UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CALIFORNIA 92278-8100

CCO 5239.2E
G-6
DEC 1 2 2024

COMBAT CENTER ORDER 5239.2E

From: Commanding General
To: Distribution List

Subj: CYBERSECURITY

Ref: (a) MCO 5239.2B
(b) CCO 2620.1C
(c) MARADMIN 330/16

Encl: (1) Listing of Marine Corps Enterprise Cybersecurity Manuals

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 can 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), as well as, any other network employed in support of training and installation operations.

c. The Marine Corps Sensitive Compartmented Information (SCI) networks and systems are protected under the Marine Corps Director of Intelligence 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 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, Defense Intelligence Agency and the National Security Agency.

d. 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 to information systems that may potentially lead to mission failure. Detailed Cybersecurity actions are distributed separately by the Marine Air Ground Task Force Training Command (MAGTFTC), Marine Corps Air Ground Combat Center (MCAGCC) Information System Security Manager (ISSM).

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

2. Cancellation. CCO 5239.2D.

3. Mission. Implement Cybersecurity on Communications and Information Systems (CIS) and Information Technology (IT) resources procured, developed, operated, maintained, or managed at MAGTFTC, MCAGCC. Cybersecurity policy, procedures, tasks, conditions, and standards will be distributed by the MAGTFTC, MCAGCC ISSM in accordance with reference (a). Supplemental cybersecurity guidance, updates, or revisions will be provided through Enterprise Cybersecurity Manuals (ECSMs), Marine Administration (MARADMIN) messages, and Marine Corps Bulletins (MCBUL).

4. Execution. Per the references, MAGTFTC, MCAGCC will adopt a "life cycle management" approach in applying uniform standards for the protection of United States Marine Corps IT resources that produce, process, store, or transmit information. The MAGTFTC, MCAGCC Cybersecurity team will also assess threats, vulnerabilities, and their associated risks to identify appropriate countermeasures to effectively reduce risks to an acceptable operational level. Those that procure or develop information systems will ensure, through certification of technical features, that all information systems under their functional area, sponsorship, or direction are developed, acquired, and managed in accordance with the provisions of this Order. Furthermore, commanders will identify all information systems within their purview and will be accountable for the Assessment and Authorization of these systems.

a. Commander’s Intent and Concept of Operations

(1) Commander’s Intent

(a) Develop a cybersecurity capability that supports a robust infrastructure-wide defense in depth strategy.

(b) Establish procedures for reviewing the effectiveness of local cybersecurity programs and policies in accordance with directions from the ISSM.

(c) Establish a comprehensive framework for security controls over information resources.

(d) Conduct periodic reviews of existing policies and procedures, and update or modify as warranted by environmental and systemic needs.

(e) Assimilate new technologies and information processing methodologies in a flexible, pro-active program.

(f) Deliver procedures and annual cybersecurity awareness training, which covers individual user responsibilities, to all users of Marine Corps IT resources within their area of responsibility.

(g) Continue to improve efforts to monitor network and system activities, as well as detect, report on, and take countermeasures against unauthorized activities.

(h) Establish a cybersecurity governance board to conduct compliance readiness reviews.

(2) Concept of Operations. Cybersecurity is employed to defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the timely restoration of information systems by incorporating protection, detection, reaction, and recovery capabilities.

b. Subordinate Element Missions

(1) Major Subordinate Commands, Commanding Officers, Assistant Chiefs of Staff, Division Directors, and Special Staff Officers

(a) Commands utilizing command owned/managed Information Systems are responsible for tasks listed in reference (a), paragraph 4a(3)(j).

(b) Appoint in writing an Information Systems Coordinator (ISC) to assist the commander in all matters related to CIS in accordance with reference (b).

(2) ISSM. ISSMs are responsible for tasks listed in reference (a), paragraph 4a(3)(k). The ISSM functions as the MAGTFTC, MCAGCC focal point and principal advisor for all cybersecurity matters on behalf of MAGTFTC, MCAGCC. The ISSM reports to the Commanding General, or appointed representative, and implements overall cybersecurity requirements within their area of responsibility.

(3) Information System Security Officers (ISSO). ISSOs are responsible for tasks listed in reference (a), paragraph 4a(3)(l). ISSOs are privileged users who are appointed by, and report to, the ISSM and ensure an appropriate cybersecurity posture is maintained for a command, site, system, or enclave. They provide direct support to the ISSM for all cybersecurity matters. They also assist the ISSM in evaluating risks, threats, and vulnerabilities to determine if additional safeguards are needed within their area of responsibility.

(4) System and Network Administrators (SYSADMIN/NTWKADMIN) SYSADMINs and NTWKADMINs are responsible for tasks listed in reference (a), paragraph 4a(3)(m). SYSADMIN/NTWKADMINs are privileged users who manage user accounts and provide cybersecurity safeguards and assurances to the data under their control and take appropriate administrative or programmatic actions to minimize security risks and insider threats, reporting cybersecurity issues to the ISSM.

(5) Unit ISCs. Per reference (b), ISCs shall be appointed by their unit as a trusted liaison between their unit and the MAGTFTC, MCAGCC Assistant Chief of Staff (AC/S), G-6 Communications for all matters related to communications and information systems, and to assist users in performing

their required cybersecurity tasks. Such tasks include, but are not limited to, assisting Marine Corps Enterprise Network (MCEN) users in submitting a DD 2875 System Authorization Access Request (SAAR), and assisting users with receiving cybersecurity indoctrination training and annual cybersecurity refresher training.

(6) <u>MCEN Users</u>

(a) All information system end users are responsible for tasks listed in reference (a), paragraph 4a(3)(n) and reference (c). A user is defined as any military, government civilian, or contractor who has authorized access to the Department of Defense Information Network or Marine Corps IT resources. 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. Users shall receive cybersecurity indoctrination training and attend annual cybersecurity refresher training. Users shall submit and have an approved SAAR.

(b) 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.

c. <u>Coordinating Instructions</u>

(1) <u>Prohibited Activities</u>. The activities listed in reference (a), paragraph 4a(3)(o) are specifically and expressly prohibited. Such activities include, but are not limited to:

(a) Do not use any personally owned devices on the MCEN.

(b) Do not use government owned assets 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.

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

(d) Do not participate in on-line gambling or other activities inconsistent with public service.

(e) Do not participate in, install, configure, or use unauthorized peer-to-peer technologies.

(f) Do not release, disclose, or alter information without the consent of the data owner, the original classification authority, the individual’s supervisory chain of command, Freedom of Information Act official, Public Affairs Officer, or the disclosure officer’s approval.

(g) Do not attempt to strain, test, circumvent, or bypass security mechanisms.

(h) Do not modify system or software, use it in any manner other than its intended purpose, introduce malicious software or code, add userconfigurable or unauthorized software, disable or remove security or protective software or mechanisms, or misuse/abuse a privileged account.

(i) Do not relocate or change information system equipment or change network connectivity without proper security authorization.

(j) Do not acquire commercial or unauthorized internet service provider (ISP) network access into Marine Corps operational facilities or implement commercial wireless components without approval from the ISSM.

(k) Do 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 ISSM.

(l) Do not auto forward emails 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.

(m) Do not use removable secondary storage media on government information system without prior written approval from the MAGTFTC, MCAGCC AC/S, G-6 Communications. 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.

(n) Do 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.

(o) Do 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.

(2) The point of contact for cybersecurity is the Command ISSM at (760) 830-0099.

5. Administration and Logistics. Directives issued by this Headquarters are published and distributed electronically. Electronic versions of Combat Center order can be found at https://www.29palms.marines.mil/Staff-Offices/G-1-Manpower-Directorate/Adjutant/#combat-center-orders.

6. Command and Signal

a. Command. This Order is applicable to all MAGTFTC, MCAGCC personnel and organizations aboard the Combat Center.

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

R. D. STORER
Chief of Staff

DISTRIBUTION: A

Listing of Marine Corps Enterprise Cybersecurity Manuals

Headquarters Marine Corps Deputy Commandant for Information, Information Command, Control, Communications & Computers reviews and updates the Marine Corps Enterprise Cybersecurity Manuals (ECSMs). For current ECSMs, access the ECSM folder at:

https://usmc.sharepoint-mil.us/sites/DCI_IC4_CY/SitePages/ECSMs.aspx

ECSM 001 Computer Security Incident Handling

ECSM 002 Protected Distribution System

ECSM 003 Container and Platform Security Framework

ECSM 004 Remote Access Systems

ECSM 005 Portable Electronic Devices and Wireless Local Area Network Technologies

ECSM 007 Resource Access Guide

ECSM 008 Cross Domain Solutions (CDS) and Secure Data Transfer (SDT)

ECSM 009 North Atlantic Treaty Organization Information Handling on the Marine Corps Enterprise Network

ECSM 010 Unauthorized Disclosure of Classified Information and Electronic Spillages

ECSM 011 Personally Identifiable Information (PII)

ECSM 012 Marine Corps Enterprise Network Cybersecurity Reference Architecture (MCEN CRA) Framework

ECSM 013 Public Key Infrastructure (PKI)

ECSM 014 Disaster Recovery (DR) and Contingency Plan (CP)

ECSM 018 Marine Corps Assessment and Authorization Process (MCAAP)

ECSM 019 Program of Record (POR) Cybersecurity Playbook

ECSM 020 Marine Corps Information Assurance Vulnerability Management Program

ECSM 021 Ports, Protocols, and Services Management

ECSM 024 Marine Corps Cyberspace Information Technology / Cybersecurity Workforce Qualification Program (Cyber IT/CSWF QP)

ECSM 026 Concept of Operations for Host Based Security System

ECSM 030 Commercial Internet Service Provider (C-ISP) Connection Processing and Management