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

MCO 5239.2B
C4
05 NOV 2015

MARINE CORPS ORDER 5239.2B

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS CYBERSECURITY

Ref: (a) Armed Forces, Title 10 U.S.C. § 2223 The Clinger-Cohen Act (CCA)
(b) Title 40 U.S.C. § 11331 Federal Information Security Management Act (FISMA),
(c) Title 44 U.S.C. § 3541 Management of Federal Information Resources,
(d) Circular No. A-130 Revised
(e) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014
(f) MCO 5400.52, "Department of the Navy Deputy Chief Information Officer Marine Corps Roles and Responsibilities," January 5 2010
(g) CJCSI 6510.01F, “Information Assurance (IA) and Support to Computer Network Defense (CND),” October 10 2013
(h) DoD Instruction 8520.03, “Identity Authentication for Information Systems”, May 13 2011
(i) DoD 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling, " May 24 2011
(j) DoD Directive 8500.01, “Cybersecurity,” March 14, 2014
(k) SECNAVINST 5239.3B, "Department of the Navy Information Assurance Policy," June 17 2009
(k) SECNAV M-5239.1, "Department of the Navy Information Assurance Program, Information Assurance Manual" November 2005
(m) DON DIACAP Handbook, "DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook," July 15 2008
(n) DoD Instruction 8580.1, “Information Assurance (IA)in the Defense Acquisition System,” July 9, 2004
(o) DoD Instruction 5220.22, “National Industrial Security Program (NISP),” March 18, 2011

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

(p) MCO 2281.1A, " Electronic Key Management System (EKMS) Policy," June 11 2014
(q) DoD Instruction 8551.01, “Ports, Protocols, and Services Management (PPSM),” May 28, 2014
(r) CJCSI 6211.02D, “Defense Information System Network (DISN) Responsibilities,” January 24, 2012
(s) MCO 7300.21b, " Marine Corps Financial Management Standard Operating Procedure Manual Program," July 2 2013
(t) SECNAV 7510.7F, "DON Internal Audit," December 27 2005
(u) MARADMIN 375/11 "Information Technology (IT) Funding, Approval, And Procurement," July 6 2011
(v) Joint Publication 3-12 (R), “Cyberspace Operations,” 5 February 2013
(w) DoD Instruction O-8530.2, “Support to Computer Network Defense (CND),” March 9 2001
(x) DoD Manual O-8530.1-M, “Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program,” December 17, 2003 (NOTAL)
(y) DoD Directive 5205.02-M, “DOD Operations Security (OPSEC) Program,” November 3 2008
(z) CJCSM 6510B, “Cyber Incident Handling Program” July 12 2012
(aa) Defense Acquisition Guidebook, June 7 2013
(ab) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003, certified current 20 Nov 2007
(ac) CJCS CM-0363-08, Updated Definition of Cyberspace, July 10 2008
(ad) NIST Special Publication 800-37,” Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” June 10 2014
(ae) DoD Directive 8570.01, “Information Assurance (IA) Training, Certification, and Workforce Management,” April 23 2007
(af) SECNAVINST 5239.19, "Department Of The Navy Computer Network Incident Response And Reporting Requirements," March 18 2008
(ag) DoD Instruction 5230.29, “Security and Policy Review of DOD Information for Public Release,” August 13 2014
(ah) SECNAVINST 5211.5E, "Department Of The Navy (DON) Privacy Program," December 28 2005

(ai) MCO 3070.2A, "The Marine Corps Operations Security (OPSEC) Program," July 2 2013
(aj) ALNAV 070/07, "Department of the Navy (DON) Personally Identifiable Information (PII) Annual Training Policy," October 4 2007
(ak) SECNAVINST 3030.4C, "Department of the Navy Continuity of Operations Program," July 22 2009
(al) DoD 8570.01-M CH 3, “Information Assurance Workforce Improvement Program,” January 24 2012
(am) DoD 5500.7-R, “Joint Ethics Regulations (JER),” November 17 2011
(an) DoD Directive 1344.10, “Political Activities by Members of the Armed Forces,” February 19 2008
(ao) SECNAV M-5210.1, "Department of the Navy Records Management Program," January 2012
(ap) HQMC C4 The Marine Corps Information Enterprise (MCIENT) Strategy, December 14 2010
(aq) CJCSM 6510.01A, “Information Assurance and Computer Network Defense Volume 1 (Incident Handling Program)”, June 24 2009
(ar) Interim DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” November 25, 2013
(as) MCO 3100.4, "Cyberspace Operations," July 27 2013
(at) DoDM 5200.01, “DoD Information Security Program: Volume 2, Marking of Classified Information”, March 19 2013
(au) SECNAV M-5239.2, "Department of the Navy Information Assurance (IA) Workforce Management Manual to Support the IA Workforce Improvement Program," May 29 2009
(av) SECNAVINST 5400.15C CH-1, "Department of the Navy Research and Development, Acquisition, Associated Life-Cycle Management, and Logistics Responsibilities and Accountability," December 2 2011

Encl: (1) Definitions
(2) Acronyms
(3) Appendix A - MARINE CORPS COMMAND CYBER READINESS INSPECTION (CCRI) PREPARATION PROCESSES AND REQUIREMENTS

1. Situation

a. Our adversaries continue to become more technically and tactically sophisticated. They are utilizing low-cost attack tools making them a formidable and dangerous threat. Others are

far more sophisticated with financial backing and nation state support. The implementation and adherence to policies and guidelines that support strong protection, detection, response, restoration, remediation, and mitigation activities are key to achieving and maintaining dominance on the cyber battlefield. It is imperative to implement timely, cost-effective, and proactive cybersecurity practices to increase the Marine Corps' ability to identify and mitigate vulnerabilities and threats before exploitation can occur.

b. Marine Corps Cybersecurity takes an enterprise-wide approach to protect United States Marine Corps critical information and intelligence from internal and external threats and attacks. This ensures that our Warfighters and Supporting Organizations are able to achieve and maintain information dominance across the full spectrum of military operations. The Marine Corps Cybersecurity plan will be implemented in a unified approach to ensure the confidentiality, integrity, and availability of unclassified, sensitive, and classified information that is received, stored, processed, displayed, or transmitted by Marine Corps information systems; consolidates and focuses Marine Corps efforts in securing the information, including its associated systems and resources; increases the level of trust of this information and the originating source; and provides identity assurance to all users accessing the Marine Corps Enterprise Network (MCEN).

c. Operationally, failure to implement the proactive or corrective cybersecurity measures identified in this Order may result in critical information loss, capture, corruption, or lack of timely access which may potentially lead to mission failure. Administratively, it may prevent system or enclave accreditation, installation, or operation. System administrators or network personnel may block access to information systems that have been determined to adhere to poor cybersecurity practices or fail to implement identified corrective measures. Additionally, systems on the MCEN processing intelligence information are required to adhere to the provisions of this Order.

d. The Marine Corps Sensitive Compartmented Information (SCI) networks and systems are protected under the Marine Corps Director of Intelligence (DIRINT) SCI Enterprise Office (SEO). The SEO provides an enterprise-wide approach to protect Marine Corps critical SCI residing within Marine Corps Intelligence Surveillance and Reconnaissance Enterprise (MCISR-E) from intended or unintended malicious attacks from internal and

external threats. The SEO Cybersecurity responsibilities are governed by policies and directives from the Office of the Director of National Intelligence (ODNI), Defense Intelligence Agency (DIA) and the National Security Agency (NSA).

e. The Marine Corps Cybersecurity order develops policy and provides guidance that is in accordance with the references shown throughout this Order.

2. Cancellation. MCO 5239.2A, MARADMIN 333/08

3. Mission. This Order in accordance with reference (a) provides cybersecurity policy, procedures, tasks, conditions, and standards implementation guidance applicable to enhance and enable command and control on the MCEN. An Annex providing the policy, procedures, and standards implementation guidance for Marine Corps SCI Networks will be published 180 days from the issuance of this Order. Supplemental cybersecurity guidance, updates, or revisions will be provided through Enterprise Cybersecurity Manuals (ECSMs), Marine Administration (MARADMIN) messages, and Marine Corps Bulletins (MCBUL).

a. This Order in accordance with reference (b) delineates all organizational actions required to ensure the security of voice video, and data communications, digital information in all of its forms, and the security of the systems and networks where information is stored, accessed, processed, and transmitted. This includes precautions taken to guard against cyber attacks in order to provide an end-to-end secure networking capability to protect and deliver secure information at the right time, to the right place, and in a useable format, enabling commanders to exercise freedom of command and control.

b. The MCEN is the Marine Corps network-of-networks and approved interconnected network segments supporting the Marine Corps Command, Control, and business process communications. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate according to Marine Corps policy. The MCEN is both, the MCEN - NIPRNet (MCEN-N) and the MCEN SIPRNet (MCEN-S); however, this document will refer to both networks as one MCEN.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. In accordance with references (c) and (d) the Marine Corps will employ a comprehensive cybersecurity program designed to protect and defend the MCEN and the data in transit and the data at rest on the MCEN to ultimately support the commander's information needs. New technologies such as web services and portals are emerging in support of developmental, training, testing, exercise, and operational deployments. This Order contains a comprehensive framework for security governance and controls over information resources and will facilitate the rapid assimilation of new technologies and information processing methodologies. Per references (e) and (f) a professional cyber workforce will execute this framework in a flexible, proactive manner and will continue to improve efforts to effectively manage and monitor network performance and system activities. The Marine Corps must employ a cybersecurity capability that supports a robust, enterprise-wide, "best network security practices", and posture to improve cybersecurity implementation and situational awareness across the MCEN. In accordance with this Order, the Marine Corps will incorporate proactive protection, detection, reaction, disaster recovery, and restoration capabilities to include the detection of, reporting on, and employment of countermeasures against unauthorized activities. Concurrently, the effectiveness of cybersecurity programs, policies, and procedures will be reviewed by means of established procedures (i.e., Headquarters Marine Corps Command, Control, Communication, and Computer Cybersecurity Division (C4 CY) monthly security evaluations; Marine Corps Operational Test and Evaluation (MCOTEA) operational Information Assurance (IA) assessments; CCRIs; Inspector General of the Marine Corps (IGMC)).

(2) Concept of Operations. The Marine Corps will adopt an information system "life-cycle management" approach as shown in references (g), (h), and (i), in applying uniform standards for the protection of Marine Corps Information Technology (IT) resources that display, transact, transmit, or receive information. The Marine Corps will iteratively assess threats, vulnerabilities, risks, and a spectrum of cybersecurity practices to identify, document, and implement appropriate countermeasures to effectively mitigate risks to an acceptable operational level.

(3) Responsibilities

(a) Director, Command, Control, Communications, and Computers (C4)/Deputy Department of the Navy Chief Information Officer Marine Corps (Deputy DON CIO MC) shall:

1. Per reference (c) and (j), exercise oversight authority and CIO governance for all matters and programs regarding Marine Corps Cybersecurity and be responsible directly to the CMC for all cybersecurity policies and programs enacted throughout the Marine Corps (excluding SCI networks) as outlined in reference (k).

2. Establish a comprehensive program to implement, document, and manage a standard Configuration Management Program (CMP) across the MCEN for all non POR systems.

3. Ensure Marine Corps networks are Public Key-enabled and User-based Enforced in accordance with reference (l) and the United States Cyber Command (USCYBERCOM) directives.

4. Execute the duties as the Marine Corps Authorizing Official (AO) (excluding SCI systems) for the MCEN in accordance with references (a) through (g).

5. Designate a Marine Corps Senior Information Security Officer (SISO) for the MCEN (as defined in Title 40 § 11331, Title 10 §2223, and Title 44 §3544(a)(2) & (3)) references (a), (b), and (c).

(b) Marine Corps Senior Information Security Officer (SISO)

1. Carry out the Director C4/DDONCIO (MC)’s cybersecurity responsibilities in accordance with reference (c).

2. Pocesses professional qualifications, including training and experience, required to administer the functions and tasks listed in this Order.

3. Create, promulgate, inspect, validate, oversee, and execute cybersecurity processes throughout the Marine Corps.

4. Develop, issue, validate, and maintain Marine Corps cybersecurity policies and procedures to implement cybersecurity throughout the Marine Corps and serve as the focal

point for Marine Corps cybersecurity programs, tasks, standards, and prioritize cybersecurity resource requirements in the planning, programming, budgeting and execution process for the MCEN.

5. Standardize Marine Corps' cybersecurity policies, procedures, directives, and guidance in accordance with references (e) through reference (n), to adhere to applicable Federal, Department of Defense (DoD), DON, and Marine Corps cybersecurity directives.

6. Coordinate with the DIRINT to ensure SEO representation in the cybersecurity working groups, the Cross Domain Solution (CDS) Office, and the Cybersecurity Steering Group (CSSG) to adequately represent SCI networks.

7. Chair the CSSG, chartered under the C4 Operational Advisory Group (C4 OAG), responsible to coordinate and standardize cybersecurity standards and practices implemented throughout the MCEN.

8. Ensure Marine Corps cybersecurity requirements are developed, validated, and forwarded for inclusion in appropriate Federal, DoD, and DON cybersecurity directives.

9. Ensures Marine Corps representation to DoD, Joint, and DON cybersecurity panels and working groups.

10. Establish and maintain a standardized Marine Corps Security, Test, and Evaluation (ST&E) methodology, Certification and Accreditation (C&A) Program, and security requirements as part of the Marine Corps C&A Process (MCCAP) in accordance with references (e) through reference (n).

11. Establish and maintain a Marine Corps Institutional Cybersecurity Enterprise Defense Monitoring Team (Marine Corps ICE DEMon aka "White Team") in accordance with reference (k), with perisistant enterprise privileges and credentials to independently identify and validate vulnerabilities on all systems and network devices in order to reduce the overall risk to the MCEN in a collaborated effort.

12. Document, develop, coordinate, advocate, and prioritize Marine Corps cybersecurity program resource requirements in the planning, programming, budgeting and execution process.

13. Coordinate with the Naval Communications Security (COMSEC) Management Service (NCMS) per reference (o) for policy development and dissemination, support, tactics, techniques, and procedures (TTPs) for the design, implementation, and operation of the Key Management Infrastructure (KMI) and systems to support Marine Corps cryptographic requirements.

14. Provide program oversight for Marine Corps implementation of the KMI and funding aspects of the Electronic Key Management System (EKMS) and provide cybersecurity guidance to Marine Corps elements to identify and incorporate requirements consistent with the KMI in project development.

15. Represent the Marine Corps as a voting member on the Key Management Executive Committee (KMEC) and Joint Key Management Infrastructure Working Group (JKMIWG).

16. Provide program oversight for the Marine Corps implementation of the Public Key Infrastructure (PKI) as directed by DoD.

17. Prepare the annual Marine Corps Cybersecurity Readiness Report and Marine Corps input to the annual DON Cybersecurity Report to include FISMA data collection and reporting in accordance with references (b), (g) through (i) and reporting to DoD IT Portfolio Repository – Department of the Navy (DITPR-DON).

18. Manage the IGMC Functional Area Checklist (405) "Information System Management" program and per references (s) and (t) provide technical and operational assistance to the Naval Audit Service (NAS) and the Marine Corps Inspector General in audits and reviews of Marine Corps information systems.

19. Evaluate technological trends in cybersecurity and sponsor research activities to identify, define, and develop requirements and standards for inclusion into the Marine Corps capability sets of cybersecurity.

20. Provide Marine Corps voting representation for the following:

a. Committee on National Security Systems (CNSS) and the Subcommittees for Telecommunications Security (STS) and Information System Security (SISS).

b. Defense/IA Security Accreditation Working Group (DSAWG) per reference (q).

c. DoD Enterprise-wide IA and Defensive Cyber Operations (DCO) Solutions Steering Group (ESSG) per reference (f).

d. C4/Cybersecurity Leadership Board.

21. Provide policy, guidance, and oversight to employ the National Institute of Standards and Technology (NIST) approved cryptography standards to protect unclassified and sensitive information.

22. Provide oversight and direction per references (k), (q), and (r) for Marine Corps Web Risk Assessment Cell (MWRAC) cybersecurity and support to OPSEC programs and initiatives.

23. In conjunction with CS and CR Divisions coordinate with Commanding General, Training and Education Command (TECOM) per reference (k), to ensure cybersecurity training requirements are identified, developed, met, and provided to all military members, government civilians, and contract personnel who have access to any portion of the DoD Information Network (DoDIN) and the MCEN.

24. Coordinate with Commander, Marine Corps Systems Command (MARCORSYSCOM) and Deputy Commandant, Combat Development and Integration (CD&I) per references (k) and (o), to validate Marine Corps COMSEC and cybersecurity capabilities are advocated for during the development of the DON Program Objective Memorandum (POM).

25. Coordinate with Commander, Marine Corps Installation Command and Deputy Commandant, Installations and Logistics (I&L) to validate Marine Corps communication facilities, structure, and spaces to ensure they are fully defined and resourced during the development of the DON POM.

26. Evaluate IT procurement requests (ITPRs) within the ITPR Review and Approval System per MARADMIN 375/11, for compliance with cybersecurity policies and MCEN authorized configuration requirements prior to approval.

27. Represent the Marine Corps on the DoD Ports, Protocols, and Services Configuration Control Board (CCB) and

provide oversight for Marine Corps Ports, Protocols, and Services Management program per reference (p).

28. Provide Marine Corps voting member representation to the DoD Information Assurance Workforce Improvement Program.

29. Provide member participation in the HQMC PP&O Contigency Planning working group as the lead for IT Contingency Planning and Disaster Recovery.

30. Provide Marine Corps C4 representation to the National Insider Threat Task Force, and coordinate Marine Corps Insider Threat policies, programs, and capability implementations with PP&O.

31. Establish skill requirements and appoint Marine Corps Validators.

(c) Deputy Commandant for Combat Development and Integration (CD&I) shall:

1. Ensure cybersecurity requirements are incorporated into applicable Joint Capabilities Integration and Development System (JCIDS), Military Construction (MILCON) and other facilities documentation (e.g., Installation Master Plan, Base Facilities Request, Urgent Universal Needs Statement (UUNS)) for all facilities, structures, and spaces that have information technology requirements.

2. Ensure that throughout the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities (DOTMLPF) process includes Cybersecurity requirements.

3. Coordinate with the Director C4/DDONCIO (MC), Commander MARFORCYBER, Commander Naval Facilities Command and Army Corps of Engineers and the Commander, MARCORSYSCOM as shown by refences (j) and (k), for the integration of enterprise level cybersecurity interoperability requirements.

4. Coordinate with the SEO for integration of SCI level systems, capabilities, requirements and interoperability.

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

1. Ensure cybersecurity requirements are incorporated into applicable MILCON and other facilities documentation (Installation Master Plan, Base Facilities Request) for all facilities, structures, and spaces that have a information technology requirement.

2. Ensure that througouth the DOTMLFP process and follow on processes for Facilities includes Cybersecurity requirements.

3. Coordinate with Director C4/DDONCIO (MC), Commander Naval Facilities Command and Army Corps of Engineers for the intergration of enterprise level cybersecurity interoperability requirements.

(e) Commander, MARFORCYBER shall:

1. As required by references (a) through (c) and (j) through (k), coordinate with Director C4/DDONCIO (MC) and the Marine Corps SISO regarding the operations and defense of Marine Corps computer systems and networks on the MCEN as directed by the USCYBERCOM.

2. Per references (a) through (c) and (j) through (k), coordinate Cyber Conditions (CYBERCON) with Director C4/DDONCIO (MC) and the Marine Corps SISO in response to Offensive Cyber Operations (OCO) and report the Marine Corps CYBERCON status to USCYBERCOM.

3. As required by reference (q) aggregate MCEN Intrusion Detection/ Prevention Systems (IDS/IPS) data and key network device logs and provide incident trend and correlation analysis of network traffic across the MCEN and make this information available to organizations with a valid need to know.

4. Integrate DCO, OPSEC, and CYBERCON activities into cyber and other applicable information related capabilities in accordance with references (g), (o), (p), and (v) through (z) in coordination with Director C4/DDONCIO (MC) and the Deputy Commandant for Plans, Programs, and Operations (DC PP&O).

5. Develop and maintain a Marine Corps DCO vulnerability and threat database for situational awareness monitoring, reporting, event correlation, and trend analysis.

6. Develop TTPs for a threat warning and notification process.

7. Develop procedures to issue DCO lessons learned identified from incidents, intrusions, forensic analyses, or other technical processes in coordination with Director C4/DDONCIO (MC) and the Marine Corps SISO to higher, adjacent, and supporting cybersecurity organizations.

8. Coordinate and collaborate with Director C4/DDONCIO (MC), HQMC Intelligence (HQMC I), adjacent MARFORs, MCCDC, and Marine Corps Installation Command (MCICOM), to conduct, receive and/or provide technical analyses and studies concerning cyber threats in order to support cybersecurity decision makers.

9. Coordinate with Intel Department to provide intelligence support to cybersecurity decision makers.

10. Coordinate with Director C4/DDONCIO (MC) to execute Cyber Red Team Operations against MCEN targets through effective employment of remote network operations, wireless exploitation, and close access to validate and test the MCEN security posture. Ensure operation plans are provided 90 days in advance to the Marine Corps SISO to coordinate with DoD CIO, as directed in reference aa.

11. Coordinate with the Director C4/DDONCIO (MC) and the Marine Corps SISO to ensure Marine Corps Network Operations and Security Center (MCNOSC) provides persistent enterprise access and credentials to the C4 ICE DEMons in accordance with 4a(3)(b)11 of this Order.

12. In coordination with the Marine Corps SISO, monitor Marine Corps Information Assurance Vulnerability Management (IAVM) program compliance and act as the Marine Corps' reporting agent and clearinghouse for Information Assurance Vulnerability Alert (IAVA) compliance and Information Assurance Vulnerability Bulletins (IAVBs).

13. Coordinate, as required, with Combatant Command (COCOM), Commander MCICOM, and Marine Force Commanders to provide DCO support for deployed units.

14. Coordinate vulnerability assessments on the MCEN with Marine Corps SISO to maintain the highest security posture.

15. Coordinate with Marine Corps Public Affairs to ensure Marine Corps websites are configured and maintained in compliance with prescribed Federal, DoD, DON, and Marine Corps website administration policies and procedures.

16. Monitor network traffic between MCEN Point of Presence (POP) sites, the DoDIN, and all network layers from external boundary to host level for intrusions, incidents, and anomalies. Provide real time and appropriate impact assessments and responses to cyber security organizations who have a valid need to know.

17. Provide Commanders via Regional Network and Operations Security Centers and Marine Air Ground Task Force Information Technology Centers (MITSCs) with threat related information relevant to their particular Area of Responsibility so incident response actions can be initiated as required.

18. In addition to the appropriate chain of command or law enforcement/counter intelligence agencies, report to Director C4/DDONCIO (MC) via the Marine Corps SISO all major impacts on Marine Corps operations; unusual network activities; violations of Federal, DoD, DON, and Marine Corps cybersecurity policies; and criminal acts conducted on Marine Corps IT resources.

19. Establish TTPs for the DCO Section (DCOS) personnel in coordination with Marine Corps SISO as required for cyberspace operations.

20. Integrate computer incident response, impact assessment capabilities, cybersecurity, and DCO service provider activities into network operations (NETOPS), network management, and information dissemination to ensure timely situational awareness across the MCEN.

(f) Director, Intelligence shall:

1. As the Marine Corps principal for intelligence and SCI programs to include Marine Corps SCI Facilities (SCIFs), networks and systems, adhere to the cybersecurity directives, policies, and guidance from ODNI, DIA, and NSA.

2. Exercise oversight authority for all SCI matters and programs regarding the MCCSP and be responsible

directly to the CMC for SCI cybersecurity policies and programs enacted throughout the Marine Corps.

3. The DIRINT will publish an ANNEX 180 days from the issuance of this Order, in coordination with the Director C4/DDONCIO (MC), providing the policy, procedures, standards and implementation guidance for Marine Corps SCI Networks.

4. Provide Director C4/DDONCIO (MC) and the MARFORs with service-level intelligence support of foreign cyber intelligence threats.

(g) Commander, Marine Corps Systems Command shall:

1. Execute Technical Authority responsibilities as delegated to MARCORSYSCOM under reference (u) to ensure cybersecurity execution for Program of Record (POR)/Centrally Managed Programs.

2. Acquire and field validated materiel solutions in support of defined capability requirements compliant with DoD, DON, and Marine Corps cybersecurity policy and guidance applicable to the particular materiel solutions. The information systems and products will be developed and supported per this Order.

3. Integrate cybersecurity, identity management, COMSEC, and Telecommunications and Electrical Machinery Protected from Emanations Security (electromagnetic compatibility) TEMPEST, now known as Emissions Security (EMSEC) into the entire system lifecycle. This will ensure that the use of market-driven/industry-developed (MDID), commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), or other products that are consistent and tested will comply with cybersecurity requirements and do not introduce unacceptable levels of risk.

4. Ensure cybersecurity requirements are engineered, embedded, and incorporated in the earliest phases of the system acquisition, contracting, and development life cycles in accordance with reference (s).

5. Ensure program managers acquire systems in accordance with the provisions of this Order to establish timely, cost-effective, and proactive cybersecurity capabilities. Included in this effort are identity management and

cybersecurity measures which are designed to identify vulnerabilities and threats.

6. Identify cybersecurity funding requirements needed to ensure the security design, implementation, and maintence of security configuration for Programs of Record used within the Marine Corps. As directed by reference (s) report the amount and percentage of Program Manager (PM)-programmed funding allocated to Marine Corps cybersecurity processes and implementations quarterly to the Marine Corps SISO. The report will include current and planned MCEN cybersecurity investments and will be included in annual budgetary reports from Director C4/DDONCIO (MC) to DoD and DON.

7. Ensure Programs of Record systems and those command networks which they use have an accreditation package developed and submitted to the Marine Corps SISO, or SEO for SCI Systems, for approval. Provide a copy of the final system security documentation via the directed automated Marine Corps C&A Support Tool for accreditation approval before operational deployment of the system in accordance with references (c) through (k) and (t). For UUNS or officially designated urgent requirements, coordinate with the Marine Corps AO no less than 90 days prior to operational deployment to ensure an accreditation approval can be completed within 30 days.

8. Ensure the establishment CMP standards for programs of record across the MCEN. This includes ensuring integrated readiness reviews and compliance processes are in accordance with references (r) through (w).

9. In coordination with DC CD&I, and the DOTMLPF process, ensure appropriate manpower studies are conducted which reflect the addition of IT/cybersecurity personnel required to operate, administer, or maintain a new or expanded information system or network.

10. Integrate cybersecurity engineering practices into pre-Milestone A through Milestone C activities and events as defined in references (h), (i), (k), (q), and (s).

11. Assume responsibility for IT system life cycle management per references (q) through (s).

12. Perform acquisition and life cycle management of materiel in support of the acquisition IA strategy.

13. Adhere to cybersecurity standards for equipment per the DoD IT Standards, the DoDIN cybersecurity architecture, and Marine Corps Single Security Architecture and maintain an systems configuration inventory of each fielded information systems products, equipment, locations, and contact information.

14. Adhere to USCYBERCOM, Marine Corps SISO, and MARFORCYBER patching requirements for all applications that support Programs of Record, by enacting timely IAVM compliance measures (e.g., testing, patching, compliance reporting, and program management). Incorporate them into life cycle management and sustainment procedures to ensure compliance actions are reported to MARFORCYBER through the MCNOSC in accordance with USCYBERCOM task orders.

15. Ensure cryptographic life cycle management is implemented during the system design phase for applicable capabilities.

16. Submit Marine Corps COMSEC POM requirements to support cybersecurity programs to Director C4/DDONCIO (MC) via DC CD&I, for validation and endorsement.

17. Coordinate with the Marine Corps SCI Enterprise Office to ensure SCI systems and capabilities comply with SEO and IC enterprise initiatives.

18. Ensure Program Managers appoint Information System Security Managers (ISSMs) and forward appointment letters to the Marine Corps AO for endorsement.

19. Develop and maintain an Approved Products list and Approved Software List for the MCEN to standardize the Enterprise Network.

(h) Commanding General, Training and Education Command shall:

1. Coordinate with Director C4/DDONCIO (MC) and MARFORCYBER to develop appropriate Military Occupational Specialty (MOS) Training and Readiness (T&R) events that integrate approved cybersecurity tools, doctrine, and TTPs into applicable programs of instruction to meet or exceed validated MCCSP requirements.

2. Incorporate cybersecurity training and education into all pertinent Marine Corps formal schools and distance learning classrooms from entry level training and continuing throughout a Marine's career to meet or exceed validated MCCSP requirements.

3. Coordinate with DC CD&I, Director C4/DDONCIO (MC), and MARFORCYBER to develop and maintain current and timely Marine Corps-wide cybersecurity training literature and training aids that leverage secure electronic distribution and remote access capabilities.

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

1. In conjunction with MARFORCYBER, coordinate with Director C4/DDONCIO (MC) and the Marine Corps SISO regarding the operations and defense of Marine Corps computer systems and networks on the MCEN as directed by the USCYBERCOM.

2. Acquire and field validated materiel solutions in support of defined capability requirements compliant with DoD, DON, and Marine Corps cybersecurity policy and guidance applicable to the particular materiel solutions. The information systems and products will be developed and supported per this Order.

3. Coordinate with Director C4/DDONCIO (MC) and the Marine Corps SISO to ensure MITSCs under MCICOM purview and Marine Corps bases provide persistent enterprise access and credentials for all systems and networks to the C4 ICE DEMons in accordance with 4.a.(3)(b)11 of this Order.

4. Adhere to cybersecurity standards for equipment per the DoD IT Standards, the DoDIN cybersecurity architecture, and Marine Corps Single Security Architecture and maintain an accountability inventory of each of the information systems and their components, locations, and contact information.

5. Adhere to USCYBERCOM, Marine Corps SISO, and MARFORCYBER patching requirements for all applications that support Programs of Record, by enacting timely IAVM compliance measures (e.g., testing, patching, compliance reporting, and program management). Incorporate them into life cycle management and sustainment procedures to ensure compliance actions are reported to MARFORCYBER through the MCNOSC in accordance with USCYBERCOM task orders.

6. Coordinate with DC I&L and establish sustainment support capability for each information system and network assigned at each Marine Corps Base and Station.

(j) Commanding Generals and Commanding Officers shall:

1. Be responsible for cybersecurity practices for all information systems and networks within their purview and to ensure systems' site C&A is in accordance with reference (j).

2. Appoint, in writing, an ISSM for the MCEN and another for the SCI network capabilities within the command. Ensure the ISSM receives applicable certifications in accordance with reference (ag) and can perform required duties. The ISSM functions as the Command focal point and principal advisor for all cybersecurity matters on behalf of the Commander. The ISSM reports to the Commander or appointed representative and implements the overall cybersecurity program within their area of responsibility.

3. Ensure an Information Systems Security Officer (ISSO) is designated, as appropriate, for each information system and network in the organization. Ensure the ISSO receives applicable training in accordance with reference (ag) to carry out their duties. The ISSO acts on behalf of the ISSM to ensure compliance with cybersecurity procedures at the operational site or facility.

4. Ensure all personnel performing privileged user functions (e.g., system administrators, network administrators, and operators) receive initial basic cybersecurity and system specific training as well as annual, refresher, and follow-on cybersecurity training. Ensure that all personnel with privileged user capabilities are certified in accordance with reference (ag).

5. Ensure cybersecurity awareness indoctrination and annual refresher training is conducted and documented down to the user level and is tailored to specific site requirements in accordance with reference (y).

6. Ensure current cybersecurity standard operating procedures are available, used, and updated regularly to include each IT resource.

7. Report as directed all security incidents (e.g., intrusions, malware, breaches, spillages, etc.) and incident suspicions to MARFORCYBER via the MCNOSC or SEO for SCI systems, in accordance with reference (aa). Incident response, handling, and reporting requirements shall be conducted in accordance with reference (y).

8. Review certification documentation for systems under their purview, including UUNS, to evaluate and determine an acceptable level of risk and recommend accreditation to the Marine Corps AO accordingly. Ensure the proper Plan of Actions and Milestones (POA&Ms) are generated for documentation and monitoring purposes.

9. Ensure compliance with Federal, DoD, DON, and Marine Corps information systems and web site administration policies and implement content-approval procedures to minimize the occurrence of cybersecurity, OPSEC, or Personally Identifiable Information (PII) violations in accordance with references (g), (v), and (ab) through (af).

10. Develop a Disaster Recovery/Contingency Plan (DR/CP) in accordance with references (a), (u), and (ad) to ensure recovery and sustainment of information systems and services following an event, incident, or disaster. Provide a copy of the DR/CP for Marine Corps AO signature, as required in reference ff, and maintain annually as required in reference c.

11. Ensure the implementation of a privacy program in accordance with reference (ac) which provides guidance regarding the collection, safeguarding, maintenance, use, access, amendment, and dissemination of PII maintained by DoD, DON, and the Marine Corps in Privacy Act programs and systems of records.

12. Ensure the establishment and implementation of a CMP, consistent with Information Technology Infrastructure Library (ITIL) that includes a CCB for command-owned information systems. Additionally, ensure the local configurations are consistent with command configurations. It is a command responsibility to update the Configuration Management Database (CMDB) and ensure that the Enterprise Configuration Control Board (ECCB) is aware of any system or network issues).

13. Ensure that all information technology users are properly and completely trained on the legitimate and authorized use of systems, have signed user agreements, and have

a valid need to access Marine Corps IT systems per reference (y), (ab)and (aj).

14. Ensure that only validated materiel solutions are acquired in support of defined capabilities compliant with DoD, DON, and Marine Corps cybersecurity policy and guidance applicable to the particular materiel solutions.

(k) Marine Corps Information Systems Security Managers (ISSMs):

1. ISSMs are privileged users, which are defined as individuals who have access to system control, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating system (OS) or computing environment (CE) they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have IT-I security designation. A person with privileged access must have a National Agency Check with Inquiries (NACI) and/or an initiated Single Scope Background Investigation (SSBI) per reference (e) and reference (ar).

2. Establish and manage the cybersecurity program within a command, site, system, or enclave in accordance with DoD, DON, and Marine Corps cybersecurity guidance and policies.

3. Manage the command, site, system, or enclave RMF/DIACAP process to ensure that information systems within their purview are approved, operated, and maintained throughout its life cycle in accordance with the information system’s accreditation package.

4. Serve as the principal advisor to the local G6 for site, system, or enclave cybersecurity matters on behalf of the Marine Corps AO.

5. Assess the cybersecurity program effectiveness and mitigate deficiencies in accordance with the references (e) through (j).

6. Ensure information systems are compliant with the IAVM Program (i.e., IAVAs, and IAVBs) and all

applicable Security Technical Implementation Guide (STIG) in addition to accurate compliance information reporting in accordance with references (e), (y), and (aa).

7. Ensure cybersecurity workforce personnel receive required security training commensurate with their security duties in accordance with reference (ag).

8. Report all issues/concerns regarding POR, CMP, and UUNS via appropriate report chain to the appropriate MARCORSYSCOM program offices, MCNOSC Vulnerability Management Team (VMT), or DC CD&I CDD integration division for resolution.

9. Ensure that security incidents (e.g., malicious code, attacks, intrusions, violations, spillages, PII breaches, etc.) are reported to the MCNOSC DCOS in a timely manner in accordance with references (y) and (aa).

10. Ensure MCNOSC DCOS directed protective/corrective actions are implemented for security incident remediation or mitigation in accordance with the timelines provided, regardless of overtime costs or issues in accordance with references (y), (af), and (al).

11. Serve as an active member of CCBs to affect control and security management of all information systems, devices, configurations, and cybersecurity implementations within their purview.

12. Ensure users and system support personnel have the required security clearances, authorization, and need-to-know, and are indoctrinated on command security practices before granting access to information systems.

13. Report directly to the Marine Corps AO on compliancy requirements.

(l) Marine Corps Information Systems Security Officers (ISSO):

1. ISSOs are privileged users, which are defined as individuals who have access to system control, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating system (OS) or computing environment (CE) they are

required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have IT-I security designation. A person with privileged access must have a NACI and/or an initiated SSBI per reference (e) and reference (ar).

2. Report to the ISSM and ensure an appropriate cybersecurity posture is maintained for a command, site, system, or enclave in accordance with reference (y).

3. Provide direct support to the ISSM for all cybersecurity matters.

4. Assist the ISSM in updating, creating, and reviewing accreditation packages.

5. Enforce system-level cybersecurity controls in accordance with the proper program and policy guidance in accordance with references (e) through (i), and (y).

6. Evaluate risks, threats, and vulnerabilities to determine if additional safeguards are needed to protect the command, site, system, or enclave in accordance with reference (y).

7. Ensure that all information systems and networks within their purview are planned, installed, operated, maintained, managed, and accredited within the security requirements of the information system or network.

8. Develop and issue any additional specific cybersecurity policies, guidance, and instructions as needed.

9. Assist the ISSM in monitoring, reporting, and enforcing the Command, site, system, or enclave IAVM program.

(m) Marine Corps System and Network Administrators (SYSADMIN/NTWKADMIN):

1. SYSADMIN/NTWKADMINs are privileged users, which are defined as individuals who have access to system control, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating system (OS) or computing environment (CE) they are

required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have IT-I security designation. All person with privileged access must have a NACI and/or an initiated SSBI per reference (e) and reference (ar).

2. Monitor user account activity and establish procedures for investigating, deactivating, and deleting accounts that do not show activity over time and report these actions and findings to the ISSM.

3. Provide cybersecurity safeguards and assurances to the data under their control as well as their personal authentication and authorization mechanisms, reporting to the ISSM.

4. Analyze patterns of non-compliance or unauthorized activity and take appropriate administrative or programmatic actions to minimize security risks and insider threats, reporting to the ISSM.

5. Recognize potential security violations, take appropriate action to report the incident as required by regulation, and remediate or mitigate any adverse impact.

6. Implement applicable patches, including IAVAs and IAVBs and critical security updates in a timely manner to avoid potential compromise or loss of functionality.

7. Manage accounts, network rights, and access to information systems and equipment.

8. Configure, optimize, and test hosts (e.g., servers and workstations) and network devices (e.g., hubs, routers, and switches) to ensure compliance with security policy, procedures, and technical requirements.

9. Install, test, maintain, and upgrade operating systems, software, and hardware to comply with prescribed cybersecurity requirements.

10. Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner compliant with system security plans, requirements, and regulations.

11. Perform audit log review on network, systems and applications in accordance with the applicable STIGs.

(n) MCEN Information Systems Users:

1. A user is defined as any military, government civilian, or contractor who has authorized access to the DoDIN or Marine Corps IT resources.

2. Users shall obtain a favorable background investigation and hold a security clearance or access approvals commensurate with the level of information processed or available on the system.

3. Users shall comply with this Order and other cybersecurity directives, policies, and guidance as established by higher headquarters. Supplemental cybersecurity guidance, updates, or revisions will be provided through ECSMs, MARADMIN messages, and MCBULs.

4. Users shall comply with the guidelines established in accordance with reference (y) and submit a DD 2875 System Authorization Access Request (SAAR) along with an Acceptable Use Agreement when using Government-owned information systems. One SAAR is required for NIPR, SIPR, and Joint Worldwide Intelligence Communications System (JWICS) access. The SAAR is good for three years or until the individual is issued a new common access card (CAC). No additional SAAR requirements within the Marine Corps are authorized.

5. Users shall receive cybersecurity indoctrination training and attend annual cybersecurity refresher training in accordance with references (y) and (ab).

6. Users shall mark, label, and safeguard all media, devices, peripherals, and information systems at the security level for which they are intended and in accordance with DoD, DON, and Marine Corps policies and procedures. Dissemination shall only be made to individuals with a valid need to know and clearance level at or above the classification level of the shared media, device, or peripheral in accordance with reference (ap).

7. Users shall protect all media, devices, peripherals, and information systems located in their respective area of responsibility in accordance with physical security and data protection requirements.

8. Users shall practice safe Intranet and Internet operating principles and take no actions that threaten the integrity of the system or network in accordance with reference (ag) and this Order.

9. Users shall report incidents or suspicious events regarding suspected intrusions or unauthorized access; circumvention of security procedures; presence of suspicious files or programs; receipt of suspicious email attachments, files, or links; spillage incidents; and malicious logic (e.g., viruses, trojan horses, worms, spamming, phishing, chain letters, etc.) to the ISSM, ISSO, or SYSADMIN in accordance with reference (aa) and this Order.

10. Users shall report the receipt or discovery of unfamiliar or unauthorized removable media (e.g., CD-ROM, thumb drives, external hard drives, etc.) to the ISSM, SYSADMIN, or NTWKADMIN in accordance with in accordance with reference (aa), applicable directives, and this Order.

11. User shall use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the information system.

12. Users shall report suspicious, erratic, or anomalous information systems operations; missing or added files; and non-approved services or programs to the SYSADMIN or NTWKADMIN in accordance with local policy and cease operations on the affected information system until authorized to start operations again by higher authority in accordance with reference (aa), applicable directives, and this Order.

13. Users shall comply with cryptographic log-in requirements and password or pass-phrase policy directives, and protect information systems from unauthorized access in accordance with references (y), (am), and this Order.

14. Users shall logoff and secure the information system and work environment (i.e., secure For Official Use Only [FOUO]/Controlled Unclassified [CUI] media, remove CAC, etc.) at the end of each workday or when out of the immediate area in accordance with references (y), (am), (ap), and this Order.

15. User shall access only data, controlled information, software, hardware, and firmware for which they are

authorized access and have a need to know. Assume only authorized roles and privileges.

16. Users shall ensure government-provided and installed cybersecurity products (e.g., anti-virus, virtual private networks [VPNs], personal firewalls, etc.) will not be altered, circumvented, or disabled on Marine Corps information systems.

17. Users are encouraged to install and update authorized Government-provided cybersecurity products (e.g., AV, VPNs, personal firewalls, etc.) on personal systems as required by the Marine Corps AO for approved remote access.

18. Users shall digitally sign and encrypt all sensitive information on external media or in email exchanges, using Federal Information Processing Standard (FIPS) 140-2 validated encryption (e.g., DoD CAC, DoD Alternate Token). Such information includes marked FOUO/CUI information, financial data, contract related information, health information, personally identifiable information, network or technical diagrams with identifiable labels (e.g., IP addresses) or other information that may have an operational security impact if compromised.

(o) Prohibited Activities. The following activities are specifically and expressly prohibited:

1. Users will not use any personally owned devices on the MCEN, or use official Government information systems for commercial gain or conduct illegal activities or in any manner that interferes with official duties, undermines readiness, reflects adversely on the Marine Corps, or violates standards of ethical conduct.

2. Users will not intentionally send, store, or propagate sexually explicit, threatening, harassing, prohibited partisan political, or unofficial public (e.g., “spam”) communications.

3. Users will not participate in on-line gambling or other activities inconsistent with public service.

4. Users will not participate in, install, configure, or use unauthorized peer-to-peer (P2P) technologies.

5. Users will not release, disclose, or alter information without the consent of the data owner, the original

classification authority (OCA), the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Officer (PAO), or the disclosure officer's approval.

6. Users will not attempt to strain, test, circumvent, or bypass security mechanisms, perform unauthorized network line monitoring or keystroke monitoring, share personal accounts and passwords, or allow remote access to non-privileged users.

7. Users will not modify system or software, use it in any manner other than its intended purpose, introduce malicious software or code, add user-configurable or unauthorized software, disable or remove security or protective software or mechanisms, or misuse/abuse a privileged account.

8. Users will not relocate or change information system equipment or information system equipment, or change network connectivity without proper security authorization.

9. Users will not acquire commercial or unauthorized internet service provider (ISP) network access into Marine Corps operational facilities, or implement commercial wireless components (e.g., access points, base stations, clients, etc.) without approval from the Marine Corps AO.

10. Users will not use wireless technologies for storing, processing, and transmitting unclassified information in areas where classified information is discussed, stored, processed, or transmitted without the express written consent of the Marine Corps AO.

11. Users will not auto forward email from government accounts to commercial ISP email services, engage in the creation or forwarding chain mail, or open email attachments or internet links received from unknown sources.

12. Users will not use removable secondary storage media on government IS without prior written approval from the G-6. This includes, but is not limited to: removable flash media, thumb drives, smartphones, camera memory cards, and external hard disk drives, or any device that is capable of being inserted into and removed from an IS that can store data.

13. Users will not connect any IS to a network of higher or lower classification than the IS's own classification level, commonly known as a cross domain violation, without using an approved cross domain solution.

14. Users shall not introduce classified information onto an IS of a lower classification level, commonly known as a spillage, or expose personally identifiable information to unauthorized recipients, commonly known as a breach.

b. Coordinating Instructions

(1) Military users in violation of DoD, DON, and Marine Corps cybersecurity policies and procedures may be subject to disciplinary actions under the Uniform Code of Military Justice (UCMJ), Federal, or State criminal statutes and laws.

(2) Violation of this Order by government or contractor civilian personnel may result in personnel actions under 5 CFR 2635.101(b)(9) and (14), the Federal Acquisition Regulation (FAR), or referral of criminal violations to appropriate civilian authorities.

5. Administration and Logistics

a. This Order shall not alter or supersede existing authoritative policies issued by the ODNI regarding the protection of SCI and special access programs (SAPs) for intelligence. The application of the provisions and procedures of this Order to SCI or other intelligence information systems is encouraged where they may complement or address areas not otherwise specifically identified.

b. Detailed cybersecurity practices and procedures supporting this Order will be published and released by Director C4/DDONCIO (MC), or HQMC I/SEO (for SCI systems).

c. Recommendations for changes to this Order should be submitted to HQMC C4 via the appropriate chain of command.

d. All developers, owners, and users of information systems and applications within MCEN have the responsibility to establish and implement adequate operation and information technology controls including records management requirements to ensure the proper maintenance and use of records, regardless of

format or medium, to promote accessibility and authorized retention per the approved records schedule and reference (ao).

e. No additional restrictions or limitations are authorized. Further restrictions to any parts of this Order require the express permission of the Director C4/DDONCIO (MC).

f. Records created as a result of this Order shall be managed according to National Archives and Records Administration approved dispositions per reference (ao) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium.

g. The generation, collection, or distribution of PII, and management of privacy sensitive information shall be in accordance with the Privacy Act of 1974, as amended, per reference (ab). Any unauthorized review, use, disclosure, or distribution is prohibited.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps to include Marine Corps Reserves and any personnel employed by or in support of Marine Corps Total Force System.

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

D. A. CRALL
Director, Command, Control,
Communications, and Computers

DISTRIBUTION: PCN 10207719100

DEFINITIONS

Authorizing Official (AO) - 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). (Reference CNSSI 4009)

Configuration Control Board (CCB) - The purpose of the CCB is to ensure each proposed change to an item's performance or physical characteristics is thoroughly evaluated with respect to technical, logistics, cost, and schedule impacts and benefits. Review and input by the CCB allows the approval authority to make sound, informed management decisions. (Reference CNSSI 4009)

Configuration Management Database (CMDB) – A database that contains relevant details (e.g., settings, firmware revisions,

etc.) of Configuration Items (CIs) and the relationships between them. For example, information about a network switch might include the software release installed on it, and the servers that connect directly to it, all of which would also be CIs. (Reference ITIL Version 2.0)

Configuration Management Program (CMP) – Applies appropriate processes and tools to establish and maintain consistency between the product and the product requirements and attributes defined in product configuration information. Configuration Management shall be applicable to all hardware, software, and firmware items and associated documents. A disciplined CM process ensures that products conform to their requirements and are identified and documented in sufficient detail to support the product life cycle. (Defense Acquisition Guidebook)

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. (Reference CNSSI 4009 and NIST IR 7298.)

Cybersecurity – Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoD Instruction 8500.01)

Cybersecurity Steering Group (CSSG) – Established under the C4 OAG to facilitate the timely formulation of security solutions to meet current and future force objectives. The CSSG will address, mitigate, and validate security issues in order to protect the Marine Corps to an acceptable level. Core members of the CSSG include HQMC C4, MARCORSYSCOM, MARFORCYBER, DC CD&I, MCOTEA, Marine Corps TECOM, Marine Corps Intelligence Activity (MCIA), and Marine Corps Community Services (MCCS).

Enterprise Configuration Control Board (ECCB) - The ECCB exists to approve or otherwise act on Requests for Change (RFC) to established or nominated configuration items that operate within the MCEN. RFCs may contain a range of capabilities from minor changes to major system projects. It will be the concern of the ECCB to enforce good practices, enforce DoD, DON, and Marine Corps standards and accepted industry methodologies when considering configuration changes.

Identity Assurance – The capability to affix, verify, and/or determine the identity of a person (living, deceased, unconscious, non-functioning, uncooperative, or unaware), an organization, or other entity. Identity Assurance can facilitate intelligence collection, targeting, combat identification, and analysis on individuals, groups, and their activities. It can also be referenced as part of Supply Chain Protection. (Reference NIST SP 800-63.)

Information Systems - These include, but are not limited to, computers, processors, devices, or environments (operating in a prototype, test bed, training, stand-alone, integrated, embedded, or networked configuration) that receive, process, store, display, or transmit government or government supporting information, regardless of mission assurance category, sensitivity or classification, with or without handling codes and caveats. This includes information systems used for teleworking and telecommuting; contractor owned or operated information systems residing on the MCEN; information systems obtained with Non-Appropriated Funds; UUNS, automated tactical systems; automated weapons systems; platform information technology; and distributed computing environments. Systems processing intelligence information are required to adhere to the provisions of this Order. (Reference CNSSI 4009)

Information Systems Security Manager (ISSM) - The roles and responsibilities of the Information Systems Security Manager, as referenced in this document, are aligned to the roles and responsibilities of the DoDD 8500.01 and DoDI 8510.01 Information Assurance Manager and the CJCSI 6510.01F Information Systems Security Manager. This term has replaced IAM. (Reference CNSSI 4009)

Information Systems Security Officer (ISSO) - The roles and responsibilities of the Information Systems Security Officer, as referenced in this document, are aligned to the roles and responsibilities of the DoDI 8500.2 Information Assurance

Officer and the CJCSI 6510.01F Information Systems Security Officer. This term has replaced IAO. (Reference CNSSI 4009)

Marine Corps Certification and Accreditation Process (MCCAP) - Marine Corps Enterprise Cybersecurity Directive 018, 12 July 2012, established the MCCAP to provide a comprehensive and uniform approach to the certification and accreditation process for the Marine Corps, to include all subordinate commands, bases, and organizations.

MCEN – Marine Corps network-of-networks and approved interconnected network segments supporting the Marine Corps Command, Control, and business process communications. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate according to Marine Corps policy. The MCEN is both, the Marine Corps Enterprise Network - NIPRNet (MCEN-N) and the Marine Corps Enterprise Network - SIPRNet (MCEN-S); however, this document will refer to both networks as one MCEN.

Marine Corps Intelligence, Surveillance, Reconnaissance – Enterprise (MCISR-E) – The MCISR-E is a framework to develop an ISR enterprise to meet the specified and implied tasks identified in the Marine Corps Service Campaign Plan.

Marine Corps SCI Enterprise Office (SEO) - The SEO administers and operates the Marine Corps SCI Enterprise by providing policy implementation, governance, technical support, and assistance in establishing and sustaining Marine Corps SCI activities. The SEO coordinates strategic and enterprise initiatives in support of MCISR-E to meet operational requirement for Distributed Operations, Net-Centric Operations, Interoperability, Enterprise Architectures, Service-oriented Architecture, and Information Management. The SEO provides Enterprise Management, Network Operations, Network Security, Information Assurance and Asset Management across the Marine Corps in accordance with relevant directives and guidance from the ODNI, Department of Defense Intelligence Information Systems (DoDIIS), DIA, and NSA.

Marine Corps Web Risk Assessment Cell (MCWRAC) - The MCWRAC conducts Web Risk Assessments of Marine Corps organizational web sites to identify OPSEC and Cybersecurity vulnerabilities, issues, and/or concerns. The MCWRAC mission is to ensure that publicly accessible, non-restricted, Marine Corps World Wide Web sites are protected against malicious activities intended to deny, degrade, or disrupt public access to Marine Corps web sites or modify the content in any way.

Point of Presence (POP) - A demarcation point or interface point between network or communications entities. (Reference CJCSI 6211.02D.)

Ports, Protocols, and Services Management (PPSM) - Are the different processes utilized to move data across the network. The management of them will help to improve both the interoperability of joint applications, systems, and the security of the overall DoD information infrastructure. (Reference DoDI 8551.01)

Vulnerability Management Team (VMT) – The primary reporting agent within the MCNOSC designated to manage the Marine Corps vulnerability management programming support of the USCYBERCOM and DoD IAVM program. The VMT is responsible to maintain access and administration of the Marine Corps Vulnerability Management System (VMS) and ensure dissemination or availability of IAVM notifications for personnel responsible for implementing and managing responses to information system vulnerabilities.

ACRONYMS

AO	Authorizing Official
AV	Anti-Virus
C4	Command, Control, Communications, and Computers
C&A	Certification and Accreditation
CAC	Common Access Card
CCB	Configuration Control Board
CD&I	Combat Development and Integration
CDS	Cross Domain Solution
CI	Counter Intelligence
CIO	Chief Information Officer
CMC	Commandant of the Marine Corps
CMDB	Configuration Management Database
CMP	Configuration Management Program
CND	Computer Network Defense
CNSS	Committee on National Security Systems
COCOM	Combatant Command
COMSEC	Communication Security
COTS	Commercial Off the Shelf
CSSG	Cybersecurity Steering Group
CYBERCON	Cybersecurity Condition
DAA	Designated Accrediting Authority
DC PP&O	Deputy Commandant Plans, Policy, and Operations
DCO	Defensive Cyberspace Operations
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIRINT	Director of Intelligence
DISN	Defense Information Systems Network
DITPR-DON	Department of Defense Information Technology Portfolio Repository Department of the Navy
DITS	Digital Integrated Transport Suites
DoD	Department of Defense
DoDIN	Department of Defense Information Network
DON	Department of the Navy
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities
DR/COOP	Disaster Recovery/Continuity of Operations Plan
DSAWG	Defense/Information Assurance Security Accreditation Working Group
ECCB	Enterprise Configuration Control Board
ECSM	Enterprise Cybersecurity Manual
EIAD	Enterprise Information Assurance Directive
EKMS	Electronic Key Management System

ESSG	Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GOTS	Government Off the Shelf
IA	Information Assurance
IASG	Information Assurance Steering Group
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection System
IGMC	Inspector General of the Marine Corps
IO	Information Operations
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JCIDS	Joint Capabilities Integration Development Systems
JKMIWG	Joint Key Management Infrastructure Working Group
KMEC	Key Management Executive Committee
KMI	Key Management Infrastructure
LE	Law enforcement
MAIS	Major Automated Information System
MARADMIN	Marine Corps Administrative Messages
MARCERT	Marine Corps Computer Emergency Response Team
MARFOR	Marine Forces
MARFORCYBER	Marine Corps Forces Cyber Command
MARCORSYSCOM	Marine Corps Systems Command
MCBUL	Marine Corps Bulletin
MCCAP	Marine Corps Certification and Accreditation Process
MCCAT	Marine Corps Cyber Assessment Team
MCCSP	Marine Corps Cybersecurity Program
MCEN	Marine Corps Enterprise Network
MCISR-E	Marine Corps Intelligence, Surveillance, Reconnaissance – Enterprise.
MCNOSC	Marine Corps Network and Operations Security Center
MDAPS	Mandatory Procedures for Major Defense Acquisition Programs
MDID	Market-Driven/Industry-Developed
MOS	Military Occupational Specialty

MWRAC	Marine Corps Web Risk Assessment Cell
NAS	Naval Audit Service
NCIS	Naval Criminal Investigative Service
NCMS	Naval Communications Security Management Service
NETOPS	Network Operations
NIST	National Institute of Standards and Technology
NTWKADMIN	Network Administrator
NSA	National Security Agency
OAG	Operational Advisory Group
OCA	Original Classification Authority
ODNI	Office of the Director of National Intelligence
OCO	Offensive Cyber Operations
OPSEC	Operations Security
P2P	Peer to Peer
PAO	Public Affairs Officer
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
POP	Point of Presence
POR	Program of Record
PM	Program Manager
PPSM	Ports, Protocols, and Services Management
RMF	Risk Management Framework
RDT&E	Research, Development, Test, and Evaluation
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SEO	Sensitive Compartmented Information (SCI) Enterprise Office
SISO	Senior Information Security Officer
SISS	Subcommittee for Information Systems Security
STIG	Security Technical Information Guidelines
ST&E	Security, Test, and Evaluation
STS	Subcommittee for Telecommunications Security
SYSADMIN	Systems Administrator
T&R	Training and Readiness
TTP	Tactics, Techniques, and Procedures
UCMJ	Uniform Code of Military Justice
USCYBERCOM	United States Cyber Command
UUNS	Urgent Universal Needs Statement
VMT	Vulnerability Management Team
VPN	Virtual Private Network

APPPENDIX A

MARINE CORPS COMMAND CYBER READINESS INSPECTION (CCRI) PREPARATION PROCESSES AND REQUIREMENTS

A.1. This appendix is to outline the process used to assess cyber security readiness at specified service organizations. These processes will serve to inform service organizations of their requirements and responsibilities and to define the end goal of these processes which is a successful completion of both the scheduled CCRI and corrective/remediation actions required in order to preserve and maintain the Marine Corps C2.

Listed below are the responsibilities and tasks for the named organizations with regard to the CCRI process.

A.2. MARFORCYBER

(1) Notify subordinate commands to be inspected of CCRI and CCRI tasking.

(2) Participate in pre-CCRI, final coordination brief, and Defense Information Systems Agency (DISA) CCRI SVTCs out briefs.

(3) Conduct analysis of CCRI results to include Category (CAT) I, II, and III findings, overall scores (pre/actual), and trends.

(4) Track status of post CCRI deliverables (through completion), including, (1) risk assessment plan, (2) after action plan, and (3) mitigation of CAT I, II, and III findings.

A.3. MCNOSC

(1) Provide inspected commands with technical support and review of DISA required CCRI documents (scoping document, architecture diagrams, site accreditation documentation, etc.).

(2) Provide sites with subject matter expert for host based security system secure configuration guidance.

(3) Perform analysis of weekly site vulnerability scan files and provide sites with a detailed vulnerability report.

(4) Upon receipt of requests create VMS user accounts.

(5) Within two business days of DISA CCRI out-brief release site specific MCEN direct tasking message (MDTM) detailing required post CCRI requirements with nlt completion dates.

(6) Participate in Pre-CCRI, final coordination brief, and DISA CCRI SVTCS out briefs.

A.4. HQMC C4 CY

(1) No Later Than (NLT) 90 Days Prior To Inspection, Coordinate Pre-CCRI Inspection Scheduling And Execution (conducted NLT 60 Days prior to the DISA CCRI Date).

(2) Conduct Pre-CCRI inspections to identify current network configuration, accreditation, security readiness, traditional and physical security, and compliance with Department Of Defense (DoD) policies and regulations.

(3) NLT 75 days prior to the CCRI, approve and submit to DISA DoD Information Network Readiness Inspections, CCRI Branch all CCRI scoping documents submitted from inspected commands. Scoping documents identify detailed configuration, Internet Protocol (IP) space, topology and layout of the circuit(s) to be inspected.

(4) Conduct reviews of the effectiveness of other technical security policies as required, recommend or direct changes, and provide insight into operational readiness.

(5) As the service lead for CCRI, participate in pre-CCRI, final coordination brief, and DISA CCRI Secure Internet Protocol Routing Network Video Telecommunications Conference (SVTC) out briefs.

A.5. Marine Forces Command. Notify subordinate commands to be inspected of CCRI dates and CCRI taskings.

A.6. Marine Forces Pacific. Notify subordinate commands to be inspected of CCRI dates and CCRI taskings.

A.7. Marine Corps Installation Command. Notify subordinate commands to be inspected of CCRI dates and CCRI taskings.

A.8. Marine Forces Reserve. Notify subordinate commands to be inspected of CCRI dates and CCRI taskings.

A.9. Marine Corps Recruiting Command. Notify subordinate commands to be inspected of CCRI dates and CCRI taskings.

A.10. Inspected Commands. Commanders, working with the G-3, G-6, and security personnel must meet the following requirements:

(1) NLT 90 Days Prior To CCRI date perform the following actions:

(a) Provide the inspection primary point of contact (POC) info to message POCs. Include POC rank (Military Or Civilian), Full Name, Commercial Phone Number, Unclassified E-Mail Address, And Classified E-Mail Address.

(b) Submit All CCRI related correspondence and deliverable documents (i.e., scoping document, architecture diagrams, site accreditation documentation, etc.) to HQMC C4 CY Assessments Branch and carbon copy (ac) the MCNOSC VMT Operational Mail Box (OMB).

(2) NLT 75 Days Prior to CCRI date perform the following actions:

(a) Identify at least (1) and not more than (4) personnel that will require VMS user accounts. Submit a completed SAAR DD 2875 and current copies of Information Assurance and Privacy Identifiable Information training completion certificates (no older than one year at time of submission) to the HQMC C4 CY Assessments Branch and cc MCNOSC VMT OMB.

(b) Submit network(s) to be inspected IP space (to generate coverage) and subnet coverage queries to the MCNOSC and cc the VMT OMB.

(c) Submit current all audit/vulnerability scan files to the MCNOSC VMT for each network classification to be inspected. Continue to provide the MCNOSC VMT with updated vulnerability scan each week thereafter up to the actual DISA CCRI inspection date.

At the conclusion of the Pre-CCRI conducted by HQMC C4 CY, all commands will receive guidance on the allowed reduction of online assets for the CCRI. Commands will not exceed seven percent decrease of online assets for the CCRI.

(3) NLT 30 days prior to inspection date:

(a) Provide the MCNOSC VMT with either a POA&M or a waiver request for any CAT I Vulnerability that cannot be remediated.

(b) Provide the MCNOSC VMT with a POA&M or MCEN AO approved waiver for any CAT II or III vulnerability that cannot be mitigated.

(4) NLT 14 days prior to the inspection date:

(a) Provide MARFORCYBER And HQMC C4 CY with a final coordination brief status of all Pre-CCRI out brief findings. Commands are to identify Pre-CCRI findings which have and have not been remediated.

(b) The command must report all online assets and compare that number with the Pre-CCRI online asset number. If there is a difference of seven percent between the two numbers, the command must provide justification for all assets.

(5) NLT 14 working days **POST** DISA CCRI:

Comply with all MCNOSC site specific MDTM requirements through completion. MCNOSC MDTMS will be released within two business days after the DISA CCRI out brief.
Participate in Pre-CCRI, Final Coordination Brief, and DISA CCRI SVTC Out Briefs.