UNITED STATES MARINE CORPS
MARINE CORPS RECRUIT DEPOT/EASTERN RECRUITING REGION
PO BOX 19001
PARRIS ISLAND, SOUTH CAROLINA 29905-9001

IN REPLY REFER TO:
DepO 5239.2
G-6
3 DEC 2014

DEPOT ORDER 5239.2

From: Commanding General
To: Distribution List

Subj: MARINE CORPS RECRUIT DEPOT PARRIS ISLAND (MCRDPI) CYBER SECURITY PROGRAM (PICSP)

Ref: (a) MCO 5239.2A
(b) DoD 8570.01M

1. Situation. Due to the increasing threat of cyber-based attacks, personnel aboard Marine Corps Recruit Depot, Parris Island, SC (MCRDPI), herein referred to as "the Depot", must be made aware of how commonly used Information Technology (IT) resources can be compromised and how to mitigate this risk. HQMC C4I has produced reference (a), introducing an enterprise level solution to the security of the Marine Corps Enterprise Network (MCEN). This order reinforces and expands upon reference (a) in order to tailor its instructions to the mission and capabilities of the Depot. At no time will this order supersede the references in the case of conflicting instructions or information, the references are to be considered the authority.

2. Mission. In accordance with references, this order will implement a local cyber security policy to ensure the protection and defense of the MCEN, and the information residing on it.

3. Execution

a. Commander's Intent. PICSP mission success will be accomplished by employing a comprehensive cyber security program designed to protect and defend the MCEN and the information residing on the MCEN, to ultimately support the Commander's information needs. In accordance with the references, the PICSP aims to improve efforts to effectively manage and monitor network and system activities, particularly in regards to new IT technologies. The Depot must employ a cyber security capability that supports robust network security practices to improve cyber security implementation and situational awareness across the MCEN. The PICSP will incorporate proactive protection, detection, reaction, disaster recovery, and restoration

capabilities to include the detection of, reporting on, and countermeasures against unauthorized activities. Concurrently, the effectiveness of cyber security programs, policies, and procedures will be reviewed by means of established procedures.

b. Concept of Operations. The Depot will adopt an information system life-cycle management approach in applying uniform standards for the protection of IT resources that display, transact, transmit, or receive information. The Depot will iteratively assess threats, vulnerabilities, risks, and a spectrum of cyber security practices to identify, document, and implement appropriate countermeasures to effectively mitigate risks to an acceptable operational level.

c. Required Actions

(1) Assistant Chief of Staff (AC/S) G-6

(a) Be responsible for cyber security practices for all information systems and networks within their purview, and to ensure systems' site certification and accreditation (C&A) is in accordance with the references.

(b) Appoint, in writing, an Information Systems Security Manager (ISSM) for the Depot. Ensure the ISSM receives applicable certifications in accordance with the references and can perform required duties. The ISSM reports to, and functions as the Depot's focal point and principal advisor for all cyber security matters on behalf of, the AC/S G-6, and implements the overall cyber security program for the Depot.

(c) Appoint, in writing, an Information Systems Security Officer (ISSO) for the Depot. Ensure the ISSO receives applicable certifications in accordance with the references and can perform required duties. The ISSO acts on behalf of the ISSM to ensure compliance with cyber security procedures aboard the Depot.

(d) Ensure all personnel performing privileged user functions that have cyber security impacts (e.g., system administrators and network administrators) receive initial basic cyber security and system specific training as well as annual, refresher, and follow-on cyber security training. Ensure that all personnel with privileged user capabilities are certified in accordance with the references.

(e) Ensure cyber security awareness indoctrination, and annual refresher, training is conducted and documented down to the user level.

(f) Ensure current cyber security standard operating procedures are available and updated regularly.

(g) Report as directed all security incidents (e.g., intrusions, malware, spillages, etc.) and incident suspicions to the Marine Corps Network Operations and Security Center (MCNOSC) in accordance with reference (a). Incident response, handling, and reporting requirements shall also be conducted in accordance with reference (a).

(h) Ensure compliance with Federal, Department of Defense (DoD), Department of the Navy (DoN), and Marine Corps information systems and web site administration policies and implement content-approval procedures to ensure that no cyber security, operational security, or Personally Identifiable Information (PII) violations occur in accordance with reference (a).

(i) Develop a Disaster Recovery/Continuity of Operations Plan (DR/COOP) in accordance with reference (a) to ensure recovery and sustainment of information systems and services following an event, incident, or disaster.

(j) Ensure the implementation of a privacy program in accordance with reference (a) 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.

(k) Ensure the establishment and implementation of a Configuration Management Program (CMP), consistent with Information Technology Infrastructure Library (ITIL) that includes a Configuration Control Board (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).

(l) Ensure that all IT users are appropriately trained on the legitimate and authorized use of systems, have

signed user agreements, and have a valid need to access Marine Corps IT systems.

(m) Ensure that only validated material solutions are acquired in support of defined capabilities compliant with DoD, DoN, and Marine Corps Cyber Security Policy and guidance applicable to the particular material solutions.

(2) Information Systems Security Manager

(a) Establish and manage the Cyber Security Program within a command, site, system, or enclave in accordance with DoD, DON, and Marine Corps Cyber Security guidance and policies.

(b) Manage the command, site, system, or enclave C&A process to ensure that information systems within their purview are approved, operated, and maintained throughout their life cycle in accordance with the information system's accreditation package.

(c) Serve as the principal advisor to the commander for site, system, or enclave cyber security matters.

(d) Assess the cyber security program effectiveness and mitigate inefficiencies in accordance with reference (a).

(e) Ensure information systems are compliant with the Information Assurance Vulnerability Management (IAVM) Program (i.e., Information Assurance Vulnerability Alerts (IAVAs), and Information Assurance Vulnerability Bulletins (IAVBs)) and all applicable Security Technical Implementation Guides (STIGs) in addition to accurate compliance information reporting in accordance with reference (a).

(f) Ensure cyber security workforce personnel receive required security training commensurate with their security duties in accordance with the references.

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

(h) Ensure that security incidents (e.g., malicious code, attacks, intrusions, violations, spillages, etc.) are reported to MARCERT in a timely manner in accordance with reference (a).

(i) Ensure MARCERT directed protective/corrective actions are implemented for security incident remediation or mitigation.

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

(3) Information Systems Security Officer

(a) Report to the ISSM and ensure an appropriate cyber security posture is maintained for a command, site, system, or enclave.

(b) Provide direct support to the ISSM for all cyber security matters.

(c) Assist the ISSM in updating, creating, and reviewing accreditation packages.

(d) Enforce system-level Information Assurance (IA) controls in accordance with the proper program and policy guidance.

(e) Evaluate risks, threats, and vulnerabilities to determine if additional safeguards are needed to protect the command, site, system, or enclave.

(f) 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.

(g) Develop and issue any additional specific cyber security policies, guidance, and instructions as needed.

(h) Assist the ISSM in monitoring, reporting, and enforcing the command, site, system, or enclave IAVM program.

(4) System and Network Administrators

(a) Monitor user account activity and establish procedures for investigating, deactivating, and deleting accounts that do not show activity over a 120 day period.

(b) Provide cyber security safeguards and assurances to the data under their control as well as their personal authentication and authorization methods.

(c) Analyze patterns of non-compliance or unauthorized activity and take appropriate administrative or programmatic actions to minimize security risks and insider threats.

(d) Recognize potential security violations, take appropriate action to report the incident as required by reference (b), and remediate or mitigate any adverse impact.

(e) Implement applicable patches, including IAVAs and IAVBs and critical security updates in a timely manner to avoid potential compromise or corruption.

(f) Manage accounts, network rights, and access to information systems and equipment.

(g) 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.

(h) Install, test, maintain, and upgrade operating systems, software, and hardware to comply with prescribed cyber security requirements.

(i) 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.

(j) Perform audit log review on network systems and applications in accordance with the applicable STIGs.

(5) MCEN Users

(a) A user is defined as any military, government civilian, or contractor who has authorized access to the Global Information Grid (GIG) or Marine Corps IT resources.

(b) Obtain a favorable background investigation and hold a security clearance or access approvals commensurate with the level of information processed or available on the IT system.

(c) Comply with this order and other cyber security directives, policies, and guidance as established by higher headquarters. Supplemental cyber security guidance, updates, or revisions will be provided through Enterprise Information Assurance Directives (EIADs)/Enterprise Cyber Security Directives (ECSDs), Marine Administration (MARADMIN) messages, and Marine Corps Bulletins (MCBUL).

(d) Comply with the guidelines established in accordance with reference (a) and submit a DD 2875 System Authorization Access Request (SAAR) along with an Acceptable Use Agreement when using government-owned information systems. Receive cyber security indoctrination training and attend annual cyber security refresher training in accordance with reference (a).

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

(f) Protect all media, devices, peripherals, and information systems located in their respective AOR in accordance with physical security and data protection requirements.

(g) Practice safe Intranet and Internet operating principles and take no actions that threaten the integrity of the system or network in accordance with this order.

(h) 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 or ISSO.

(i) Report the receipt or discovery of unfamiliar or unauthorized removable media (e.g., CD-ROM, floppy disk, thumb drives, external hard drives, etc.) to the ISSM or ISSO in accordance with applicable directives.

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

(k) Report suspicious, erratic, or anomalous information systems operations; missing or added files; and unapproved services or programs to the ISSM or ISSO in accordance with this order, and cease operations on the affected information system until authorized to start operations again by higher authority.

(l) Comply with cryptographic log-in requirements and password or passphrase policy directives, and protect information systems from unauthorized access.

(m) Lock or logoff the information system (e.g., secure For Official Use Only (FOUO) media, remove and take Common Access Card (CAC), etc.) at the end of each workday or when out of the immediate area.

(n) Access only data for which they are authorized access and have a need-to-know.

(o) Government-provided and installed cyber security products (e.g., anti-virus, virtual private networks (VPNs), personal firewalls, etc.) will not be altered, circumvented, or disabled on Marine Corps information systems.

(p) Authorized government-provided cyber security products (e.g., AV, VPNs, personal firewalls, etc.) are available and encouraged to be installed and updated on personal systems as required for approved remote access.

(q) Prohibited activities. The following activities are specifically prohibited and users will not:

1. Use official government information systems for commercial gain or to conduct illegal activities.

2. Use information systems in any manner that interferes with official duties, undermines readiness, reflects adversely on the Marine Corps, or violates standards of ethical conduct.

3. Intentionally send, store, or propagate sexually explicit, threatening, harassing, prohibited partisan political, or unofficial public (e.g., "spam") communications.

4. Participate in online gambling or other activities inconsistent with public service.

5. Participate in, install, configure, or use unauthorized peer-to-peer (P2P) technologies.

6. Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA), the individual's chain of command, Freedom of Information Act (FOIA) official, Public Affairs Officer (PAO), or the disclosure officer's approval.

7. Attempt to strain, test, circumvent, or bypass security mechanisms; perform network line monitoring; or keystroke monitoring.

8. Modify system or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (e.g., unauthorized instant messaging, P2P applications).

9. Relocate or change information system equipment or network connectivity without proper security authorization.

10. Share personal accounts and passwords, or allow remote access to non-privileged users.

11. Disable or remove security or protective software or mechanisms.

12. Acquire commercial or unauthorized internet service provider (ISP) network access into Marine Corps operational facilities without approval from the Marine Corps Approving Official (AO).

13. Implement commercial wireless components (e.g., access points, base stations, clients, etc.) without approval from the Marine Corps AO.

14. 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.

15. Auto forward email from government accounts to commercial ISP email services; engage in the creation or forwarding chain email; or open email attachments or internet links received from unknown sources.

(6) Coordinating Instructions

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

(b) 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.

(c) Establish a comprehensive program to implement, document, and manage a standard CMP across the MCEN for all non-POR systems.

(d) Ensure Marine Corps networks are Public Key enabled in accordance with reference (a) and USCYBERCOM directives.

4. Administration and Logistics

a. Detailed cyber security practices and procedures supporting the PICSP will be published and released by the G-6.

b. Recommendations for changes to this order should be submitted to the G-6 via the appropriate chain of command.

c. All developers, owners, and users of information systems and applications within the MCEN have the responsibility to establish and implement adequate operational and IT 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 (a).

d. Further restrictions to any parts of this order require the express permission of the G-6.

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

5. Command and Signal

a. Command. This order is applicable to all MCRD Parris Island personnel.

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

M. R. BOWERSOX
Chief of Staff