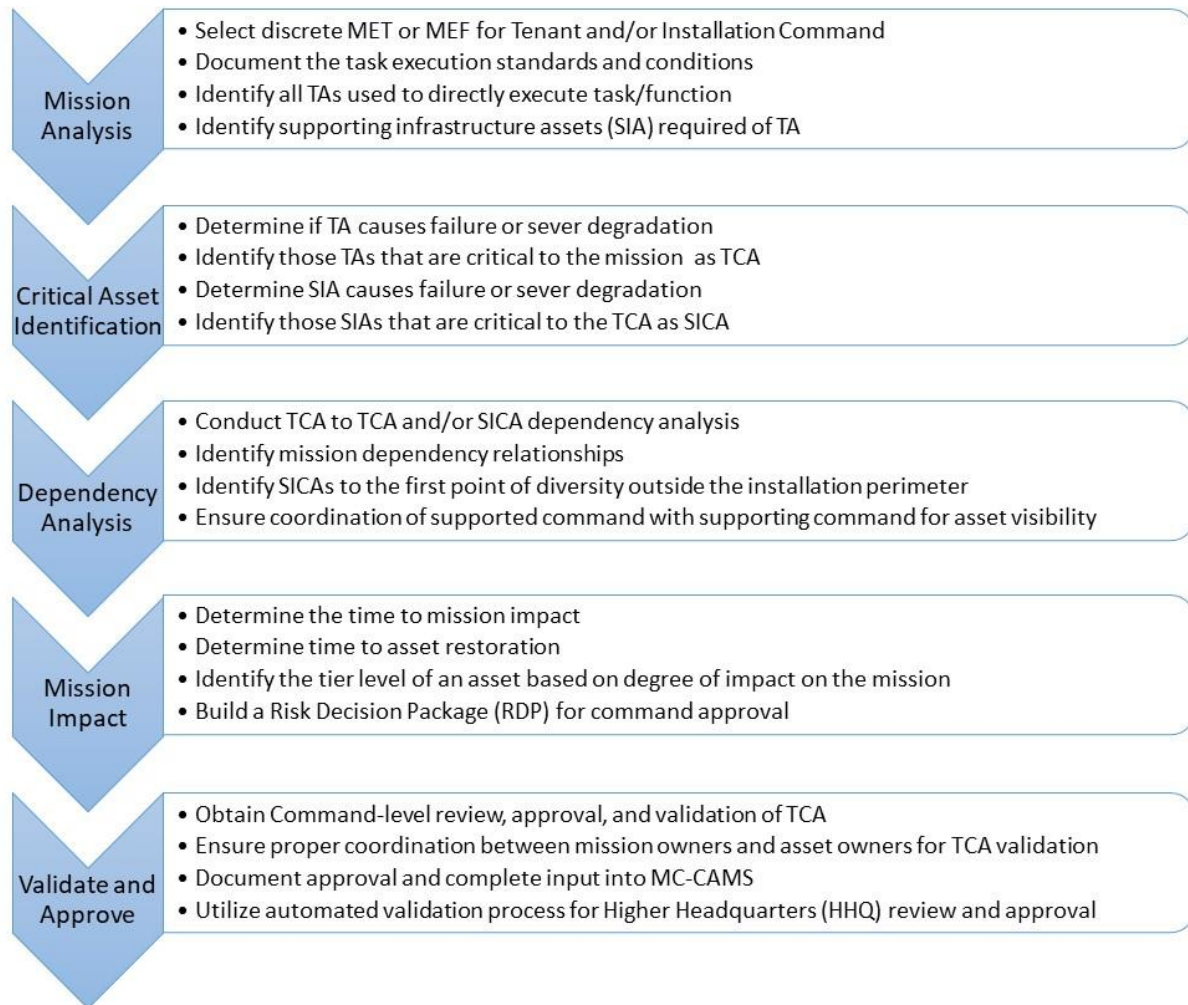


Figure 2-1. Critical Asset Identification Process

b. Commands have the responsibility and technical expertise to identify and analyze assets and infrastructure supporting their missions, tasks, functions. A TA, TCA, SIA, or SICA may be owned by another command or organization; however, it is incumbent upon the commander to identify and analyze these assets and infrastructure with the support of the owning command or organization.

c. The remainder of this enclosure outlines the steps of the CAIP, details sub-elements, and provides a list of terms and definitions. Those steps include:

- (1) Conduct mission analysis and critical asset identification.
- (2) Conduct a mission impact analysis.
- (3) Determine criticality of assets.
- (4) Validate and nominate assets.

2. Mission Analysis and Critical Asset Identification. To identify critical assets and infrastructure, commands will:

a. Conduct a mission analysis to identify assets critical to the execution of each assigned mission, task, and function. Comprehensive mission analysis includes Defense Readiness Reporting System (DRRS)-reportable and non-reportable missions, functions, and tasks.

b. Document task standards and conditions for each discrete MET and MEF.

(1) Task Standards are the minimum proficiencies required in the performance of a task. Each standard is determined by the mission owner and consists of one or more measures and criteria for execution.

(2) Task conditions are variables in the physical, military, or civil environment that affect the performance of an organization in accomplishing a specific task to the prescribed standards.

c. Identify all TAs necessary to execute each task and function.

d. Determine the criticality of a TA and when it meets the criteria in Section 9, identify it as a TCA.

e. Identify SIA - infrastructure that directly supports a TA or TCA - such as power, water, and communication networks.

f. Determine the criticality of a SIA and when it meets the criteria in Section 9, identify it as a SICA.

g. Conduct a dependency analysis of SICAs up to the first point of diversity outside of the installation perimeter. Figure 2-1 provides a notional TCA-to-SICA dependency chain.

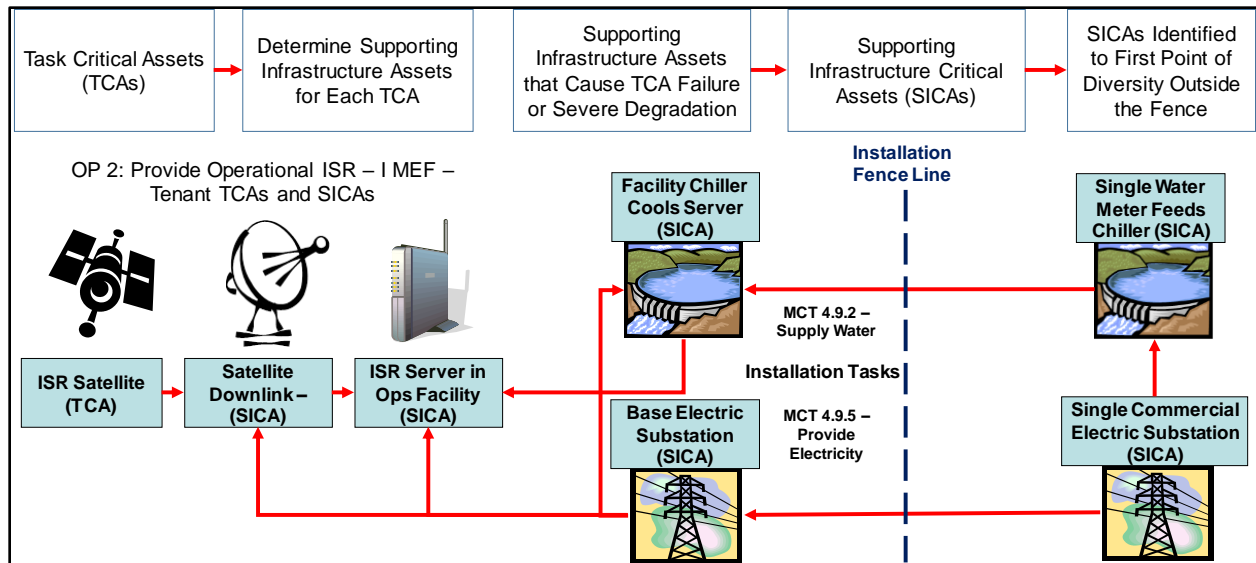


Figure 2-2. Notional Dependency Chain

h. Supported Commands coordinate with supporting Commands to ensure visibility of TCAs, SICAs, and dependencies when assets are not owned by the supported commands.

3. Mission Impact. Mission impact analysis includes the degree of impact, time to mission impact, and time required to restore support to the mission.

a. Mission Impact is the effect to mission execution if the TCA is lost, incapacitated, or disrupted. Mission impacts include:

(1) Failure: One or more standards of the MET cannot be executed due to the unavailability of the critical asset.

(2) Severe Degradation: All standards can be executed, but one or more conditions associated with the MET cannot be executed due to the unavailability of the critical asset.

b. Time to mission impact measures the time between the time the TCA becomes unavailable to support the mission, until the time the execution of the mission is impacted, assuming the MEF or MET is being executed when the TCA becomes unavailable.

c. Time to asset restoration measures the time between the discovery of the unavailability of a critical asset, and the time it takes to reestablish the asset or its capability, assuming the critical asset is totally destroyed.

4. Critical Asset Tiers. Table 2-1 provides Marine Corps definitions for critical asset tiers based on the degree of impact to mission. Following identification of a Tier 1 asset, the command must execute (or request HHQ support to execute) a risk assessment of that asset and develop a Risk Decision Package (RDP) to address identified vulnerabilities. Risk assessment data and the RDP must be entered into MC-CAMS and submitted through the chain of command for approval.

Table 2-1. Critical Asset Tiers

Tier	Impact	Description
Tier 1 TCA/ SICA	Mission failure of a Strategic Level Task or Function	An asset whose loss, incapacitation, or disruption of which could result in mission (or functional) failure at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level. More specifically, critical asset loss/disruption results in failure of Strategic National/Theater-level missions or functional capabilities.
Tier 2 TCA/ SICA	Severe Mission Degradation of a Strategic Level Task or Function	An asset whose loss, incapacitation, or disruption would result in mission (or functional) failure at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level. More specifically, critical asset loss/disruption results in severe degradation of Strategic National/Theater-level missions or functional capabilities.
Tier 3 TCA/ SICA	Mission Failure or Severe Degradation Of An Operational or Regional Level Task or Function	An asset whose loss, incapacitation, or disruption of which could result in mission (or functional) failure or severe degradation below the Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level. More specifically, critical asset loss/disruption results in failure or severe degradation of Operational-level missions or functional capabilities.
Tier 4 TCA/ SICA	Mission Failure or Severe Degradation of A Tactical Level Task or Function	An asset whose loss, incapacitation, or disruption of which could result in mission (or functional) failure or severe degradation below the Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level. More specifically, critical asset loss/disruption results in failure or severe degradation of Tactical-level missions or functional capabilities.

5. Command Approval and Validation of TCAs and SICAs. Once the initial mission and critical asset dependency analysis has been completed, Commanders review, approve, and validate mission, TCA, and SICA data.

a. Command-level review and approval must be documented via official correspondence. A copy of this official document must be uploaded in MC-CAMS by the command CIP Officer.

b. Once approved, the CIP Officer can mark these critical assets in MC-CAMS as command-approved.

c. The Commander should verify the description of the mission impact caused by the loss of a TCA. Command approval of an asset as a TCA requires a clear, sufficient, and accurate mission impact statement.

6. Installation and Tenant Command Validation

a. Enter TCAs and associated mission data in MC-CAMS once the command missions and critical assets have been approved by the Commander or the Commander's official representative.

b. Utilize the automated validation process in MC-CAMS to forward the command-approved TCA and associated mission data to the next higher headquarters (HHQ) for review and approval. Only TCAs are forwarded to a HHQ in the validation process; SICAs are not forwarded.

c. Send the validation data to the next HHQ for review and approval by checking the validation box in MC-CAMS.

7. HHQ Validation. Validation requirements apply to all echelons of command. Validation by the upper echelon or a supported command verifies the accuracy of TCA, MET, and MEF data submitted by the lower echelon or supporting command and confirms its impact on the HHQ supported missions. Validation at each reviewing echelon requires:

a. Verification of the accuracy of mission data and mission impact caused by the loss of the TCA at each echelon of command.

b. Verification of baseline elements of information (BEI) for each mission and TCA, including time to mission impact and time to restore the TCA.

c. Determining whether the impact of loss of a subordinate command TCA and inability to execute its supported MET/MEF has any impact on its MET/MEF execution. If so, document the mission impact, impact description, and time to impact for the HHQ-supported MET/MEF.

(1) If there is no mission impact to the HHQ-supported MET/MEF, then no mission impact should be documented for that MET/MEF in MC-CAMS.

(2) Validation through the chain of command should filter lower-level tactical TCAs that are less critical to the execution of a HHQ MET, including Strategic National (SN), Strategic Theater (ST), and Operational (OP) tasks.

(3) The HHQ echelon should also determine if other assets are available at the higher echelon of command that can be utilized to replace the TCA and support the associated task identified by the lower echelon command.

(4) Validation is the responsibility of the organization that owns the asset and the organization that executes the mission the TCA has been

MCO 3501.36B
12 Feb 2021

associated with; ownership of the TCA itself does not impact the validation responsibility. Coordination between asset and mission owners is necessary to effectively validate TCA data.

Critical Asset Restricted Area Designations

1. Reference (m) provides definitions and security requirements for Level One, Level Two, and Level Three restricted areas.

2. To support uniform application of security measures for Marine Corps critical assets and infrastructures, critical assets shall be assigned restricted area levels of protection as follows:

a. Defense Critical Assets and Tier 1 Critical Assets shall be designated as Level 2 Restricted Areas at a minimum.

b. Tier 2 Critical Assets shall be designated as Level 2 Restricted Areas at a minimum.

c. Tier 3 Critical Assets may be designated as Level 1 Restricted Areas, or other lesser protective measures may be undertaken as approved by the Commander.

d. Tier 4 Critical Assets may be designated as a Level 1 Restricted Area, or other lesser protective measures may be undertaken as approved by the Commander.

3. Commanders shall consider local threats and hazards in the designation of restricted areas.

4. Physical Security Surveys shall be conducted for each critical asset assigned a restricted area designation in accordance with reference (m). Physical Security Surveys shall be classified in accordance with reference (n) and documented in MC-CAMS.

Guidance for Resourcing Risk Reduction Plans

1. General. For Marine Corps Critical Infrastructure Program (CIP) risk reduction plans to be funded in a resource-constrained environment, plans must clearly demonstrate the ability to reduce risk to the command's mission-critical assets and supporting infrastructure. Internal Fiscal Year (FY) budgets and effective Mission Assurance (MA) Risk Management (RM)-based resource funding strategies must be developed and executed to capture total life-cycle costs and demonstrates positive return on investment. In the context of CIP, a significant part of return on investment is the degree to which risk to mission has been reduced. The FY budget and funding strategy must focus on a mission impact-based priority list of risks generated from the RM process detailed in reference (j) of this Order. Funding avenues described in this Enclosure should be considered and used when developing budgets and CIP risk reduction plan funding requests.

2. Internal CIP Budget Development. The command CIP Point of Contact (POC) will review current critical asset risk reduction plans with estimated project costs to determine a total funding request amount that has been or will be submitted during the FY. The POC will estimate funding requirements for projects that are under planning/development that will likely be submitted in the FY. By adding the funding requests together, the CIP POC completes a rough FY CIP budget development plan that encompasses priority risk reduction plans, projects, and actions. The command CIP Working Group is responsible for developing the FY Prioritized Risk Reduction Plan Matrix and Budget.

3. Resource Planning Process. The primary mechanism used to coordinate CIP risk reduction resource planning is the command CIP Working Group (CIPWG). This Working Group is a discrete subgroup of the Mission Assurance Working Group (MAWG) made up of protection stakeholders and funding experts in order to best match resourcing needs with risk reduction plan requirements. The CIPWG will analyze all risk reduction plans and associated risk assessment data that support prioritizing resource needs, and will recommend to the MAWG placement of each resource requirement in one of four categories of importance in relation to risk to mission: 1) Critical Priority, 2) High Priority, 3) Medium Priority, and 4) Low Priority. The command MAWG will review and vet the risk reduction plan matrix and budget, and assign resource categories of importance to each plan element.

a. Prioritizing Resource Categories

(1) Critical Priority. A critical resource requirement is any risk reduction plan that addresses mission critical assets and supporting infrastructure with mission impact ratings - taken from the "Criticality" piece of the risk assessment methodology - between 0.76 and 1.00 and overall asset risk ratings between 0.76 and 1.00. These ratings justify a critical resourcing priority because of the potential risk for very significant mission impact and/or failure if the risk reduction plan is not implemented. A critical priority resource requirement addresses an unacceptable risk and should be considered in the top 20 percent of the commander's funding priorities.

(2) High Priority. A high resource requirement is assigned to risk reduction plans that address mission critical assets and supporting infrastructure with mission impact ratings between 0.51 and 0.75 and asset risk ratings between 0.51 and 0.75. These ratings justify a high priority

category because of the potential risk for significant degradation and disruption to mission execution if the risk reduction plan is not implemented. This rating indicates highly probable threats/hazards could exploit very significant asset vulnerabilities. The high priority resource requirement addresses an unacceptable risk in the top 21-40 percent of the commander's funding priorities.

(3) Medium Priority. A medium resource requirement is assigned to risk reduction plans that address mission critical assets and supporting infrastructure with mission impact and asset risk ratings between 0.26 and 0.50. These ratings justify a medium priority category because of the potential risk for some degradation and disruption to mission execution if the risk reduction plan is not implemented. The medium priority resource requirement addresses an unacceptable risk in the top 41-60 percent of the commander's funding priorities.

(4) Low Priority. A low resource requirement is assigned to risk reduction plans that address mission critical assets and supporting infrastructure with minimal mission impact and asset risk ratings between 0.01 and 0.25. These ratings reflect the low likelihood of threat/hazards that could exploit asset vulnerabilities. These ratings are indicative of situations where risk may be acknowledged or deferred until the requirement can be included in other funding requirements.

b. Risk Decision Package (RDP) Development and Decision. To facilitate the determination of the appropriate resource priority to assign to a risk reduction plan, an RDP will be developed by the CIPWG for presentation to the MAWG and Mission Assurance Executive Committee. RDPs are an instrumental tool to present risk management data and Courses of Action (COAs) to address the risk to assets and missions and to support the resource prioritization and request process. Although the RDP is not a funding request vehicle, it is developed to assist commanders in risk decision making. RDPs present two or more COAs designed to address and reduce identified risk to critical assets and supporting infrastructure. Importantly, the RDP recommends the best COA based on the optimization of both risk reduction effectiveness and cost of implementation.

(1) The RDP must include the asset's baseline elements of information, including its supported missions and mission impact if lost; the most likely threats and hazards that could exploit specific asset vulnerabilities; and other information necessary to facilitate the commander's decision to reduce risk, including the resource requirements needed to execute the risk reduction plan.

(2) Commanders may respond to RDPs in three ways: acknowledge risk, reduce risk by implementing remediation measures, or defer the risk decision package to Higher Headquarters for decision, funding, or other direction. Commanders may fund RDP decisions through resources within the control of the local command or resources that require Higher Headquarters submission and prioritization.

c. Resourcing Options

(1) Planning, Programming, Budgeting, & Execution (PPBE) Process. PPBE is the business process of allocating resources within the DoD. Resource planning and programming is accomplished through the Program Objective Memorandum (POM) process, and budgeting and execution is accomplished during

the execution of the Future Years Defense Plan. CIP personnel must maintain awareness of the local comptroller timeline 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. See Figure 4-1.

Oct / Nov	Dec	Jan / Feb	Mar / Apr / May	Jun / Jul	Aug / Sept
Continuing Resolution Authority of Current Year Budget Distribution		Current year Mid-Year Review*	Results of Mid-Year Review	Close-Out and Year-End Sweep	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	Def	Def
Program Objective Memorandum/Program Review (Future Years)					

Figure 4-1. Budget/Data Call Timeline

(a) POM Process. The POM process is the primary method of programming resources, and addresses the programming of funding execution of two years in advance of the current year. POM submissions are evaluated by Program Evaluation Boards for each type of appropriation and Marine Corps Programming Codes (MCPCs).

(b) Universal Needs Statement (UNS). An UNS is the most important component in the Marine Corps Force Development System (MCFDS) and it is a component of the planning and programming element of PPBE. As the primary means of entry into the MCFDS, the UNS acts as a work request for current and future capabilities within EFDS. The UNS identifies operational enhancement opportunities and deficiencies in capabilities. Opportunities include new capabilities and the elimination of redundant or unneeded capabilities. The term "Universal" highlights its common use by Marine Corps organizations to capture both current needs and future needs developed through analysis, assessment, and experimentation with future concepts.

(c) Deliberate UNS (D-UNS). A D-UNS is a mechanism to communicate future desired capabilities to HQMC for consideration to enter the MCFDS and other deliberate requirements planning and resourcing processes. The D-UNS identifies capability gaps, recommended solutions, or operational enhancement opportunities that 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.

(d) Urgent UNS (U-UNS). A U-UNS is an accelerated UNS. The U-UNS process provides rapid acquisition of a capability to meet an urgent requirement in support of combat and contingency operations that threaten mission accomplishment or are life-threatening.

(e) Combatant Commander Initiative Fund (CCIF). The primary focus of the CCIF is to support unforeseen requirements critical to CCMD's joint war-fighting readiness and national security interests. The strongest candidates for approval are initiatives that support CCMD 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 expense of defense personnel for bilateral or regional cooperation programs.

(2) Types of Appropriation

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

(b) Procurement. Procurement is a three-year appropriation that finances the purchase of weapons, combat vehicles, guided missiles and equipment, communications and electronics equipment, and contracts. Procurements made with non-appropriated funds should aid in obtaining products and services through purchasing and contracting operations. Items purchased with procurement funds are investment items subject to the limitations of the current expense/investment threshold.

(c) Military Construction. Military Construction (MILCON) funds are obtained through a formal process using DD Form 1391 and must be approved by Congress under applicable procedures. These funds are used to prepare ground for construction; purchase construction materials; and pay construction labor, crane rental, and other expenses related to the construction of buildings, locks, dams, and roadways. The Facility Sustainment, Restoration, and Modernization (FSRM) Project Process to improve existing facilities is similar to the MILCON process and follows the same steps for planning, justification, validation, project management, funding allocation/execution.

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

(3) Cost-Benefit Analysis. Cost-benefit analysis must be conducted twice in the RM and resource management process - first, during consideration of executable risk reduction COAs, and second, to prioritize resource requirements in a CIPWG/MAWG or other command forum. At a minimum, a cost-benefit analysis is an analytical process 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. In addition to monetary and resource expenses, CIP-related cost estimates should also incorporate the reduction of risk from near-term implementation of the mitigation plan as well as long-

term efforts through the PPBE process, and compare residual risk among potential mitigation measures to determine which measures will provide the greatest risk reduction impact. Employing a comprehensive cost-benefit analysis of each potential mitigation measure will assist the commander with managing risks and prioritizing funding requests.

(4) Advocacy. If a funding request is submitted to Higher Headquarters via the appropriate means, CIP personnel will seek advocacy from their Higher Headquarters chain of command. This advocacy is critical for ensuring protection projects are properly prioritized in terms of mission impact at each Higher Headquarters level.

(5) Tracking. The CIPWG or CIP POC will maintain a POA&M that captures the status of RDPs, projects, and resourcing requests. Project and resourcing status will be updated every quarter and results provided to the CIPWG. All risk reduction plans and projects status will be updated in Marine Corps Critical Asset Management System (MCCAMS) every quarter. In particular, Project Start Date and Project End Date will be updated as required to reflect accurate status.

APPENDIX A

Glossary of Acronyms and Abbreviations

AT	Antiterrorism
ADC	Assistant Deputy Commandant
AVN	Aviation
BCS	Building Control System
BEI	Baseline Elements of Information
C2	Command and Control
C4	Command, Control, Communications, and Computers
CAIP	Critical Asset Identification Process
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
CIR	Critical Information Requirement
COA	Course of Action
CONPLAN	Contingency Plan
COOP	Continuity of Operations
CPI	Critical Program Information
CS	Control System
D-UNS	Deliberate Universal Needs Statement
DBS	Defense Business System
DC	Deputy Commandant
DCI	Defense Critical Information
DCIP	Defense Critical Infrastructure Protection
DIB	Defense Industrial Base
DIR	Director
DRRS	Defense Readiness Reporting System
DTRA	Defense Threat Reduction Agency
DON	Department of the Navy
FRCS	Facility Related Control System
FY	Fiscal Year
HHQ	Higher Headquarters
HQMC	Headquarters Marine Corps
HRA	High Risk Area
HS	Health Services
HVT	High Value Target
I	Information
I&L	Installations and Logistics
I&W	Indications and Warnings
ICS	Industrial Control System
IGMC	Inspector General of the Marine Corps
iNFADS	internet Navy Facilities Asset Data Store
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JCA	Joint Capabilities Area Assessment
MA	Mission Assurance
MAA	Mission Assurance Assessment
M&RA	Manpower and Reserve Affairs
MARFOR	Marine Forces
MARFORCYBER	Marine Forces Cyberspace
MC-CAMS	Marine Corps Critical Asset Management System
MCCAST	Marine Corps Compliance and Authorization Support Tool
MCEIP	Marine Corps Enterprise Integration Plan
MCEN	Marine Corps Enterprise Network
MCIA	Marine Corps Intelligence Activity

MCICOM	Marine Corps Installations Command
MCTIMS	Marine Corps Training Information Management System
MDI	Mission Dependency Index
MEF	Marine Expeditionary Force
MEF	Mission Essential Function
MET	Mission Essential Task
METL	Mission Essential Task List
MILCON	Military Construction
MCRC	Marine Corps Recruiting Command
MRT-C	Mission Relevant Terrain in Cyberspace
NIPR	Non-classified Internet Protocol Router
O&M	Operations and Maintenance
OPLAN	Operations Plan
OPR	Office of Primary Responsibility
OPREP-3	Operational Report - 3
OT	Operational Technology
PII	Personally Identifiable Information
POM	Program Objective Memorandum
PPBE	Planning, Programming, Budgeting, and Execution
PP&O	Plans, Policies, and Operations
P&R	Programs and Resources
PIR	Priority Intelligence Requirement
RDP	Risk Decision Package
RM	Risk Management
SAP	Special Access Program
SAR	Special Access Requirement
SCADA	Supervisory Control and Data Acquisition
SIA	Supporting Infrastructure Asset
SICA	Supporting Infrastructure Critical Asset
SIPR	Secret Internet Protocol Router
TA	Task Asset
TCA	Task Critical Asset
TECOM	Training Education Command
U-UNS	Urgent Universal Needs Statement
UCS	Utility Control System
UNS	Universal Needs Statement
WS	Weapons System

APPENDIX B

Glossary of Terms and Definitions

Activity. A unit, organization, or installation performing a function or mission.

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.

Command. A unit or units, an organization, or an area under the command of one individual.

Critical Infrastructure. Synonymous with DCI. See "Defense Critical Infrastructure" below.

Defense Critical Asset. An asset of extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DoD to fulfill its mission

Defense Critical Infrastructure. The composite of DoD and non-DoD assets essential to project, support and sustain military forces and operations worldwide. DCI is a combination of TCAs and DCAs.

Dependency Analysis. The process of identifying other assets each TCA depends upon to function or operate as intended in support of a MET or MEF.

Mission Essential Function (MEF). The specified or implied tasks required to be performed by, or derived from, statute, executive order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to achieve DoD component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control.

Mission Essential Task (MET). A MET is a mission task selected by a commander deemed essential to mission accomplishment and defined using the common language of the universal joint task list in terms of task, condition, and standard.

Supporting Infrastructure Asset (SIA). Any asset on which a TCA, TA, or other supporting infrastructure uses or depends on to operate. While TCAs and TAs are utilized to directly execute a MET or function, SIAs are used to directly support the operation of other assets - such as a TA, TCA, or SICA (e.g., an earth station or satellite downlink asset [SICA] which receives feeds of information from a satellite [TCA]).

Supporting Infrastructure Critical Asset (SICA). A SIA that directly supports the functioning or operation of a TCA (or another designated SICA), and the unavailability of the SIA will cause impact - asset failure or asset severe degradation - to the operation of the supported TCA or SICA.

Task Asset (TA). An asset that is directly used to support execution of one or more Mission Essential Task (MET), core functions or capabilities (e.g., a satellite used to directly execute a surveillance task). One or more task assets may support execution of a single task or function.

Task Critical Asset (TCA). An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or Defense Infrastructure Section Lead Agent organizations to execute the task or MET it supports. TCAs are used to identify Defense Critical Assets.

Time to Mission Impact. The time to mission impact is measured from the time the TCA becomes unavailable to support the function/MET, until the time the function/MET execution is impacted. The measurable impact is either failure or severe degradation of the function or task. In determining the time to mission impact, assume that the function or MET is currently in execution when the TCA becomes unavailable.

Time to Asset Restoration. This is the time between the discovery of the unavailability of a TCA and the time it takes to bring that asset - or its' capability - back on-line to support execution of the supported function or MET. For purposes of determining asset restoration time, assume that the critical asset has been totally destroyed (worst-case scenario).