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

MCO 3100.4A
DC I (IMD)
25 Mar 2026

MARINE CORPS ORDER 3100.4A

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS CYBERSPACE OPERATIONS

Ref: See enclosure (1)

Encl: (1) References
(2) DCO-IDM and DOWIN Activities
(3) Cyberspace Fires in the MAGTF

Report Required: Operations Event/Incident Report (OPREP-3) Serious Incident Report (SIR) (Report Control Symbol EXEMPT), par. 4b(2)(d)

1. Situation. The Marine Corps depends on cyberspace to enable the successful execution of warfighting functions across the range of military operations and to fulfill Marine Corps business functions. To retain freedom of action within the information environment, the Marine Corps must develop and maintain robust capabilities to secure, operate, and defend the Marine Corps Cyberspace Environment (MCCE) as a part of the Marine Corps Information Environment Enterprise (MCIEE). Our networks and systems are central to our warfighting capability. Therefore, commanders across all echelons have a responsibility to secure and defend their portion of Marine Corps cyberspace. The Marine Corps executes cyberspace operations to perform warfighting functions including command and control, fires, force-protection, maneuver, intelligence, and information. These cyberspace operations are executed in concert with other Marine Corps operations, to identify, understand, disrupt, attack, protect against, and defeat a wide range of adversaries; while supporting, securing, and enabling friendly force capabilities, in accordance with references (a) through (ba). Cyberspace operations consist of offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of War information network (DOWIN) operations.

a. As Service Chief, the Commandant of the Marine Corps (CMC) is responsible for resourcing and operating the MCIEE and is therefore the owner of all elements of the MCCE. In September 2024, reference (au) identified the CMC as the United States Marine Corps (USMC) Sector Commander and established DOWIN Area of Operations (DAO) Marine

Corps with Marine Corps Forces Cyberspace Command (MARFORCYBER) as Commander DAO Marine Corps.

b. Through this order, CMC delineates roles, responsibilities, and relationships between Marine Corps organizations that conduct cyberspace operations or provide cyberspace capabilities to enable naval and joint combined arms in accordance with references (f) through (s). Additionally, the CMC sets service cyberspace priorities for action by Commander, U.S. Marine Corps Forces Cyberspace Command (COMMARFORCYBER). These priorities enable COMMARFORCYBER to execute DOWIN operations across the MCCE and as perform the duties of the Marine Corps Cybersecurity Service Provider (CSSP), see reference (ar). In this operational role, MARFORCYBER ensures the availability and security of cyberspace systems so that Fleet Marine Force mission requirements are satisfied.

c. The Marine Corps has several military occupational specialties (MOS), civilian cyberspace roles, and contractors who make up a workforce designed to operate, extend, secure, maintain, and sustain the MCCE as part of DOWIN operations. In accordance with reference (ao), this workforce requires training and resources as well as qualifications, certifications, and authorities to provide DOWIN services in support of our warfighters. DOWIN operators are required to comply with the standards and policies established by the Department of War Chief Information Officer (DoW CIO), the Deputy Commandant for Information (DC I), United States Cyber Command (USCYBERCOM), and MARFORCYBER to ensure the security and availability of systems, devices, and networks across various enclaves to provide quality service globally.

d. In addition to DOWIN operators, Marine Corps personnel who conduct DCO and OCO include military uniformed, civilian, and contractor work roles. In accordance with reference (ao), these military and civilian professionals require training, resources, qualifications, certifications, and authorities to successfully execute missions against adversaries in and through cyberspace. These professionals conduct combat operations with or in support of Fleet Marine Forces (FMF) and MARFORCYBER in accordance with applicable law, policy, and executive orders. These professionals are the community that will plan, conduct, integrate, and supervise DCO and OCO for Marine Corps forces.

e. This order establishes significant updates to roles, responsibilities, and authorities of key organizations. It should be read in its entirety.

2. Cancellation. MCO 3100.4.

3. Mission. This order promulgates policy, guidance, and organizational responsibilities for the conduct of cyberspace operations to provide access to MCCE resources, deliver desired effects on the enemy, and deny the same desired effects or access to

MCCE resources for adversaries. Execution of this order will be done in accordance with references (a) through (ba).

4. Execution.

a. Commander's Intent and Concept of Operations.

(1) Commander's Intent. Organize, man, train, and equip the Marine Corps to conduct cyberspace operations across echelons of command in the FMF, at Marine Forces component commands including MARFORCYBER, and at supporting establishment (SE) units. The end state is a professionalized Marine force that executes cyberspace operations in support of combatant command requirements across the Joint Force. These forces provide secure access to the MCCE, enable freedom of action across all warfighting domains, and deny the same to adversaries while achieving Marine Corps desired effects.

(2) Concept of Operations. The Marine Corps will:

(a) Organize, man, train, and equip, Marine Corps cyberspace operations forces and capabilities to support joint and naval service operations in accordance with references (t) through (z).

(b) Develop cyberspace operations tactics, techniques, and procedures (TTPs), at the unit level or in conjunction with other services and government agencies.

(c) Train and develop sufficient Marine Corps personnel to execute cyberspace operations per references (y) and (z).

(d) Acquire, provide, and maintain cyber equipment for use by Marine Forces in accordance with references (t) through (x).

(e) Educate and train Marine Corps leadership at all levels in cyberspace operational concepts, capabilities, limitations, employment, and support request procedures.

(f) Coordinate and synchronize DOWIN operations and DCO Internal Defensive Measures (DCO-IDM) across all Marine Corps organizations to ensure the protection and operation of the MCCE. This coordination and synchronization must enable local commanders to successfully accomplish unit missions and tasks assigned from combatant commands. In accordance with reference (au), cyberspace risk decisions regarding assets within Marine Corps sector areas of operation are made by COMMARFORCYBER while coordinating with affected Marine Corps organizations.

(g) Ensure cyberspace operations are properly resourced, planned, integrated, and sustained to meet military objectives throughout the competition continuum. This planning and execution process includes implementing procedures for command and control (C2)

and adhering to doctrine, organization, training, materiel, leadership and education, personnel, facilities, policy, and cost (DOTMLPF-PC). DCO and OCO must be coordinated and synchronized through a planning cell of cyberspace planners at tactical echelons of command. Authority to conduct OCO typically resides at the joint level. USMC service elements seeking to incorporate OCO into their scheme of maneuver should follow the processes explained in enclosure (3).

(h) Implement a process to manage and restrict access of MCCE users, system administrators, or network administrators who pose or create unacceptable risk to the MCCE, in accordance with references (aa) and (j).

(i) Establish, implement, and maintain an integrated DOWIN/MCCE risk mitigation decision framework and cyberspace mission alignment process that enables the efficient and responsive employment of MCCE resources. The processes described above must incorporate CMC and COMMARFORCYBER priorities and integrate DoW mission areas (MAs) and the governance process prescribed in references (aa) through (ad).

(j) Ensure Commanders and DOWIN workforce personnel conduct risk assessments to inform the prioritization of efforts of cybersecurity and response requirements.

b. Tasks.

(1) Deputy Commandant for Information (DC I). DC I develops and supervises plans, policies, and strategy for operating in the MCIEE. In support of cyberspace operations, DC I shall:

(a) General.

1. Advise the CMC on the development of the Marine Corps' position on cyberspace operational issues. Represent those positions that support FMF and the SE.

2. Serve as the Marine Corps representative and point of contact to the Office of the Secretary of War (OSW), Joint Staff, Services, and external agencies regarding Service cyberspace policy and strategy matters.

3. Represent Marine Corps equities in the development of naval, joint, interagency, and allied cyberspace operations policy.

4. Assign personnel to serve as members or observers on commissions, boards, advisory groups, and committees external to the Marine Corps that require Marine Corps representation on cyberspace policy matters.

5. Monitor and participate in liaison with OSW, Joint Staff, Services, external agencies, private industry, and academia

involving the exchange of information pursuant to improving cyberspace operations.

6. Participate in the Planning, Programming, Budgeting, Execution, and Assessments (PPBEA) process for appropriate Marine Corps systems that support cyberspace operations.

7. Inform each DC and other Marine Corps agencies/commands on DC I positions with respect to cyberspace operational capabilities, systems, planning, programming, and policy.

8. In accordance with references (y) and (z), sponsor 02XX, 06XX, 17XX, and 26XX occupational fields and Civilian Occupational Series 0331, 0335, 0391, 0854, 1550, 2210, 0132, and 0134, and civilian communities of interest (COIs). Ensure applicable tables of organization (T/O) are appropriately structured and staffed to facilitate cyberspace operations, including intelligence support, information network activities, and cybersecurity.

9. Advise Deputy Commandant for Training and Education (DC T&E) on required entry, intermediate, and advanced individual cyberspace operations training required through Service, joint, intelligence community (IC), and interagency schoolhouses.

10. Advocate for funding to support Marine Corps' cyberspace operational capability requirements.

11. Establish, coordinate, and maintain policy for Marine Corps cyberspace operations.

12. Direct coordination and federation of Marine Corps intelligence, counterintelligence, cryptologic, and security support to cyberspace operations.

13. Represent or designate a representative to national and defense intelligence enterprise-wide councils, boards, and decision forums that coordinate, synchronize, and de-conflict intelligence, counterintelligence, and security operations in support of cyberspace operations.

14. In coordination with MARFORCYBER, develop and maintain policies that detail authorized cyberspace activities and the consequences for violations of policy for all Marine personnel who conduct cyberspace operations.

15. Annually publish a training and certification Marine Corps Bulletin that identifies and codes cyberspace workforce skillsets from the DoW Cyberspace Workforce Framework (DCWF) to Marine Corps training and readiness (T&R) standards. This bulletin will provide guidance to Marine units looking for training resources and paths to meet certification requirements.

(b) DOWIN Operations.

1. Chair MCIEE Board, DC I Advisory groups, the Network Governance Board (NGB), and supporting working groups for DOWIN operations.

2. Develop strategies, plans, policies, and programs to provide a unified MCCE that provides commanders and staffs the ability to conduct operations and business activities through shared, secured, reliable information technology environments in accordance with references (d) through (f), while enabling secure, critical connection to the larger global information environment.

3. As Department of the Navy Deputy Chief Information Officer (DON Deputy CIO) (Marine Corps), provide information technology (IT) capital planning and portfolio management in accordance with references (ae) and (al); develop and manage an IT architecture and workforce; and provide leadership and governance of IT activities for the Marine Corps in accordance with references (k) and (s).

4. As the authorizing official for the MCCE, in coordination with MARFORCYBER, 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 the CIO and the Senior Information Security Officer.

5. In coordination with the Marine Corps Systems Command (MARCORSYSCOM) and MARFORCYBER, adjudicate requests for authorization to operate (ATO) and authorization to connect (ATC).

6. In coordination with MARFORCYBER, utilize the Marine Corps Assessment and Authorization Process (MCAAP) to identify risks associated with the employment of systems. Formally approve or disapprove systems for operation and continuously evaluate operational systems. When appropriate, revoke operational approval if unacceptable security risk exists.

7. Conduct planning for a resilient DOWIN architecture that enables the remediation, mitigation, and assurance of critical Command, Control, Communications, and Computers (C4) systems, assets, and infrastructure so that a minimum essential level of C2 functions can be sustained.

8. Assist MARFORCYBER in assessing network risks that have an impact on Marine Corps operations and advise/assist Deputy Commandant Plans, Policies, and Operations (DC PP&O) in developing guidance to Marine Corps commanders in operational risk assessments.

9. Establish and maintain the Service-level policy for DOWIN incident reporting, handling, and management in accordance with reference (aa).

10. In accordance with reference (j), exercise oversight authority regarding the implementation and maintenance of the Cybersecurity Program.

11. Provide subject matter expertise to the Inspector General of the Marine Corps (IGMC) and maintain the functional area checklist for cybersecurity management, one of the CMC directed critical or required evaluation (CoRE) functional areas.

12. When requested, designate qualified and trained personnel to serve as temporary assistant Inspectors General (TAIG) in support of the IGMC.

13. Coordinate with DC PP&O, DC Deputy Commandant Combat Development and Integration (CD&I), DC Installations and Logistics (I&L), MARCORSYSCOM, and MARFORs for the assessment of Marine Corps critical capabilities and infrastructure, in accordance with references (w), (x), (ae) and (af) for cybersecurity and assured C2 services. These assets may be defended as warranted in coordination with DC PP&O and MARFORCYBER.

14. coordination with MARFORCYBER, review and assess all IT and software procurement requests as the Marine Corps information technology expenditure approval authority in accordance with reference (k) and provide IT resource audit information to Deputy Commandant Programs and Resources (DC P&R) as required.

15. In coordination with DC CD&I, (I&L), (P&R), Aviation (AVN), MARCORSYSCOM, and MARFORs, ensure appropriate validation, acquisition expenditures, integration, maintenance, and allocation of critical C4 systems, assets, and infrastructure capabilities and resources sufficient to meet MARFORs, FMF, and installation commanders' DOWIN operations requirements in accordance with reference (k).

(c) DCO/OCO

1. Chair an Operational Advisory Group (OAG) and appropriate working groups representing DCO/OCO equities.

2. In coordination with COMMARFORCYBER and DC T&E, develop Service-level training and certification policies in accordance with reference (ak) and (aq) for cyberspace operations forces (COF) and Service-retained DCO/OCO forces and ensure they are aligned to Commander to United States Cyber Command (CDRUSCYBERCOM) standards to include individual and unit level training, as outlined in reference (aj).

3. Advise Deputy Commandant Combat Development & Integration (DC CD&I) on Marine Corps equities and requirements to train cyberspace warfare forces on a reliable and sustainable cyberspace range, that include COF and Service-retained forces. In coordination with DC PP&O and MARFORCYBER, develop mission rehearsal guidance and support the development of rehearsal capabilities for use by cyberspace warfare forces.

4. Represent Marine Corps equities on the Cryptologic Training Council and USCYBERCOM training boards as appropriate.

(2) Deputy Commandant for Plans, Policies and Operations (PP&O). PP&O is the operations deputy for the Commandant on all Joint Chiefs of Staff (JCS) matters and is responsible for coordinating the development and execution of service plans and policies related to the structure, deployment, and employment of Marine Corps forces in general. In support of CO, PP&O shall:

(a) Provide representation to the appropriate DC I OAGs and working groups.

(b) Ensure that appropriate mission assurance and critical infrastructure mechanisms for cyberspace operations are in place in accordance with reference (ae).

(c) In coordination with DC I, MARFORs, FMF, SEs, and Marine Corps installation commanders, oversee, manage, and conduct the periodic identification, prioritization, and assessment of cyberspace assets and infrastructure critical to the execution of Marine Corps missions, capabilities, core functions, and to determine and protect key terrain in cyberspace in accordance with references (ae) through (ag).

(d) Publish Operations Event/Incident Report Serious Incident Report (OPREP-3 SIR) reporting thresholds for MCCE outages via CMC commander’s critical information requirements.

(e) In coordination with DC I, COMMARFORCYBER, MARFORs, and the supporting establishment (SE), prioritize the allocation of critical cyberspace operations resources and capabilities to support/enable Service Title 10 responsibilities. Coordinate with MARFORs, FMF, Marine Expeditionary Forces (MEFs), and SE commanders in addition to DC I and MARFORCYBER, to assess and prioritize potential ongoing risks and appropriate office of primary responsibility (OPR) to risk events.

(f) Serve as primary intermediary between OSD, the Joint Staff, and HQMC per reference (ap).

(3) Deputy Commandant Combat Development and Integration (CD&I) and Commanding General, Marine Corps Combat Development Command (MCCDC). CD&I designs and develops a modernized Marine Corps to

campaign in an evolving threat environment. MCCDC develops concepts, plans, doctrine, training and equipment for the 21st century Marine Corps. Together, in support of cyberspace operations, CD&I and MCCDC shall:

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

(b) Conduct all combat development activities for the execution of cyberspace operations within the context of the Marine Corps capability-based assessment (CBA) process in accordance with references (w), (x), and (y). Identify and validate cyberspace operations capability requirements and establish necessary changes to DOTMLPF in accordance with references (t) through (y).

(c) Provide representation to the appropriate information related OAGs, the NGB, and applicable working groups.

(d) Coordinate with DC I on the assignment of personnel to serve as members or observers on commissions, boards, advisory groups, or committees external to the Marine Corps that require Marine Corps representation on cyberspace operations capability requirements or integration matters.

(e) Establish and maintain cyberspace operations, assured C2, and CSSP concepts to facilitate the development of requirements, doctrine, and other force development processes.

(f) Ensure the unique personnel, training, authorities, capabilities, and operational requirements for cyberspace operations, C4 communications, and CSSP are considered and whenever possible, integrated as a combined arms capability.

(g) Conduct mission area analyses for all assigned cyberspace operation mission areas and ensure relevant Marine Corps cyberspace capabilities are included in appropriate simulations, models, and exercises.

(h) Collaborate with DC I, Deputy Commandant Installations and Logistics (DC I&L), and MARCORSYSCOM to inform cyberspace operations related acquisition priorities and the development of capabilities.

(i) As a subject matter expert in Marine Corps capabilities, inform and advise on operational impacts to MARFORCYBER when notified of cyber threats and risks against Marine Corps capabilities.

(j) Execute capability based analysis approach on behalf of the CSSP to identify their capability requirements and funding needs.

(k) Integrate cyberspace operations into service-level wargames and experimentation.

(4) Deputy Commandant, Installations and Logistics (I&L). I&L shapes logistics plans and policies to sustain excellence in warfighting. In support of cyberspace operations, I&L shall:

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

(b) Coordinate with Headquarters Marine Corps departments, Naval Facilities Engineering Command, and United States Army Corps of Engineers on DOWIN operations requirements and technical standards for installations and facilities. Inform DC I when new requirements emerge and the status of enduring cyberspace operations requirements.

(c) Coordinate the assignment of personnel to serve as members or observers on commissions, boards, advisory groups, and committees that require Marine Corps I&L representation for cyberspace operations fiscal management, program management, installations and logistics management requirements.

(d) Through the Commander, Marine Corps Installations Command (COMMCICOM), coordinate assigned Marine Corps and maintenance activities in support of cyberspace operations aboard Marine Corps bases, posts, and stations.

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

(f) Provide representation to the appropriate DC I OAGs, sub-working groups, the NGB, and applicable working groups.

(g) In coordination with DC I, DC CD&I, DC PP&O, MARFORs, FMFs, and Marine Corps installation commanders, coordinate and report findings on periodic identification, prioritization, and assessment of cyberspace assets; and infrastructure critical to the execution of Marine Corps missions, capabilities, and core functions in accordance with references (ae) through (ag).

(h) In coordination with MARFORCYBER, ensure all installation commanders' tables of organization are appropriately structured and staffed to facilitate installation communication grid, services, and required DOWIN operations.

(i) In coordination with MARFORCYBER, conduct risk assessments for MCCE outages to determine the operational impact.

(5) Deputy Commandant for Training and Education (DC T&E). CG TECOM leads the Marine Corps training and education continuum from individual entry-level training, professional military education and continuous professional development, through unit, collective, and service-level training to produce warfighters. In support of cyberspace operations, DC T&E shall:

(a) Establish and maintain doctrine pertaining to cyberspace operations.

(b) Ensure implementation of published doctrine within applicable Marine Corps training and education programs.

(c) In coordination with DC I, DC CD&I, COMMARFORCYBER, and DC M&RA develop and maintain appropriate MOS descriptions and requirements, T&R events, Training Input Plan (TIP), and student quota management requirements in support of entry-level training (ELT) and career progression cyberspace operations training.

(d) Ensure the fundamentals of cyberspace operations are integrated across common skills, MOS training, and professional military education curricula, where appropriate, to reinforce the fundamentals of network and cyber defense and multi-domain warfighting.

(e) Coordinate with joint and other-service schools to ensure cyberspace operations curriculum represents Marine Corps equities (i.e. USMC integration into joint cyberspace operations, including multi-domain warfare, theater-specific operational requirements, and cyberspace systems employment, etc.).

(f) Integrate cyberspace operations into Service-level training exercises.

(g) Provide representation to the appropriate DC I OAGs, sub working groups, the NGB, and applicable working groups.

(h) Develop and publish cyberspace operations capability requirements, studies, and TTPs in accordance with references (t) through (y).

(6) Commander, Marine Corps Forces Cyberspace Command (MARFORCYBER). MARFORCYBER conducts full spectrum cyberspace operations. In support of cyberspace operations MARFORCYBER shall:

(a) General

1. Serve as the Marine Corps Service component commander to USCYBERCOM, advising on the proper employment and support of Marine Corps Forces, to include support to maritime and FMF operations.

2. Serve as DAO Commander for DAO Marine Corps with authority to synchronize, coordinate, and direct cyberspace operations.

3. In coordination with DON Principle Cyber Advisor (PCA), serve as an advisor to the CMC to employ forces for the conduct of cyberspace operations. Provide Marine Corps-wide guidance, direction, awareness, expertise and, when required, deploy tactical elements to support DOWIN operations, cybersecurity, planning, and DCO/OCO activities and effects.

4. Exercise Directive Authority for Cyberspace Operations (DACO) in accordance with reference (au) over all Marine Corps organizations and components that execute DOWIN operations, DCO-IDM, cybersecurity actions, or cyberspace defense actions to achieve unity of effort for protection of the MCCE.

5. Develop program and budget requests to comply with USCYBERCOM guidance on warfighting requirements and priorities.

6. When directed, receive OPCON of cyberspace forces from the Service to secure, operate and defend the MCCE.

7. Advise DC I, DC CD&I, and DC T&E on requirements for individual and unit level training events and Mission Essential Task List (METL) development.

8. Identify gaps in the tables of equipment and tables of organization of units that conduct cyberspace operations.

9. Establish, implement, and maintain an integrated cyberspace risk mitigation decision framework and cyberspace mission alignment process that enables the efficient and responsive employment of Service cyberspace resources. This process must incorporate CMC and CDRUSCYBERCOM priorities.

10. In coordination with DC I, assist in the development and maintenance of policies that detail authorized cyberspace activities, behaviors, and personal/unit conduct during actions within cyberspace; and the consequences for violations for all Marine Corps users and privileged users who conduct DOWIN Operations, and COF who conduct DCO and OCO.

11. In coordination with DC PP&O and DC I, release and maintain operations order(s) (OPORDs) to identify OPRs for MCCE areas, and publish battlespace areas, assets, and responsibilities to MARFORs, MEFs, or other commanders. These orders will specify required actions in response to any MCCE event and will specify the reporting requirements for progress and status of compliance and will include roles and responsibilities for DOWIN and DCO forces to include determining and protecting key terrain in cyberspace.

12. In coordination with CDRUSCYBERCOM and Commander Department of War Cyber Defense Command (DCDC), conduct planning, direction, coordination, execution, and oversight of DOWIN operations within the Marine Corps portions of the DOWIN and of DCO/OCO within approved areas of operation (AO).

13. In coordination with MCICOM, support the strategic development and integration of installation communications.

14. In support of CDRUSCYBERCOM, assist in the conduct of Commanders Operational Risk Assessments (CORA) and provide guidance on the reporting of classified risk assessments based on MARFORCYBER reporting requirements and MCCE operational risk assessments, in accordance with reference (g).

15. Man, train and equip assigned Marine Corps cyberspace forces as delegated or designated by the Commandant of the Marine Corps.

16. Plan and execute cyberspace operation-related security cooperation activities in support of USCYBERCOM and adjacent MARFORs in coordination with DC PP&O, in accordance with reference (az).

17. In coordination with MARCORSYSCOM and other program management offices, transition capabilities from DC CD&I on to the MCCE.

18. When directed, serve as a joint task force, or other similar joint headquarters.

(b) DOWIN Operations.

1. On behalf of CDRUSCYBERCOM and the CMC, plan, coordinate, and direct DOWIN operations in support of the Marine Corps to secure and operate the MCCE. As the Commander DAO Marine Corps, conduct C2 of the MCEN and all Marine Corps DoW cyberspace to include owned and leased information capabilities and networks.

2. Draft, submit for comment, assign and publish MCCE battlespace areas, cyberspace areas of operation (CyAO), assets, and responsibilities to MARFORs, MEFs, or and other commanders as required to enable operations, manage risk, and maintain situational awareness of MCCE status in order to take appropriate action in any MCCE event.

3. Advise DC I and MARCORSYSCOM on acceptance or rejection of cyber risk to the MCCE as part of the DC I managed MCAAP. Assume or mitigate resulting risk in support of ongoing cyberspace operations in coordination with operational commanders and battlespace owners to generate informed understanding of operational impacts. To the greatest extent possible, coordinate and consult with affected

commanders prior to taking action on systems when risk is found to be unacceptable.

4. Coordinate with DC I and mission owners on the acceptance or rejection of risk to the MCCE for all changes, configuration management, and technology pilot programs, in accordance with reference (j).

5. Assist impacted commands and DC PP&O in the assessment of institutional readiness and mission risk assessments resulting from MCCE outages. Coordinate, consolidate, and report risk assessments to DC PP&O for MCCE outages that have an operational impact.

6. Develop, staff for comment, and manage processes to block, remove, or disconnect MCCE access (either temporary or permanently) for individuals or units who pose or potentially pose an unacceptable risk to the MCCE. These may include users, system administrators, and network administrators whose actions incur risk to operations or systems. Coordinate with appropriate commanders for mitigation and restoration of access.

7. In coordination with affected commands, assess institutional readiness and risk to mission during MCCE outages, and provide DC PP&O consolidated reports for MCCE outages that cause operational impacts.

8. In coordination with DC CD&I and COMMARCORSYSCOM, establish the cyberspace incident reporting, handling, and management system for the Marine Corps, in accordance with DC I policy and reference (aa).

9. Provide representation to the appropriate DC I OAGs and NGB.

(c) CSSP

1. Provide full CSSP services for the MCCE in accordance with references (h) and (j).

2. Coordinate CSSP efforts across the Marine Corps for provisioning of CSSP services.

3. Issue OPORDs based on Commander DCDC direction or CSSP compliance.

4. Issue CSSP coverage agreements as required.

(d) DCO/OCO

1. When directed, conduct DCO and OCO in support of assigned missions.

2. Plan, prepare, and, when authorized and directed, execute cyberspace operations, intelligence, surveillance, and reconnaissance (ISR) in cyberspace, and cyberspace effects enabling activities (CE2A), deconflicting these operations with USCYBERCOM.

3. Identify operational requirements for organizing, training, and equipping Marine Corps forces in support of USCYBERCOM and to enable naval and joint operations.

4. Develop a plan to train and certify Cyber Mission Force (CMF) teams to meet the standards established by USCYBERCOM, as outlined in reference (aj).

5. In coordination with DC I and DC T&E, develop a qualification and certification process for Marine Corps Service-retained DCO and OCO cyberspace forces that meet USCYBERCOM standards, as outlined in reference (aj), (ao), and (aq).

6. Provide representation to the appropriate DC I OAGs.

7. Coordinate with adjacent Marine Forces component commands, MEFs, and their assigned cyberspace operational planners in support of Joint and Marine Corps operations.

8. Identify to DC I, DC CD&I, and the Joint Cyberspace Training Environment (JCTE) Executive Agent (EA) any training shortfalls or enhancement required by USCYBERCOM assigned and Service-retained COF to support Marine Corps and Joint Force missions.

9. Develop and maintain control programs that develop, test, coordinate, and validate all tools (to include scripts) and malware analysis capabilities installed or employed within the MCCE.

10. Coordinate Service-level DOWIN operations and DCO forces to assess, validate, and de-conflict cyberspace operations at the tactical and enterprise levels.

11. Identify long-term requirements through the DC I OAGs and requirements process in accordance with references (w) and (x).

12. Maintain situational awareness of all Marine Corps Forces that are conducting DCO and OCO.

13. Develop DCO-IDM maneuver control measures, effects coordination measures, and other planning, coordination, de-confliction, and reporting measures to enable unity of effort, visibility, technical supervision, and use of qualified and certified personnel for operations across the MCCE.

(7) Commander, Marine Corps Installations Command, (MCICOM). MCICOM is the single authority for all Marine Corps Installations matters. In support of cyberspace operations, MCICOM shall:

(a) In coordination with MARFORCYBER, conduct installations infrastructure and facilities inspections supporting DOWIN operations; to include but not limited to supporting the strategic development and integration of installation telecommunications (e.g. broadband/5G capabilities, IT infrastructure, and the cybersecurity for facility-related control systems).

(b) Inform MARFORCYBER on gaps in Marine Corps Installations tables of equipment and tables of organization employed in DOWIN Operations.

(c) In coordination with DC I, DC CD&I, MARFORCYBER, and MARCORSYSCOM, ensure all Programs of Record (POR) deployed and managed IT systems can maintain compliance with information assurance vulnerability alerts (IAVAs) and bulletins (IAVBs), task orders (TASKORDs), OPORDs, operational directives (OPDIRs), operational advisories (OPADVs), and Security Technical Implementation Guide (STIG) compliance, while building the same 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 and avoid exposing the MCCE to vulnerabilities.

(d) Plan, program, and conduct installations communications and IT inspections supporting cyberspace operations.

(e) Comply with cyberspace security related directions from MARFORCYBER as the USMC CSSP, as per references (aa) and (as).

(8) Commander, Marine Corps Systems Command (MARCORSYSCOM). MARCORSYSCOM is the acquisition command of the Marine Corps. They exercise contracting and technical authority for all Marine Corps ground weapon and information technology programs. In support of cyberspace operations, MARCORSYSCOM shall:

(a) Conduct research, development, and acquisition activities to satisfy requirements validated by the Marine Requirements Oversight Council (MROC) for cyberspace operational capabilities.

(b) In coordination with DC I, identify, research, and evaluate potentially useful new technologies and advise DC CD&I and MARFORCYBER of new or improved cyberspace operational capabilities that may be achievable through the development, enhancement, and exploitation of those technologies.

(c) Provide technical support to CD&I for assessing cyberspace operational Universal Need Statements (UNS) through the

Urgent Needs Process and the development of capability requirements documents.

(d) Provide representation to the DC I OAGs and the NGB.

(e) In accordance with reference (v), provide technical authority (TA), engineering, configuration management, and lifecycle support for cyberspace operational equipment and services.

(f) Ensure program of records deployed and managed IT systems can maintain IAVAs, IAVBs, TASKORDs, OPORDs, OPDIRs, OPADVs, and STIG compliance, building requirements into all awarded deployment and support contracts. Ensure systems comply with continuous monitoring and scanning requirements of reference (aa), while ensuring compatibility with CSSP security information and event management (SIEM), security orchestration, automation, and response (SOAR), and event management technologies. Ensure timely upgrades and refresh of IT systems to prevent them from reaching end-of-life or end-of-service while on the MCCE and avoid exposing the MCCE to vulnerabilities.

(g) Assist MARFORCYBER with risk assessments for MCCE outages that have an operational impact.

(h) Establish and maintain program of record (POR) assessment and authorization (A&A) packages to ensure that accurate information is available to assist in CSSP-related activities.

(i) Implement a rapid acquisitions process to support cyberspace operations equipment and applications resourcing to meet operational requirements and risk mitigation needs.

(j) Comply with MARFORCYBER on CSSP related functions, as per reference (aa).

(9) DCs, HQMC Agencies, FMF, COMMARFORs, and MEF CGs shall:

(a) General

1. Ensure local commanders understand and execute their responsibility to provide MCCE cybersecurity by adhering to guidance and operational orders issued by MARFORCYBER in command of DAO Marine Corps.

2. Incorporate cyberspace operations into training, exercises, wargames, experiments, and operation plans (OPLANs).

3. Establish, develop, and maintain a prioritized list of key terrain in cyberspace for use by defensive cyber operations planning.

4. When directed, task local cyberspace forces to provide direct support to DAO Marine Corps, COMMARFORCYBER, to secure, operate and defend the MCCE.

5. Integrate realistic scenarios for operating under denied, disconnected, intermittent, low bandwidth, and high latency (D-DILL) conditions in existing exercise programs and develop primary, alternate, contingency and emergency (PACE) Plan and continuity of operations plan (COOP).

6. In coordination with DC PP&O, DC I, DC I&L and COMMARFORCYBER conduct periodic risk assessments and report operational impact that identify, prioritize, and assess cyber-connected assets and infrastructure critical to Marine Corps mission essential functions and capabilities in accordance with references (ae) through (ag).

7. Comply with current OPORDs and directives appropriate to specific cyberspace operations tasks, reporting requirements, and other actions required by organizations/units within assigned MCCE battlespace.

8. Support the capability-based assessment process, urgent needs process, doctrine development, policy development, total force structure process, and Joint Capabilities Integration and Development System (JCIDS) in accordance with references (w) and (x).

9. Coordinate cyberspace operations with MARFORCYBER to ensure unity of effort across the cyberspace domain.

10. Enforce the cyberspace policies that detail authorized cyberspace activities and behaviors. Enforce consequences for violations for all Marine Corps users and privileged users who conduct DOWIN operations and cyberspace warfare operators who conduct DCO and OCO.

(b) DOWIN Operations.

1. Submit OPREP-3 SIR for MCCE outages in accordance with PP&O guidance.

2. In coordination with PP&O and MARFORCYBER, assess institutional readiness and risk to mission during MCCE outages that cause a significant impact to Marine Corps operations.

3. Comply with DOWIN mission tasks as well as routine maintenance and service support for assets on Marine Corps networks and standalone systems. Commanders who directly manage these assets will comply and report compliance in accordance with COMMARFORCYBER operational orders.

4. Implement all MCCE assets to the standards identified in the current risk management framework in accordance with DC I standing policy.

5. Comply with the DOWIN incident handling, reporting, and management system as established by COMMARFORCYBER and in accordance with reference (aa).

6. Provide representation to the DC I OAGs and the NGB.

7. Process OPDIRs in support of assigned missions to operate and secure the MCCE. Specific battlespace will be assigned and managed by COMMARFORCYBER.

(c) CSSP

1. Comply with MARFORCYBER on CSSP functions in accordance with reference (aa).

2. Obtain and maintain mandatory CSSP-related system accounts.

3. Update and maintain assessment and authorization (A&A) packages to ensure that accurate information is available to assist in CSSP-related activities.

(d) DCO/OCO

1. Identify gaps in capability to DC CD&I for resolution.

2. Establish and maintain staff expertise capable of planning and, when directed, exercising C2 of DCO and OCO. Ensure readily available assigned points of contact for coordination of DCO and OCO planning and integration for protection and fires in cyberspace.

3. Employ assigned DCO forces or capabilities within the authorities delegated by COMMARFORCYBER to ensure unity of effort and de-confliction in defense of assigned Marine Corps networks, weapon systems, and critical infrastructure.

4. Plan, coordinate, and prioritize CE2A and ISR in cyberspace for target development and information environment running estimates.

5. Receive and process requests for OCO effects from subordinate forces and assist in routing of OCO support requests through the operational chain of command; including the Geographical Combatant Command’s (GCC) Joint Cyber Center (JCC) and cyberspace

Operations Integrated Planning Element (CO-IPE), for staffing and execution by USCYBERCOM.

6. In accordance with references (j, av, aw, ax), comply with Cyber Incident Response actions, DCO-IDM maneuver control, coordination, and other reporting, planning, and de-confliction measures as delineated by MARFORCYBER to enable unity of effort across the MCCE.

7. Ensure only qualified and certified personnel plan, supervise, and execute DCO/OCO tasks, using a certification tracking tool such as Total Workforce Management Tool (TWMS) or Joint Cyber Command and Control (JCC2).

8. Provide representation to the appropriate DC I OAGs.

5. Administration and Logistics.

a. Records Management. Records created as a result of this Order shall be managed according to National Archives and Records Administration (NARA)-approved dispositions in reference (ai), 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%20Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to reference (am), for Marine Corps records management policy and procedures.

b. 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 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 [reference (an)] and implemented per references (ah) and (ba).

6. Command and Signal.

a. Command.

(1) The DoW relies on a secure and reliable cyberspace environment that protects fundamental freedoms, privacy, and the free flow of information. The United States military's ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoW missions. Through MCCE

modernization, force structure will be aligned to global DOWIN operations and DCO constructs. Enterprise, regional, tactical, cloud, and data initiatives will be synchronized. Operational C2 boundaries will be established, including geographic areas of operation, battlespace, and cyberspace area of operations assignment for all network segments. Informed by FMF operational needs and cyberspace capabilities, MARFORCYBER will draft, staff for comment, publish, assign areas of responsibility, and continue to refine DAO Marine Corps.

(2) This Order is applicable to the Marine Corps Total Force.

b. Signal.

(1) MARFORCYBER will issue orders and directives for cyberspace operations in coordination with PP&O, as follows:

(a) General Administration (GENADMIN). GENADMINs are used by MARFORCYBER to inform the Marine Corps of incoming changes or requirements in relation to cyberspace operations.

(b) Task Order (TASKORD). TASKORDs are used by MARFORCYBER to directly task Marine Corps units to ensure the integrity, confidentiality, and availability of the MCCE, enabling MARFORCYBER to secure, defend, and operate the MCCE.

(c) Operations Order (OPORD). OPORDs are used by MARFORCYBER to directly task Marine Corps units for a specific cyberspace operation.

(d) Operational Directives (OPDIRs) and Operational Advisories (OPADVs) are released by MCCOG on behalf of MARFORCYBER. OPDIRs are derived from TASKORDs, Fragmentary Orders (FRAGOs), or IAVAs and require compliance across the total force.

(e) Planning Orders (PLANORD). MARFORCYBER PLANORDs are released to direct Marine Corps units to begin planning for a cyberspace operation.

(2) All commands will coordinate DCO-IDM Concept of Operations (CONOPS) with MARFORCYBER for validation and support when conducting operations.

(3) Enclosure (2) provides clarity to the comparison of DCO and Cybersecurity tasks.

(4) Threat and Vulnerability Reporting. DC I and MARFORCYBER will develop a reporting scheme and MARFORCYBER will release an OPORD that identifies OPRs for reporting compliance and status of areas to include, but not limited to, the list below. The assigned OPR will be responsible to MARFORCYBER for identifying, processing, understanding, implementing, and responding to tasks issued by MARFORCYBER.

(a) Functional Area Managers (FAMs).

(b) USMC-wide, non-program of record applications.

(c) DC controlled programs of record.

(d) Tactical networks.

(e) Locally procured services.

(f) Facilities related control systems (FRCS).

(g) Installation communication, including base, post, and station networks.

(h) Supply chain.

(i) NDAA 2016 §1647 systems status and compliance.

(j) MARCORSYSCOM and DC Aviation POR weapon systems.

(k) MARCORSYSCOM and DC Aviation POR IT systems.

(5) This Order is effective the date signed.

J. A. MATOS III
Deputy Commandant for Information

DISTRIBUTION: PCN 10255329000

TABLE OF CONTENTS

References

(a) JP 3-12, Cyberspace Operations, 19 December 2022
(b) MCIP 3-32Ei, Marine Corps Cyberspace Operations, 6 October 2014
(c) Marine Corps Information Enterprise Strategy, 14 December 2010
(d) DoD Strategy for Operations in the Information Environment, July 2023
(e) DoD Cyber Strategy, 12 September 2023
(f) Marine Corps Strategy for Assured Command and Control, March 2017
(g) DoD Instruction 8500.01, Cybersecurity,7 October 2019
(h) DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations,31 May 2023
(i) DoD Directive 8000.01, Management of The Department of Defense Information Enterprise (DoD IE), 27 July 2017
(j) MCO 5239.2B, Marine Corps Cybersecurity, 5 November 2015
(k) MCO 5400.52, DON Deputy CIO Marine Corps Roles and Responsibilities, 5 January 2010
(l) MCO 5400.54, MCICOM Roles and Responsibilities, 19 April 2013
(m) National Security Presidential Memorandum-13 (NSPM-13), 15 August 2018
(n) National Security Presidential Memorandum-21 (NSPM-21), 27 September 2019
(o) CJCS EXORD: Implement Updated Cyberspace Operations Command and Control (C2) Framework, 22 September 2017 S/REL FVEY
(p) CJCS EXORD: Mod 001 to Implement Updated Cyberspace Operations Command and Control (C2) Framework, 27 December 2018 S/REL FVEY
(q) USCYBERCOM OPORD 16-0139: Implementation of Updated Cyberspace Operations Command and Control Framework Delegation of Directive Authority for Cyberspace Operations, 6 September 2016 U/FOUO
(r) USCYBERCOM Cyber Concept of Operation and Employment, 22 July 2014 S/REL FVEY
(s) SECNAVINST 3052.2, Cyberspace Policy and Administration within the DON, 6 March 2009
(t) DoD Instruction 5000.02, Operation of the Adaptive Acquisition Framework, 8 June 2022

(u) SECNAVINST 5000.2G, SECNAV Instruction 5000.2G, DON Implementation of the Defense Acquisition System and Adaptive Acquisition Framework, 8 April 2022

(v) SECNAVINST 5400.15D, DON Research and Development, Acquisition, Associated Life-Cycle Management, and Sustainment Responsibilities and Accountability, 19 January 2021

(w) MCO 3900.20, Marine Corps Capabilities Based Assessment, 27 September 2016

(x) MCO 3900.17, Marine Corps Urgent Needs Process (UNP) and the Urgent Universal Need Statement (Urgent UNS), 17 October 2008

(y) MCO 5311.1E, Total Force Structure Process, 18 November 2015

(z) NAVMC 1200.1K, Military Occupational Specialties Manual, 7 February 2024

(aa) CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012

(ab) USCYBERCOM TASKORD 14-0308 (FRAGORD 01), Joint Enterprise Risk Assessment Model (JERAM), 20 January 2016 S/REL FVEY

(ac) USCYBERCOM DODIN Risk Assessment Methodology (RAM) 2.1, July 2019

(ad) DoDI 8510.01, Risk Management Framework for DoD Systems, 19 July 2022

(ae) PPD-21, Critical Infrastructure Security and Resilience, 12 February 2013

(af) MCO 3501.36B, Marine Corps Critical Infrastructure Program, 12 February 2021

(ag) MCO 3030.1A, Marine Corps Continuity of Operations (COOP) Program, 14 August 2020

(ah) SECNAVINST 5211.5F, DON Privacy Program, 20 May 2019

(ai) SECNAV M-5210.1 CH-1, DON Records Management Manual, September 2019

(aj) Cyber Mission Force Training and Readiness Manual v4, 17 July 2025

(ak) MCO P3500.72A, Marine Corps Ground Training and Readiness (T&R) Program,
18 April 2005

(al) MCO 5230.21, Information Technology Portfolio Management, 3 October 2012

(am) MCO 5210.11F, Marine Corps Records Management Program, 7 April 2015

(an) 5 U.S.C. 552a, Records maintained on individuals as amended 2 October 2024

(ao) DoDD 8140.01, Cyberspace Workforce Management, 5 October 2020

(ap) CMC Guidance to Deputy Commandant for Plans, Policies, and Operations, 2 August 2024

(aq) DoDM 8140.03, Cyberspace Workforce Qualification and Management Program,
15 February 2023

(ar) COMMARFORCYBER CSSP Designation Letter, 1 Feb 2017 U/FOUO

(as) ECSM 001 Cyber Incident Response V3.0 20 Feb 2025

(at) MCBUL 11120, Installation Communications, published annually.

(au) USCC EXORD 24-0091, DODIN Command Operational Framework (DCOF) 17 September 2024

(av) SECNAVINST 5239.19A, Department of the Navy Computer Network Incident Response and Reporting Requirements, 04 September 2019

(aw) SECNAVINST 5430.107A, Mission and Functions of the Naval Criminal Investigative Service, 19 June 2019

(ax) SECNAVINST 5510.36B, Department of the Navy (DON) Information Security Program (ISP) Instruction, 12 July 2019

(ay) CYBERSPACE WARFARE PUBLICATION (CWP) 3.0.1, Identification of Mission Relevant Terrain in Cyberspace, 20 August 2021

(az) MCO 5710.6D, Marine Corps Security Cooperation, 24 April 2020

(ba) MCO 5211.5, United States Marine Corps (USMC) Privacy Program, 28 August 2024

DCO-IDM and DOWIN Activities

1. Introduction. Joint Publication (JP) 3-12, "Cyberspace Operations" provides the doctrinal framework to enable the Joint Force to "plan, execute, and assess cyberspace operations". This MCO empowers the Commander of MARFORCYBER, through the cyberspace authorities delegated by USCYBERCOM and enabled by the Commandant of the Marine Corps, to assign cyberspace areas of operations and develop the necessary frameworks and authorization processes required to enable the conduct of integrated cyberspace operations. This enclosure focuses on DOWIN and DCO-IDM activities as they pertain to the current occupational fields in the Marine Corps.

2. DOWIN and DCO-IDM Missions. JP 3-12 defines DOWIN and DCO-IDM to provide a baseline foundation for understanding the mission types and are provided below.

a. DOWIN Operations. The DOWIN operations mission is to secure, configure, operate, extend, maintain, and sustain DoW cyberspace to create and preserve the confidentiality, availability, and integrity of the DOWIN. This mission includes cyberspace security actions that address vulnerabilities of the DOWIN or specific segments of the DOWIN to prevent exploitation and operation of red teams and other forms of security evaluation and testing. DOWIN operations also include a variety of cyberspace system operation actions like the set-up of tactical networks by expeditionary forces to extend existing networks, maintenance actions, and other non-security actions necessary for the sustainment of the DOWIN. DOWIN operations are network-focused and threat-agnostic: the cyberspace forces and workforce undertaking this mission endeavor to prevent all Malicious Cyberspace Activity (MCA) from negatively impacting a particular network or system they are assigned to secure. They are threat-informed and use all available intelligence about specific threats to improve the security posture of the network and reduce risk to operations.

b. Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM). DCO-IDM are the form of DCO mission where authorized cyberspace defensive actions occur within the defended network or portion of cyberspace. DCO-IDM include risk- and intelligence-driven internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses to eliminate and mitigate these threats. CPT operations on MRT-C in response to indications of MCA, or before specific indicators of compromise exist, are an example of DCO-IDM. DCO-IDM also include active and passive internal countermeasures to defeat and mitigate the MCA. DCO-IDM of the DOWIN is directed and synchronized by DCDC using a framework of DOWIN areas of operations and sectors established by USCYBERCOM.

3. Ownership of DOWIN and DCO-IDM Tasks. DOWIN Operations include activities that are network centric and threat informed. The cyberspace security activities within DOWIN Operations are designed to

be compliance-based and focus on the protection and threat prevention of the MCCE and the data within. The security employment includes the guidelines for configuration of network systems and architectures as well the requirements and guidelines outlined through standards and regulations. These activities are operated by multiple Occupational Fields and MOSs across the Marine Corps, each with a responsibility to networks or systems within the MCCE. Per MCRP 1-10.1, Organization of the United States Marine Corps, "The Marine Air Ground Task Force (MAGTF) CE G-6/S-6 exercises staff cognizance over MAGTF communications to facilitate system planning and engineering and the communication battalion conducts concurrent planning with the MAGTF G-6/S-6"; responsible for the installation, operation, maintenance, and security activities of DOWIN. The table below identifies specific activities that are executed through the conduct of DOWIN Operations, these activities are not all inclusive but provide a collection of like tasks.

DOWIN Activities	
Activity Group	Activities
(1)	Establish the DOWIN by installing, operating, maintaining, and securing physical and logical capabilities
(2)	Map, configure, scan, patch, update and monitor
(3)	Restore secure services
(4)	Analyze and control configurations
(5)	Advise and assist incident response actions
(6)	Support reporting requirements
(7)	LE/CI coordination for possible criminal activity
(8)	Establish baseline configurations of networks and systems
(9)	Continuous Monitoring for suspicious events

Table 2-1. DOWIN Activities

a. DCO is separated into two distinct components consisting of internal defensive measures and response actions. This enclosure will focus on DCO-IDM. DCO-IDM is akin to defensive fires and include those activities that are intelligence driven, threat specific, and network agnostic; meaning activities that can be conducted on or off network but are geared towards the detection, containment, eradication/mitigation of adversary actions and the re-secure of specified cyberspace terrain within a specific AO the DCO forces are tasked to defend, including warfighting programs, platforms, and critical infrastructure. DCO is additive to the traditional cyberspace security activities and utilized to counter an ongoing or imminent attack. DCO missions are Maneuver based operations in and through the cyberspace domain and planned by the G3 and executed by the service retained DCO forces (via tasking and command/control (C2) by the MEF Information Group (MIG)). The below activities chart

identifies some (but not all) of the DCO activities conducted within DCO-IDM.

DCO-IDM Activities	
Activity Group	Activities
(1)	Conduct threat hunting
(2)	Conduct counter / clear adversary activity
(3)	Enable hardening of specified mission relevant terrain in cyberspace (MRT-C) (blue reports)
(4)	Assess response action effectiveness
(5)	Identify and coordinate the inclusion of DCO-IDM requirements into DOWIN architectures
(6)	Conduct incident response requirements for CAT I, II, IV, and VII incidents (red reports)
(7)	Adversary activity intelligence gathering

Table 2-2. DOD-IDM Activities

b. While DOWIN operations and DCO-IDM are separate and distinct activities they are mutually supportive. When combining protection and defense the overall security of the MCCE is accomplished. The synergy between DOWIN operations and DCO-IDM comes from the integration and coordination conducted within the Marine Corps Planning Process between staff functions. The incorporation of cyberspace operations into planning allows for the synchronization of cyber effects into the MAGTF scheme of maneuver and supports the commander's ability to achieve and maintain superiority in and through cyberspace.

c. An example of mutual support deals with incident management and incident response. Continuous monitoring is a cyberspace security function that is performed during steady state operations and supported through the lifecycle of targeted threat hunting operations. Upon identification of a 'suspicious event' an initial triage is conducted to identify and categorize an event. Categorization of cyber events and incidents are defined in the USMC Enterprise Cybersecurity Manual (ECSM) 001. Responsibility of actions will be transferred to the service retained cyberspace forces for resolution and recommendations for any suspicious event that is believed to be adversarial (Categories I, II, IV, VII). All events that are not adversarial in nature (Categories III, V, VI, VII, IX) are worked through cyberspace security personnel. Reporting and tracking of incidents will be conducted through traditional cyberspace security actions and upon mitigation, will return to steady state operations in accordance with CJCSM 6510.01B and Marine Corps ECSM 001. The cycle continues across all aspects of the MCCE.

4. Conclusion. The Commander of MARFORCYBER grants the cyberspace authorities to conduct DOWIN and DCO-IDM operations. Marine Corps forces will follow this MCO and the frameworks and processes provided

by MARFORCYBER to ensure all required cyberspace activities for mission accomplishment are authorized and executed by certified cyberspace operators. The expected outcome of this MCO and enclosure is to provide the foundational backbone for integrated cyberspace operations.

Cyberspace Fires in the MAGTF

Maneuver warfare is a warfighting philosophy that seeks to shatter the enemy's cohesion through a series of rapid, violent, and unexpected actions which create a turbulent and rapidly deteriorating situation with which he cannot cope. (MCDP 1 Warfighting)

Marines focus on the force of human resolve and utilize technology to leverage the chaos and complexity of the battlefield. (MCDP 1-0 Marine Corps Operations)

1. The cyberspace domain is a rapidly changing environment that is used globally by both adversaries and allies, governments, and non-governmental actors. As new conflicts emerge, adversarial cyber effects will be layered against USMC key terrain in cyberspace. Additionally, our Marines will engage adversaries with multi-domain fires, including cyber effects. For Marines, the integration of cyber fires alongside traditional warfighting capabilities enables them to overwhelm adversaries across multiple domains and hold key terrain in cyberspace. The end state is to enable freedom of action across all warfighting domains and to deny the same to adversarial forces.

2. Cyber fires are a type of non-kinetic fires. Within a Marine Expeditionary Force (MEF), these fires are planned and executed from the Information Coordination Center (ICC) as part of the MEF Information Group (MIG) in support of the MEF Fire and Effects Coordination Center (FECC). Other units within the MAGTF who possess cyber personnel but have no direct chain of command to the ICC must coordinate with their chain of command to integrate effects with cognizance of the FECC at minimum, but preferably down to the ICC. The FECC may recommend for units to directly coordinate with the MIG and ICC for planning and execution tasks. This coordination must be approved by each O-5 commander within the chain of command of each unit. A generic line and block chart is provided in figure (1) on the next page to orient the location and command of these units.

3. Currently, MAGTF units possess limited capability to plan and conduct tactical offensive cyber operations. Despite some limitations, MAGTF units must seek to sense and understand cyberspace in their areas of operation, especially key terrain in cyberspace that is in use by adversaries. In order to conduct offensive cyberspace operations, MAGTF units must register intelligence requirements to enable cyberspace targeting. Cyberspace activities may be authorized by appropriate authorities to conduct target development, plan cyber effects, and source additional intelligence collection methods.

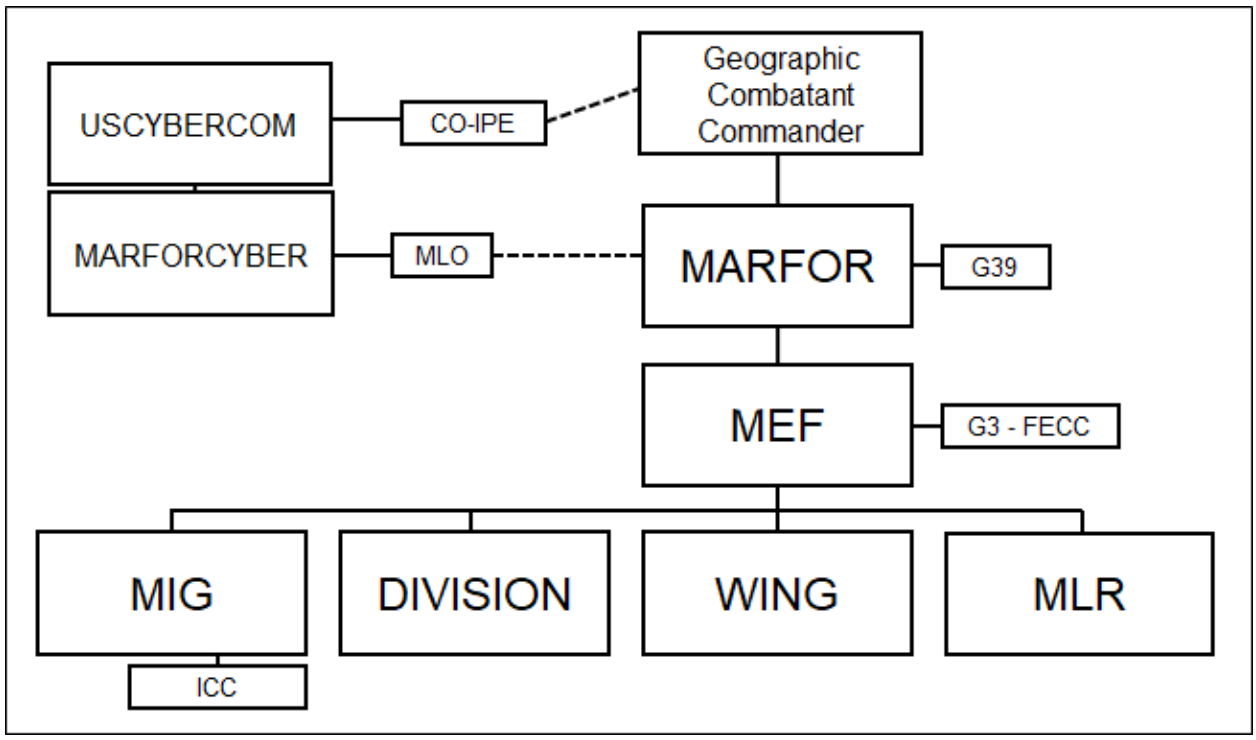

Figure (3-1): Generic FMF organization for offensive cyber planning

4. When conducting offensive cyber planning, Cyberspace Marines are reliant on MAGTF targeteers in first identifying adversary targets and target systems. Cyberspace terrain is so large and rapidly changing that the priority of work must first be to identify adversaries, and then secondly focus on the communication networks in use by adversaries. As government and non-governmental actors across the globe modernize, many have moved their entire communication processes to the global internet. In competition and in conflict, adversarial cyberspace must be identified, mapped, and prioritized for fires planning. Execution of these cyberspace fires may only occur when authorized. For questions regarding authorities, standards, qualifications, and training, MAGTF units must seek guidance from DC I policy and the G39 of their assigned component command.

5. Deconfliction of cyber operations is required before execution. Deconfliction requests must be routed through the chain of command to the joint level.

6. When local resources are insufficient to achieve desired end states, MAGTF units may plan cyber operations with USCYBERCOM via the chain of command. MAGTF units must coordinate through their chain of command prior to planning offensive cyber operations with any USCYBERCOM organization. When necessary, MAGTF units may request for support and provide forces to USCYBERCOM to achieve expected cyberspace fires. MAGTF commanders must recognize the loss of

authority over transferred Marines and that in these scenarios, risk evaluation and execution authorities for conducting offensive cyber operations remain with CDRUSCYBERCOM.

APPENDIX A

Glossary of Acronyms and Abbreviations

ATO	Authorization to Operate
ATC	Authorization to Connect
A&A	Assessment and Authorization
AO	Areas of Operation
C2	Command and Control
C4	Command, Control, Communications, and Computers
CBA	Capability Based Assessment
CCRI	Command Cyber Readiness Inspection
CD&I	Combat Development & Integration
CDRUSCYBERCOM	Commander, United States Cyber Command
CE2A	Cyberspace Effects Enabling Activities
CES	Cyber Excepted Service
CG	Commanding General
CG MCCDC	Commanding General, Marine Corps Combat Development Command
CMC	Commandant of the Marine Corps
CMF	Cyber Mission Forces
CMT	Combat Mission Team
CO	Cyberspace Operations
COF	Cyberspace Operations Forces
COI	Communities of Interest
CO-IPE	Cyberspace Operations Integrated Planning Element
COMMARCORSYSCOM	Commander, Marine Corps Systems Command
COMMARFORCYBER	Commander, U.S. Marine Corps Cyberspace Command
COMMCICOM	Commander, Marine Corps Installations Command
CONOPS	Concept of Operations
CoRE	Critical or Required Evaluation
CPT	Cyber Protection Team
CSSP	Cybersecurity Service Provider
CST	Combat Support Team
CYBERCOM	United States Cyber Command
DACO	Directive Authority for Cyberspace Operations
DCDC	Department of War Cyber Defense Command
DC CD&I	Deputy Commandant Combat Development & Integration
DC I	Deputy Commandant for Information
DC I&L	Deputy Commandant Installations and Logistics
DC PP&O	Deputy Commandant Plans, Policies, and Operations
DC T&E	Deputy Commandant for Training and Education
DCO	Defensive Cyberspace Operations
DCO-IDM	Defensive Cyberspace Operations – Internal Defensive Measures
DoW	Department of War

DoW CIO	Department of War Chief Information Officer
DOWIN	Department of War Information Network
DON	Department of the Navy
DON Deputy CIO	Department of the Navy Deputy Chief Information Officer
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
EA	Executive Agent
ELT	Entry-Level Training
EXORD	Executive Order
FAM	Functional Area Manager
FMF	Fleet Marine Forces
FRAGO	Fragmentary Order
FRCS	Facilities Related Control System
GCC	Geographical Combatant Command
GENADMIN	General Administration
GFMIG	Global Force Management Implementation Guidance
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IC	Intelligence Community
IGMC	Inspector General of the Marine Corps
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
JCC	Joint Cyber Center
JCIDS	Joint Capabilities Integration and Development System
JCTE	Joint Cyberspace Training Environment
MA	Mission Areas
MARCORSYSCOM	Marine Corps Systems Command
MARFORCYBER	U.S. Marine Corps Forces Cyberspace Command
MCAAP	Marine Corps Assessment and Authorization Process
MCCE	Marine Corps Cyberspace Environment
MCCOG	Marine Corps Cyber Operations Group
MCEN	Marine Corps Enterprise Network
MCIEE	Marine Corps Information Environment Enterprise
MEF	Marine Expeditionary Forces
MOS	Military Occupational Specialty
MPE	Mission Partner Environment
MROC	Marine Requirements Oversight Council
NGB	Network Governance Board
NSA	National Security Agency
OAG	Operational Advisory Group
OccFld	Occupational Field
OCO	Offensive Cyberspace Operations
OPADV	Operational Advisory Group
OPDIR	Operational Directive
OPORD	Operations Order
OPR	Office of Primary Responsibility

OPREP-3 SIR	Operations Event/Incident Report Serious Incident Report
OSD	Office of the Secretary of Defense
PCTE	Persistent Cyberspace Training Environment
PII	Personally Identifiable Information
PLANORD	Planning Order
POR	Programs of Record
PPBE	Planning, Programming, Budgeting, and Execution
SE	Supporting Establishment
STIG	Security Technical Implementation Guide
T&R	Training and Readiness
T/O	Tables of Organization
TA	Technical Authority
TAIG	Temporary Assistant Inspectors General
TASKORD	Task Order
TECOM	Training and Education Command
TIP	Training Input Plan
TTPs	Tactics, Techniques, and Procedures
UCP	Unified Command Plan
UNS	Universal Need Statement

APPENDIX B

Glossary of Terms and Definitions

Authorities – Authority for cyberspace operational actions undertaken by the US Armed Forces is derived from the US Constitution and federal law. Key laws that apply to DoW include Title 10, United States Code (USC), Armed Forces; Title 50, USC, War and National Defense; and Title 32, USC, National Guard. Authorities for specific types of military cyberspace operations are established within Secretary of War policies, including DoW instructions, directives, and memoranda, as well as in execute orders and operation orders authorized by the President or Secretary of War and subordinate orders issued by commanders approved to execute the subject missions. (Source: **JP 3-12**)

Authorization to Operate/Authorization to Connect (ATO/ATC) – The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. (Source: **CNSSI 4009**)

Authorizing Official – The Authorizing Official is a senior official or executive with the authority to formally assume responsibility for operating in information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and Nation. Authorizing officials typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, authorizing officials are accountable for security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Authorizing officials also approve security plans, memorandums of agreement or understanding, and plans of action and milestones and determine whether significant changes in the information systems or environments of operation system or if the system is operational, halt operations, if unacceptable risks exist. Authorizing officials coordinate their activities with the risk executive (function), chief information officer, Senior Information Security Officer, common control providers, and other interested parties during the security authorization process. With the increasing complexity of mission/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the

security plan. Authorizing officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to authorizing officials designated representatives are carried out. The role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only. This term has replaced Designated Accrediting Authority (DAA). (Source: **CNSSI 4009**)

Capability Based Assessment (CBA) – The Marine Corps CBA is a deliberate and integrated enterprise process through which the Marine Corps Total Force conducts capabilities analysis, gap analysis, solutions analysis, and risk analysis for the Operating Forces (OPFOR), Supporting Establishment (SE), and Headquarters Marine Corps (HQMC). (Source: **MCO 3900.20**)

Combat Mission Team (CMT) – Offensive cyber operation missions are normally assigned to CMTs, tactical units of the Cyber Combat Mission Force (CCMF) that support Combatant Commander (CCDR) plans and priorities to project power in support of national objectives. The CMTs are aligned, under the JFHQs-C, in support of Combatant Commands (CCMD). (Source: **JP 3-12**)

Intelligence, Surveillance and Reconnaissance (ISR) in Cyberspace – ISR in cyberspace is an activity that synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. ISR in cyberspace focuses on gathering tactical and operational information and on mapping enemy and adversary networks to support military planning. (Source: **JP 3-12**)

Command and Control (C2) – The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (Source: **JP 1-01**)

Command and Control Functions – Are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Source: **NIST SP 800-59**)

Configuration Management – A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (Source: **NIST SP 800-128**)

Cyber Incident Handling Reporting and Management – DoW cyber incident handling program protects, monitors, analyzes, and detects unauthorized or anomalous activity on the DOWIN. Information such as classified data spills, unauthorized access, and outages are collected

and distributed through a joint incident management system. (Sources: **DoDI 8530.01**)

Cyber Protection Team (CPT) – A team which is part of the Cyber Protection Force (CPF). The teams conduct cyberspace operations for internal protection of the DOWIN or other blue cyberspace when ordered. The CPT is organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of segment owners, cybersecurity service providers (CSSPs), and users. (Source: **JP 3-12**)

Cyber Support Team (CST) – Provide specialized technical and analytic support for the units of the CMF. This support includes intelligence analysis, cyberspace capability development, linguist support, and planning. (Source: **JP 3-12**)

Cyberspace Domain – A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and imbedded processors and controllers. (Source: **CNSSI 4009**)

Cyberspace Operations (CO) – Is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (Source: **JP 3-12)**

Cyberspace Operations Integrated Planning Element (CO-IPE) – Integrates within a CCDR's Cyberspace operations support staff to provide cyberspace operations expertise and reach back capability to USCYBERCOM. CO-IPEs are organized from USCYBERCOM, DCDC, and JFHQ-C personnel and are co-located with each CCMD for full integration into their staffs. CO-IPEs provide a CCDR with cyberspace planners and other subject matter experts required to support development of CCMD requirements and to assist CCMD planners with coordinating, integrating, and deconflicting cyberspace operations. (Source: **JP 3-12**)

Cyberspace Area of Operations (CyAO) – Cyberspace Areas of Operations are defined as the Marine Corps cyberspace terrain assigned to a commander or director over which they have authority or control to conduct defensive cyberspace and DOWIN Operations. CyAOs are portions of DAO Marine Corps. CyAOs are tiered based on their ability to conduct DCO-IDM per CWP 3-2 and the seven functions of cyber security outlined in DoDI 8530.01.

Defensive Cyberspace Operations (DCO) – Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (Source: **JP 3-12**)

Department of War Cyber Operations Forces (DoW COF) – Units organized, trained, and equipped to conduct offensive cyberspace operations, defensive cyberspace operations, and Department of War Information Network operations. There are eight operational groups including some that identify cyber mission forces assigned to U.S Cyber Command, forces assigned to the military services, forces assigned to combatant commands, and forces assigned to SOCOM. (Source: **SECDEF Memo 24 Jul 2025**)

Department of War Information Network (DOWIN) – The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. (Source: **JP 6-0**)

DOWIN Sector – A DOWIN Sector is defined as a DoW mission or functional area under the authority of a commander/ director that is supported by multiple DAOs. A DOWIN Sector CDR/DIR identifies and prioritizes all mission-essential capabilities on DoW cyberspace and off-DoW cyberspace relied on to assure a DoW Core function. (Source: **DODIN COMMAND Operational Framework EXORD 24-0091**).

DODIN Area of Operation (DAO) – A DAO is defined as the DOWIN terrain assigned to a DoW Component, over which they have direct authority or physical control. A DAO CDR is best postured with authority to synchronize, coordinate, and direct Cyberspace Forces as a unified force on DoW Cyberspace. (Source: **DODIN COMMAND Operational Framework EXORD 24-0091**).

Directive Authority for Cyberspace Operations (DACO) – SECWAR created DACO to grant CDRUSCYBERCOM authority and direction over all elements of the DOWIN for the purpose of conducting DOWIN Operations and executing DCO-IDM, in order to compel unity of action that enables DoW-wide integrated and synchronized protection of the DOWIN. CDRUSCYBERCOM delegates DACO over all elements of the cyberspace within a Military Service DAO to the Service Cyber Component (SCC) designated as the Military Service DAO CDR for an enduring purpose. This delegation empowers Military Service DAO CDRs with the authority and direction over all elements of the Military Service DAO to issue orders and directives to secure, operate, and defend cyberspace in order to compel unity of action within the Military Service DAO. (Source: **DODIN COMMAND Operational Framework EXORD 24-0091**)

Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Cost (DOTMLPF-C) – To ensure the supportability of any new materiel or non-materiel solution affecting force structure and to identify and address interconnected force structure issues throughout implementation. *Note: While the MC CBA develops solutions across DOTMLPF-Policy, the TFSP considers costs rather than policy when developing detailed analysis.* (Source: **USMC Force Development System User Guide**)

DOWIN Operations – Operations to secure, configure, operate, extend, maintain, and sustain Department of War cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of War information network. (Source: **JP 3-12**)

Functional Area Managers (FAMs) – FAMs shall establish IT portfolio management processes and a governance structure to enforce compliance of systems, applications, and databases within their IT portfolios. (Source: **MARADMIN 253/11**)

Future Year Defense Program (FYDP) – Program and financial plan for the DoW as approved by the Secretary of War. The FYDP arrays cost data, manpower, and force structure over a 5-year period (force structure for an additional 3 years), portraying this data by major force program for DoW internal review for the program and budget review submission. It is also provided to the Congress annually in conjunction with the President's budget. (Source: **DoDD 7045.14**)

Geographical Combatant Commands (GCC) – Have the responsibility to prevent the loss or degradation of DCI within their AORs and coordinate with the DoW asset owner, heads of DoW components, and defense infrastructure sector lead agents to fulfill this responsibility. (Source: **JP 3-12**)

Information Assurance Vulnerability Alert (IAVA) – Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoW systems and information; this alert requires corrective action because of the severity of the vulnerability risk. (Source: **CNSSI 4009**)

Joint Capabilities Integration and Development System (JCIDS) – Provides the baseline for documentation, review, and validation of capability requirements across the Department. Validated JCIDS documents facilitate DOTMLPF-P changes, guide the Adaptive Acquisition Framework pathways subject to this policy, and inform PPBE processes. Once validated, regardless of validation authority, Sponsors will upload final versions of JCIDS documents and their associated validation memoranda into Knowledge Management/Decision Support (KM/DS). This is done for archiving purposes and for visibility in the capability portfolios. (Source: **CJCSI 5123.01I**)

Malware Analysis – The process of identifying, analyzing, and characterizing reported software artifacts suspected of being adversarial tradecraft to help defense in depth mitigation actions and strategies, CI activities, and LE activities. (Source: **CJCSM 6510.01B**)

Marine Corps Assessment and Authorization Process (MCAAP) – Outlines the requirements and standards and serves as direction for users of all Marine Corps Information Systems, Information Technology systems, Operational Technology systems, (e.g., Facility Related Control Systems (FRCS), Supervisory Control and Data Acquisition (SCADA) and

Industrial Control Systems (ICS)), and the management of the information systems on the MCEN. (Source: **ECSM 018**)

Marine Corps Cyberspace Environment (MCCE) – The Marine Corps' portion of the DOWIN 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 MCISRE, including cyber discipline. Under this definition, the MCCE includes: PORs, MCEN, Amphib Networks, Tactical Networks, USMC portion of TS networks, MCISRE, Installation Communications, Platform IT, and IOT/OT. Additionally, the MCCE may include extensions to approved commercial cloud service providers, and Commercial Solutions for Classified networks, extensions to other domains (.edu, .org, etc.), and connections to MPE. The MCCE is a subcomponent of the Marine Corps Information Environment (MCIEE). (Source: **MCEN Implementation Plan January 2024**)

Marine Corps Enterprise Network (MCEN) – The MCEN is the Marine Corps' assured information systems backbone, providing unclassified and classified network enclaves to support USMC warfighting, business operations, and supporting establishment functions to maintain power projection platforms worldwide. It comprises people, processes, logical and physical infrastructure, architecture, topology, and cyberspace operations. The MCEN is characterized at a minimum to include Programs of Record that provide network services to forward deployed forces operating in the USMC.mil namespace and in USMC routable IP addresses; and Operations and Maintenance functions that provision data transportation, enterprise IT, network services, and boundary defense. (Source: **MCEN Implementation Plan, January 2024, MCIEE Blueprint v1.0**)

Marine Corps Information Environment Enterprise (MCIEE) – The MCIEE is an ecosystem of people, processes, and capabilities capable of connecting users with data to address a mission. This Information on Demand unifies organization, architectures, data, and processes across the Marine Corps. (Source: **MCIEE Blueprint v1.0**)

Marine Corps System and Network Administrators (SYSADMIN/NTWKADMIN) – Privileged users, which are defined as individuals who have access to system control, monitoring, or administration functions. (Source: **MCO 5239.2B**)

Marine Requirements Oversight Council (MROC) – Serves as the primary, senior-level Marine Corps leadership forum to advise and assist the Commandant of the Marine Corps in the execution of his Title 10 USC and Joint Chiefs of Staff (JCS) responsibilities. The MROC advises the Commandant on a wide range of Service functions within a framework of well-defined systems and processes in order to effect changes to enhance the Corps' ability to accomplish its missions. (Source: **MROC Handbook**)

Mission Partner Environment (MPE) – MPE is the operating framework enabling command and control (C2) and information sharing for planning and execution across the full range of military operations. An MPE capability provides the ability for DoD and MPs to exchange information with all participants within a specific partnership or coalition, which includes: Other Federal departments and agencies; State, local, and tribal governments and agencies; Non-government organizations; Private sector organizations; Allies, coalition members, host nations, and other nations via Multinational treaty. (Source: **DoDI 8110.01**)

Offensive Cyber Operations (OCO) – Missions intended to project power in and through cyberspace. (Source: **JP 3-12**)

Portfolio Management (PFM) – The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. (Source: **MCO 5230.21**)

Privileged User – A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Source: **CNSSI 4009**)

Program of Record (POR) – An Acquisition Program which is a directed, funded effort that provides a new, improved, or continuing materiel, weapon, or information system or service capability in response to an approved need. Acquisition programs are divided into categories that are established to facilitate decentralized decision making, execution, and compliance with statutory requirements. The Program of Record is as recorded in the current Future Year's Defense Program (FYDP) or as updated from the last FYDP by approved program documentation (e.g., APB, acquisition strategy, SAR, etc.) When this happens, the program becomes a "line item record" in the budget -- hence the term "program of record". (Source: **ECSM 019)**

Risk Assessments – Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. Risk assessment process - preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment. (Source: **SP 800-30 Rev. 1**)

Security Technical Implementation Guide (STIG) – Based on DoW policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoW baseline. (Source: **DoDI 8500.01**)

Standalone Systems – System that is not connected to any other network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary. (Source: **DoDI 8500.01**)

Technical Authority (TA) – Technical Authority is the authority, responsibility, and accountability to establish, monitor, and approve technical standards, tools, and processes in conformance with applicable DoW and DON policy, requirements, architectures, and standards.

Total Force Structure Process – The TFSP is a dynamic, non-linear process which provides a framework of understanding for developing and maintaining force structure. The TFSP transforms strategic guidance, policy constraints, and commander-generated recommendations into the integrated capabilities required to execute USMC missions. (Source: **MCO 5311.1E)**

Urgent Needs Process (UNP) – The UNP synchronizes abbreviated requirements, resourcing, and acquisition processes to distribute mission-critical warfighting capabilities more rapidly than the deliberate processes permit. Subject to statues and regulations, it is optimized for speed and accepts risk regarding doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) integration, sustainment, and other considerations. (Source: **MCO 3900.17**)

User – Defined as any military, government civilian, or contractor who has authorized access to the DOWIN or Marine Corps IT resources. (Source: **MCO 5239.2B**)

Urgent Universal Need Statement (Urgent UNS) – An Urgent UNS is used to initiate the UNP. It is an exceptional request from a combatant command-level Marine component commander for an additional warfighting capability that is critically needed by operating forces conducting combat or contingency operations. (Source: **MCO 3900.17**)