



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

Canc: JUL 2018

MCBul 3100

PP&O

14 JUL 2017

MARINE CORPS BULLETIN 3100

From: Commandant of the Marine Corps
To: Distribution List

Subj: OPERATIONS AND DEFENSE OF THE MARINE CORPS ENTERPRISE NETWORK (MCEN)

Ref: (a) MCO 3100.4
(b) EXORD CJCS, "EXORD to Cyberspace Operations Command and Control (C2) Framework", February 1, 2016
(c) USCYBERCOM OPORD 16-0139 "Implementation of Updated Cyberspace Operations Command and Control Framework Delegation of Directive Authority for Cyberspace Operations", September 6, 2016
(d) SECNAVINST 3052.2
(e) SECNAVINST 5400.15C
(f) MCO 5400.52
(g) Marine Corps Information Enterprise Strategy, December 14, 2010
(h) MCO 3501.36A
(i) MCO 5311.1E
(j) DOD Instruction 5000.02, "Operation of the Defense Acquisition System" (Incorporating Change 2, Effective February 2, 2017)
(k) SECNAVINST 5000.2E
(l) MCO 5400.54
(m) MCO 5311.6
(n) 5 U.S.C. 552a
(o) SECNAVINST 5211.5E
(p) SECNAV M-5210.1
(q) DOD Dictionary of Military and Associated Terms, as of May 2017
(r) Joint Publication 3-12, "Cyberspace Operations," February 5, 2013

Encls: (1) Glossary
(2) MCEN Technical/Logical Areas of Support (AOS)
(3) MCEN Command and Control Diagram

1. Situation

a. This Marine Corps Bulletin (MCBul) updates current Marine Corps policy in MCO 3100.4, Cyberspace Operations, reference (a). It does not alter or supersede the existing authorities or policies of the Director, Command, Control, Communications, and Computers (C4) with respect to the roles and responsibilities retained as the Authorizing Official (AO) and Deputy Department of the Navy (DON) Chief Information Officer (Marine Corps) (DDCIO (MC)), per Department of Defense (DOD), DON, and other laws and regulations. It also does not replace or supersede the Commander, Marine Corps Forces Cyberspace Command (COMMARFORCYBER) Directive Authority for Cyberspace Operations (DACO) for the security, operations and defense of the

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

Marine Corps Cyberspace Environment (MCCE) (per glossary, the Marine Corps portion of the Department of Defense Information Network (DODIN)).

b. This MCBul establishes effective command relationships between Headquarters Marine Corps (HQMC), the Supporting Establishment, and the Marine Forces (MARFORs) for operating and defending the MCEN. It also provides a bridge until Deputy Commandant, Information (DC I) has the operating capacity to consolidate and coordinate existent Marine Corps policy on cyberspace operations and cybersecurity matters.

2. Mission. Establish the command and control framework that provides unity of effort to operate and defend the MCEN, in order to provide a single network-enabled operating environment that enables Marine air-ground task force (MAGTF), naval and joint combined arms, preserves freedom of maneuver and the ability to project power in and throughout the cyberspace domain in support of the range of military operations.

3. Execution

a. Commander's Intent. To provide direction for commander and senior leader involvement in the cybersecurity performance of their organizations by establishing responsibilities and organizational relationships between the different organizations of the Marine Corps that provide MCEN operations and defense capabilities and support to the joint force, Marine Corps operating forces (OPFOR), and the supporting establishment.

b. Endstate. An agile, secure, and unified MCEN that is supported by an effective organizational framework, with clearly delineated command relationships that enable MAGTF operations in a contested or constrained cyberspace domain in support of Joint and MAGTF requirements.

c. Concept of Operations

(1) Operational responsibility and management of the DODIN is parsed into three authority tiers. Per reference (b), Tier 1 consists of the entire DODIN; Tier 1 authorities are retained by Joint Forces Headquarters (JFHQ)-DODIN. Tier 2 consists of the MCCE as the Marine Corps' portion of the DODIN, which includes the MCEN. Marine Forces Cyber Command (MARFORCYBER) is the Tier 2 authority responsible for the MCEN. Tier 3 consists of all sub-elements of the MCEN operated and defended by the Marine Corps. Commanders, Deputy Commandants, and Directors listed in paragraph 3.d are the Tier 3 authorities responsible for MCEN operations within their Area of Responsibility (AOR). Tier 3 authorities are accountable to COMMARFORCYBER for the operations and defense of the MCEN within their assigned Technical/Logical Area of Support (AOS) (see enclosures (2) and (3)); this accountability cannot be delegated. COMMARFORCYBER shall delegate specific MCEN permissions to MARFORs, Marine Corps Installation Command (MCICOM) commanders, and the Director, Marine Corps Staff (DMCS) necessary for specific operations and defense of the MCEN. Specific MCEN permissions will be prescribed and delineated by COMMARFORCYBER in the Marine Corps Cyberspace Operations Order (OPORD) to be published.

(2) Effective operation of the MCEN requires senior leadership involvement to maintain the security and integrity of the MCEN. Uncoordinated actions have the potential to impact operations beyond a given Technical/Logical AOS. All actions taken by Tier 3 authorities will be directed by or coordinated through MARFORCYBER. If coordination with

MARFORCYBER will create time delays that will affect the execution of combat operations, likely resulting in the loss of life, serious injury or mission failure; then Tier 3 authorities may delay defensive cyberspace operational actions, but must immediately notify MARFORCYBER of those delays. Tier 3 authorities may direct defensive cyberspace operations (DCO) within their Technical/Logical AOS without prior coordination. If the delay caused by this coordination will likely result in an adverse effect to operations, Tier 3 authorities must then notify MARFORCYBER of their actions.

(3) Per references (b) and (c), Commander United States Cyber Command (CDRUSCYBERCOM) delegated DACO over all Marine Corps DOD Components to COMMARFORCYBER. DACO, which was granted to CDRUSCYBERCOM via United States Strategic Command (USSTRATCOM), is the authority to issue orders and directives to all DOD components for directing the execution of global DODIN operations and DCO-internal defense measures (DCO-IDM) to compel unity of action to operate and defend the DODIN. DACO provides COMMARFORCYBER authority to implement orders from CDRUSCYBERCOM/CDRJFHQ-DODIN and independently issue orders and directives to compel unity of action in order to operate and defend the MCCE (per glossary, the Marine Corps portion of the DODIN). COMMARFORCYBER is authorized to issue orders and directives to all Marine Corps organizations to direct the execution of DODIN operations and DCO-IDM. MARFORCYBER is the supported command; all other Marine Corps organizations are in support of MARFORCYBER for the execution of actions directed under DACO. Simply stated, DACO allows COMMARFORCYBER to order network related activities necessary to defend and operate the MCEN.

(4) Deputy Commandant, Plans, Policies, and Operations (DC PP&O) is responsible for ensuring institutional readiness for Marine Corps plans and operations. DC PP&O assesses institutional, force management, and future challenge risks, and coordinates the development and execution of Title 10 activities in order to support force generation actions. For MCEN operations, DC PP&O will issue guidance to MARFORs/Marine Expeditionary Forces (MEFs), coordinate and when required consolidate risk assessments, determine prioritization, and allocation of critical cyberspace assets and infrastructure, to enable accomplishment of the Service's Title 10 responsibilities.

d. Subordinate Element Missions

(1) Deputy Commandant, Plans, Policies and Operations (DC PP&O)

(a) Ensure that law enforcement mechanisms for operations and defense of the MCEN are in place in accordance with reference (d).

(b) Oversee, manage, and approve the identification, prioritization and assessment of cyberspace assets and infrastructure critical to the execution of Marine Corps missions, capabilities, and core functions.

(c) Publish Operations Event/Incident Report Serious Incident Report (OPREP-3 SIR) reporting thresholds for MCEN outages via Commandant Marine Corps (CMC) Commander's Critical Information Requirements.

(d) During MCEN outages, publish assessments of network risk assessments, issue guidance to MARFORs/MEFs, and determine prioritization/allocation for critical cyberspace assets and infrastructure as required.

(e) Provide Service-level oversight and assistance to MARFORCYBER in assessing network risk assessments for MCEN outages that have operational and/or institutional impact.

(2) Deputy Commandant, Combat Development & Integration (DC CD&I)

(a) Conduct all combat development and integration activities for the execution of cyberspace operations within the context of the Marine Corps Capability Based Assessment process.

(b) Develop and publish operations and defense of the MCEN capability requirements, concepts, studies, doctrine, and tactics, techniques, and procedures.

(c) Conduct mission area analyses for all assigned operations and defense of the MCEN mission areas and ensure relevant Marine Corps cyber capabilities are included in appropriate simulations, models, and exercises.

(d) Identify and validate cyberspace operations capability requirements and establish necessary changes to doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF).

(e) Establish priorities for acquisition of cyberspace operations-related equipment and work collaboratively with Marine Corps Systems Command (MARCORSYSCOM) and Deputy Commandant Installations and Logistics (DC I&L) to integrate and develop cyberspace capabilities.

(f) Through Commanding General Training and Education Command, and in coordination with applicable occupational field (OccFld) managers, ensure adequate cyberspace operations training standards are developed and adequate cyberspace operations instruction is provided by Marine Corps Service Schools to include lessons provided by the College of Distance Education and Training (CDET) on MarineNet. This includes the identification of Military Occupational Specialty (MOS) and billet requirements for cyberspace operations instructors to support those programs.

(g) Serve as the capability portfolio manager for cyber-related activities. Develop and maintain Future Year Defense Program plans for cyber-related programs.

(h) Assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(3) Deputy Commandant, Installations and Logistics (DC I&L)

(a) Conduct Marine Corps installation, facilities, and logistics management and analysis for cyberspace operations.

(b) Develop and publish Marine Corps installations, facilities, and logistics policy and procedures for operations and defense of the MCEN.

(c) Coordinate with MARCORSSYSCOM, Naval Facilities Engineering Command (NAVFAC), and U.S Army Corps of Engineers (USACE) on operations and defense of the MCEN and other network requirements for installations and facilities.

(d) Coordinate with MARCORSSYSCOM, NAVFAC, and USACE to address MCEN configuration control and management requirements per reference (e).

(e) Through the Commander, Marine Corps Installations Command (COMMCICOM) coordinate assigned Marine Corps cyberspace operations, projects, and maintenance activities.

(f) Through the Commanding General, Marine Corps Logistics Command (CG LOGCOM) coordinate assigned Marine Corps cyberspace operations logistics activities.

(g) Advocate for the inclusion of cyber-related technical standards within applicable unified facilities' criteria documents.

(h) Plan, program, and conduct installations telecommunications and information technology (IT) inspections supporting cyberspace operations.

(i) Ensure all installation commanders' Tables of Organization are appropriately structured and staffed to facilitate Installation Communications Distribution System operations, IT services, and required installation MCEN operations and defense activities.

(j) Assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(4) Director, Marine Corps Staff (DMCS)

(a) Establish and maintain staff expertise capable of planning and exercising command and control of cyberspace operations within the DMCS Technical/Logical AOS, per enclosure (2). Identify gaps in capability to the Cyberspace Operational Advisory Group for resolution within existing processes.

(b) Incorporate cyberspace MCEN operations and defense into training and exercises.

(c) Include realistic scenarios for operating and defending the MCEN under degraded cyberspace conditions into existing exercise programs.

(d) Assist PP&O in the assessment of operational impacts of network vulnerability outages and DCO-IDM responses. Assist PP&O in assessing readiness and mission risk assessments resulting from MCEN outages. Assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(5) Director, Command, Control, Communications, and Computers (C4)

(a) As per reference (f), serve as principal advisor to CMC for Marine Corps wide IT execution.

(b) In coordination with COMMARFORCYBER, DC PP&O, DC CD&I, DC I&L, and COMMARCORSYSCOM, lead the development of the MCCE strategies and plans to provide a single, disciplined MCEN that provides commanders and staffs the ability to conduct operations through shared, secured, reliable environments in accordance with references (f) and (g).

(c) As the DDCIO (MC), provide IT capital planning and portfolio management; develop and manage an IT architecture and workforce; provide leadership and governance of IM/IT activities for the Marine Corps; and oversees all planning, directing, and coordinating of IT capabilities that support Marine Corps warfighting and business functions in accordance with reference (f).

(d) As the MCEN Designated Approving Authority/Authorization Official, implement policies and procedures to cost-effectively reduce risks to an acceptable level; develop and maintain a Service wide information security program as required; and coordinate activities with risk executive (function), CIO, and the senior Service Information Security Officer.

(e) Through the Authorization process, accept the risks of the systems in operation; formally approve systems for operation; disapprove systems for operation; and if the systems are already operational, halt operations if unacceptable security risks exist.

(f) Advise PP&O; I&L; CD&I; and other Marine Corps agencies/commands on C4 positions with respect to MCEN operations and defense capabilities, systems, planning, programming, and policy.

(g) In coordination with the MARFORs, MEFs, supporting establishment, and other appropriate organizations, lead the development of a future service-wide cyberspace operations and defense force structure that enables clear lines of command authority.

(h) Coordinate with PP&O Security Division, MARCORSYSCOM, MARFORs, and MCICOM for the assessment of Marine Corps critical C4 systems, permanent and tactical capital assets, and networks in accordance with reference (h).

(i) Conduct planning for redundant architecture that enables the remediation, mitigation, and assurance of critical C4 systems, assets, and infrastructure, so that a minimum essential level of command and control functions can be maintained and sustained.

(j) Review and assess all computer and software procurement requests as the Marine Corps IT Expenditure Approval Authority.

(k) In coordination with CD&I, I&L, Programs and Resources (P&R), MARCORSYSCOM, and MARFORs, and in accordance with references (i), (j), and (k), ensure appropriate validation, acquisition expenditures, integration, maintenance, and allocation of critical C4 systems, assets, and infrastructure capabilities and resources are sufficient to meet OPFOR and garrison commanders' cyberspace operational requirements.

(l) Retains responsibility for identification and acceptance of risk for all planned and developed solutions to meet MCEN requirements.

(m) Oversee, implement, and direct the formal security accreditation process, ensuring all information systems operate within acceptable levels of risk.

(n) Establish and publish network operations Service Level Requirements for use by MARCORSYSCOM in designing service capabilities.

Provide the necessary resources to design and successfully field service capabilities.

(o) Assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact and advise PP&O in the development of guidance to the MARFORs and MEFs.

(p) Conduct positive communication and coordination of AO actions to ensure MARFORCYBER has visibility on all new connections being made to the MCEN at the earliest practical point.

(6) Director, Intelligence (DIRINT)

(a) Develop plans and policy for the conduct of intelligence and counterintelligence activities in support of MCEN operations and defense in concert with Under Secretary of Defense for Intelligence, Office of the Director of National Intelligence, and joint intelligence plans and policy.

(b) Support the review and validation of operational requirements and associated capabilities that relate to intelligence, surveillance, and reconnaissance (ISR) capabilities that operate in and through cyberspace.

(c) Coordinate or provide threat assessments and intelligence support to MARFORCYBER network risk assessments for MCEN outages that have an operational impact.

(7) Commander, Marine Corps Systems Command (COMMARCORSSYSCOM)

(a) Conduct research, development, and acquisition activities to satisfy validated cyberspace operations requirements.

(b) Provide technical support for the development of capability requirements documents.

(c) Provide technical authority, engineering, and lifecycle support for MCEN operations and defense equipment and services in accordance with reference (g).

(d) As the Change Control and Configuration Management process owner, create, document, manage, and coordinate change control processes that authorize work on the MCEN and comply with guidance and direction from governance organizations external to the Marine Corps. Define standards and metrics to ensure changes are fully coordinated, implemented as prescribed, validated, and meet prescribed service levels. Implement, oversee and chair a MCEN Enterprise Change Control and Configuration Management Process.

(e) Ensure all Program of Record deployed and managed IT systems are capable of maintaining information assurance vulnerability alert and Security Technical Implementation Guide compliance, building requirements into all awarded deployment and support contracts. Ensure timely upgrades and refresh of IT systems to prevent them from reaching End-of-Life or End-of-Service while on the MCEN and avoid exposing the MCEN to vulnerabilities.

(f) Assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(8) Commander, Marine Corps Forces Cyberspace Command
(COMMARFORCYBER)

(a) Conduct full spectrum cyberspace operations to include DODIN operations, DCO, DCO-IDM, and, when directed, offensive cyberspace operations in support of CDRUSCYBERCOM.

(b) In accordance with authorities directed by CDRUSCYBERCOM, direct and as required coordinate all actions taken to operate and defend the MCEN by Tier 3 organizations.

(c) Conduct positive communication and coordination of actions taken on the MCEN with C4 at the earliest practical point.

(d) Coordinate follow-on actions with C4 and other applicable Marine Corps organizations to update the MCEN configuration and security baseline after network actions are complete.

(e) Be responsible for process ownership and process management for the enterprise - IT service management (ITSM) Service Operations & Service Transition domains and included MCEN ITSM processes; including process development, detailed documentation of enterprise-wide procedures standard operating procedures, role assignments, implementation, and enforcement.

(f) Be responsible for identifying and accepting temporary risk variances to ongoing cyberspace operations from predefined enterprise risk decisions/levels approved by the AO. In support of this responsibility, authorize the temporary installing or disconnecting of a network/system and assume resulting risk in support of ongoing cyberspace operations.

(g) Be responsible for installation, configuration, patching, and day-to-day operation of wide area network infrastructure equipment in all Marine Corps data centers.

(h) Enforce/comply with Service Level Agreements published by C4.

(i) In accordance with MCEN governance processes (Change and Configuration Management, MCEN Unification Plan; approved MCEN technology pilot programs, etc.), build, configure, and sustain certified solutions using existing hardware/software capabilities, up to and including version upgrades/enhancements inherent in fielded or purchased hardware/software solutions and associated support.

(j) Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist Tier 3 organizations and DC PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and coordinate, consolidate and report network risk assessments to PP&O for MCEN outage that have an operational impact.

(9) Commanders, Marine Forces (COMMARFORs)

(a) Establish and maintain staff expertise capable of planning and exercising command and control of cyberspace operations.

(b) As appropriate, incorporate MCEN operations and defense into training and exercises.

(c) Include realistic scenarios for operating and defending the MCEN under degraded cyberspace conditions into existing exercise programs.

(d) Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(10) Commander, Marine Corps Installation Command (COMMCICOM) per reference (1).

(a) Marine Corps Forces Level:

(1) Conduct oversight of MCI Region and subordinate Installations planning and submission of required resources: financial, personnel, and material for provision of MCEN distribution, delivery, and customer support aboard Marine Corps installations in accordance with this Bulletin and reference (1).

(2) Coordinate with MARFORCYBER, NAVFAC, and USACE for the efficient implementation of regional and installation-level MCEN projects.

(3) Supervise consolidation of telecommunications infrastructure and associated IT in order to reduce threat to the MCEN. Coordinate and identify mitigation and solution strategies to C4 and PP&O.

(4) Be responsible for establishing United States Marine Corps (USMC) data center management standards; and provide oversight for installation, configuration, and management of data center infrastructure within Marine Corps Bases and Stations. Establish data center initial Service Level Targets and Service-Level Agreements once data center standards are achieved. Effectively manage data center capacity to ensure future MCEN requirements.

(5) Be responsible for the compliance oversight for installation, configuration, and patching of Base and Local Area Network infrastructure resident within Marine Corps Bases and Stations.

(6) During enterprise configuration management, ensure MARCORSYSCOM is informed of impacts and constraints of DON construction policies and aligned facilities planning processes.

(7) Ensure MCCE matters and MCEN operations and defense are included within each installation master plan and associated base electronics systems engineering plans.

(8) Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(b) Regional Level:

1. Execute supporting, supported command relationships for operations and defense of the MCEN as outlined in this Bulletin and identify resourcing shortfalls for conduct of MCEN operations per reference (1).

2. Host and maintain regional MCEN service and security stacks required for the operation and defense of the MCEN.

3. Provide MCEN Services, in accordance with C4-published MCEN service model, to assigned OPFOR units and/or supporting establishment Commanders.

4. Provide tiered MARFOR garrison and deployed MCEN customer support in accordance with the C4-published IT customer support model.

5. Consolidate installation-level MCEN operational service and customer support to regional service support centers.

6. Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

7. Enforce/comply with service Level Agreements.

(c) Installation Level:

1. Host required installation-level MCEN authentication and cyber security hardware in support of C4-published MCEN architecture and network distribution methodologies.

2. Responsible to conduct day-to-day operations, installation, configuration, and patching to Base and Local Network infrastructure equipment resident within Marine Corps Bases and Stations.

3. Provide MCEN delivery services to the MARFORs, HQMC, and Supporting Establishment tenants while garrisoned.

4. Provide end-user support services for MCEN devices and applications.

5. Process operational directives in support of respective battlespace owner's mission to operate and defend the MCEN.

6. Coordinate with regional G6s to support MCEN hardware and software implementation projects as required.

7. Provide MCI regional G6 with identified MCEN operational customer service and support gaps.

8. Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

9. Enforce/comply with service Level Agreements.

(11) Commander, Marine Corps Forces Reserve (COMMARFORRES)

(a) Coordinate with MARFORCYBER, C4, and MARCORSYSCOM for the efficient implementation of the fiscal, personnel, and material resources required that provide seamless MCEN distribution, delivery, and customer support services at each of the 161 Home Training Centers (HTCs)

(b) Coordinate with MARFORCYBER for the efficient implementation of Reserve and HTC MCEN projects.

(c) Represent the equities of COMMARFORRES/Commander Marine Forces North and the HTCs within the MCEN governance model.

(d) Ensure MCEN operations and defense is included within each HTC master plan and associated facility electronics systems engineering plans when not located aboard a DOD installation. Develop required support agreements for HTCs that are aboard DOD installations.

(e) Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

(f) Host and maintain regional MCEN service and security stacks required for the operation and defense of the MCEN.

(g) Provide MCEN Services, in accordance with C4-published MCEN Service model, to assigned Reserve and Operating Force Commanders.

(h) Provide tiered garrison and deployed MCEN customer support IAW with C4-published IT customer support model.

(i) Coordinate with MARCORSYSCOM and MARFORCYBER for the efficient implementation of MCEN IT Hardware and Software projects.

(j) Consolidate Reserve-wide MCEN operational service and customer support in the Reserve service support center.

(k) Host required regional and HTC level MCEN authentication and cyber security hardware in support of C4-published MCEN architecture.

(l) Provide MCEN delivery services to MARFORRES, MARFORNORTH, MSCs, and HTCs.

(m) Provide end-user support services for MCEN devices and applications.

(n) Process operational directives to operate and defend the MCEN.

(o) Enforce/comply with service level agreements.

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

(a) Retain command and control of Service Level Training Installations as described in the TECOM-MCICOM Memorandum of Agreement (MCICOM-TECOM letter 7050 dated June 17, 2014).

(b) Conduct coordination with COMMCICOM IAW assigned TECOM Technical/Logical AOS per enclosure (2).

(c) Submit OPREP-3 SIR for MCEN outages in accordance with PP&O guidance; assist PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCEN outages; and assist MARFORCYBER in assessing network risk assessments for MCEN outages that have an operational impact.

e. Coordinating Instructions

(1) Exercise command control as outlines in paragraph 5.a of this Bulletin.

(2) Identify critical assets and operational impact to inform risk assessments.

(3) Configuration Management. MARFORCYBER (Tier 2) and MCICOM, MARFORRES, HQMC Information Systems Management Branch (ARI), Marine Forces Europe Command (MARFOREUR), Marine Corps Recruiting Command (MCR), TECOM, C4, I&L, and other Tier 3 organizations as required support MARCORSYSCOM development of an Enterprise Change Control and Configuration Management Process. Once the Enterprise Change Control and Configuration Management Process is developed, approved and implemented, organizational MCEN Change Control and Configuration Management Processes will be aligned with MARCORSYSCOM-led enterprise process.

(4) Permanent changes to the MCEN require AO/(DDCIO (MC)) approval.

(5) Tier 2 and Tier 3 Headquarters will publish and maintain current OPORDs or Directives appropriate to specify tasks, reporting requirements, and other actions required by organizations/units within their assigned technical/logical AOS to ensure the operations and defense of the MCEN are sustained.

(6) Be prepared to transition tasks to DC I as directed.

4. Administration and Logistics

a. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The 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 will be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII will be in accordance with the Privacy Act of 1974, as amended (reference (n) and implemented per reference (o)).

b. Records Management. Records created as a result of this Bulletin shall be managed according to National Archives and Records Administration

approved dispositions per reference (p) to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium.

c. Cancellation Contingency. This Bulletin is cancelled one year from the date of publication or when incorporated into reference (a), whichever occurs first.

5. Command and Signal

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

(1) COMMARFORCYBER is responsible for the operations and defense of the MCEN and is the principal authority for MCEN permissions and authorities.

(2) Per reference (c), CDRUSCYBERCOM delegated DACO over all Marine Corps DODIN Components to COMMARFORCYBER to effectively implement orders from CDRUSCYBERCOM through CDRJFHQ-DODIN and to ensure the timely and efficient security, operation, and defense of the Marine Corps portion of the DODIN. Delegation of this authority allows COMMARFORCYBER to issue orders and directives to all Marine Corps components for directing the execution of DODIN Operations and DCO-IDM in order to compel unity of action to operate and defend the Marine Corps portion of the DODIN.

(3) DACO, as described above, does not restrict or limit Tier 3 authorities' ability to strengthen the security of the MCEN proactively and to take authorized defensive actions against ongoing or impending cyber exploitation or attacks. Immediate actions taken by Tier 3 organizations to defend against ongoing or impending exploitation or attacks will be positively communicated and coordinated at the earliest possible opportunity.

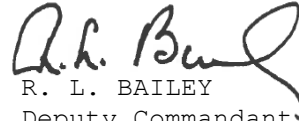
(4) Supporting/supported relationships are established between COMMARFORCYBER and all COMMARFORs; COMMCICOM; Commanding General, CG MCRC; COMMARCORSYSCOM; CG LOGCOM; Commanding General, Marine Corps Combat Development Command (CG MCCDC); Commanding General, Marine Corps National Capital Region Command (CG MCNCR); DMCS; all Deputy Commandants; Director C4; and DIRINT for the operations and defense of the MCEN. These Commanders, Deputy Commandants, and Directors will have periodic supporting/supported relationships with each other for the operations and defense of the MCEN. COMMARFORCYBER is the supported commander and retains primary responsibility and accountability for the security, operations, and defense of the MCEN. COMMARFORCYBER is the supporting commander for the execution of assigned missions of the Commanders, Deputy Commandants, and Directors.

(5) For the purpose of operations and defense of the MCEN, Commanding General Marine Corps Installations West and Commanding General Marine Corps Pacific are in direct support of COMMARFORPAC; Commanding General Marine Corps Installation East is in direct support of COMMARFORCOM; and DMCS (MITSC-HQMC/ARI) retains responsibility within the Pentagon and other designated areas, see enclosure (2). The direct support relationship is established to provide MARFOR commanders, in coordination with COMMARFORCYBER, the ability to set priorities and direct actions for the operations and defense of the MCEN.

(6) Per the Joint Information Environment Operations Concept of Operations, within the USSTRATCOM/USCYBERCOM AOR, a Technical/Logical AOS delineates the set of users, devices, and/or services within the

responsibility of an Operational Authority. Due to the unique nature of cyberspace operations, AOS assignments and responsibilities may transcend geographic boundaries and require cross-boundary coordination.

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



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

Distribution: PCN: 10203120000

Glossary

1. Cyberspace. A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Reference (r))
2. Cyberspace Operations. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (Reference (r))
3. Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (Reference (r))
4. Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM). Internal defensive measures are those DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, counterintelligence, law enforcement, and other military capabilities as required. (Reference (r))
5. Department of Defense Information Network Operations. Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (Reference (r))
6. Directive Authority for Cyberspace Operations (DACO). The authority to issue orders and directives directing the execution of DODIN operations and DCO-IDM in order to compel unity of action to secure, operate, and defend the DODIN. (References (b) and (c)).
7. Marine Corps Cyberspace Environment (MCCE). The Marine Corps' portion of the DODIN and all Marine Corps acquired, procured, or provisioned information systems and the associated collecting, processing, storing, managing, and transmission of information on all classified and non-classified networks, and components of the MCISR-E, including cyber discipline. Under this definition, the MCCE includes:
 - PORs
 - PIT (ICS, SCADA, weapons systems, etc.)
 - "Marine Corps portion" of TS networks
 - MCISRE
 - Other domains: .edu, .org, .com
 - MCEN (NIPR/SIPR)
 - Amphib networks
 - Tactical networks
8. Marine Corps Enterprise Network (MCEN). The MCEN is a segment of the MCCE, defined as the physical and logical information systems, PORs, applications, and networks that connect from the USMC Tier 2 boundary to the DISA Tier 1 Internet Access Point. The MCEN also includes active Marine Corps tactical networks and networks aboard amphibious shipping.
 - MCEN-N
 - MCEN-L (transitioning to MCEN-N/MCEN-S under Domain

- Consolidation & Elimination effort)
- MCEN-S
 - Data Centers (i.e. MCEITS)
 - Enterprise Services (i.e. email, domain controllers, Blackberry Enterprise Services, etc.)
 - Local Marine networks (i.e. MAGTF Regional Area Network (MRAN))
 - DMCEN/DSTB "extensions"

9. Technical/logical area of support (AOS). The AOS are assigned based on the logical/technical configuration of the MCEN and the placement of MAGTF IT Support Centers.

MCEN Technical/Logical Area of Support Assignments

1. DMCS, Commanders, and CG MCRC are responsible for directing actions necessary to sustain the operations and defense of the MCEN within their assigned technical/logical area of support. The AOS are assigned based on the logical/technical configuration of the MCEN and the placement of MAGTF IT Support Centers. The Technical/Logical AOS are complementary to the Supported/Supporting relationships depicted in enclosure (3). COMMARFORCYBER (Tier 2) will publish an OPORD specifying the required actions by Tier 3 headquarters organizations. The Tier 3 Headquarters specified below will publish appropriate OPORD's or Directives specifying the required actions by organizations assigned within their Technical/Logical Area of Support.
2. DMCS. CMC, ACMC, SMMC, Site-R, Henderson Hall, Marine Barracks Washington, Marine Corps IT Center Kansas City, TSO-Indianapolis, HQMC Naval Support Facility-Arlington, Target Site 2 Mechanicsburg, DC M&RA (SIPRNET only), DC PP&O, DC P&R, DC Aviation, DC I&L, HQMC Pentagon and Special Staff (C4, Intel Department, Commandants Counsel, Health Services, OLA, SJA, Environmental, Safety, Chaplain, Office of Marine Corps Communications, Marine Corps Communications, Marine Corps Motion Picture & TV Liaison Office, NYC Public Affairs, IGMC).
3. COMMARFORCOM. MARFORCOM HQ, II MEF, MCI East, Marine Corps Security Cooperation Group, Marine Corps Security Force Regiment, MCSF Blount Island, MCLB Albany, MCAS Beaufort, MCAS Cherry Point, MCB Camp Lejeune, MCAS New River, and MCRD Paris Island.
4. COMMARFORPAC. MARFORPAC HQ, I MEF, III MEF, MCIWest, MCIPAC, MCB Camp Pendleton, MCLB Barstow, MCAS Yuma, MCRD San Diego, MCAGCC, MCMWTC, Camp Mujuk, MCAS Futenma, MCAS Iwakuni, MCB Camp Butler, MCB Hawaii, Camp Fuji, MARFORK, and Marine Corps Activity Guam.
5. COMMARFOREUR/AF. MARFOREUR/AF HQ and all MARFORs within COMMARFOREUR/AF AOR.
6. COMMARCENT. MARFORCENT HQ and all MARFORs within COMMARFORCENT AOR.
7. COMMARFORRES/NORTH. MARFORRES HQ and MARFORRES/NORTH Forces.
8. CG MCNCRC. MCAF QUANTICO, CBIRF, MARFORCYBER, DC M&RA (NIPRNET only), DC CD&I, MCCDC, TECOM, TCOM, EDCOM, MARINE WARFIGHTING LAB, MCIOC, MCRC (NIPRNET only), MCESG, MCIA, CENTER for NAVAL ANALYSIS, and MARCORSYSKOM.
9. CG, MCRC. MCRC HQ (MARINE CORPS RECRUITING ENTERPRISE NETWORK (MCREN) ONLY), 1st MARINE CORPS DISTRICT (MCD) (MCREN ONLY), 4th MCD (MCREN ONLY), 6th MCD (MCREN ONLY), 8th MCD (MCREN only), 9th MCD (MCREN only), and 12th MCD (MCREN only).
10. CG TECOM. MCU.EDU network; other training and education networks listed outside the AOS.

Enclosure 3

MCEN Command and Control Diagram

Enclosure 3 is a Distribution Statement D: You may obtain a copy by contacting the sponsor:

HQMC PP&O PLI

POC: LtCol. McCuen, Patrick W. at Patrick.mccuen@usmc.mil
Mr. Harris, Russell D. at Russell.d.harris@usmc.mil

You may also find a copy on the MCAFEL & PLMS DVD set mailed out quarterly to US Government Agencies and their Contractors effective October 2017 timeframe. To obtain a copy of this DVD set, send your request to smb.hqmc.arde@usmc.mil, or subscribe to it in MCPDS under PCN #: 71000025200.