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

CCO 5239.2D
14A

SEP 09 2019

COMBAT CENTER ORDER 5239.2D

From: Commanding General
To: Distribution List

Subj: CYBERSECURITY

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

1. Situation

a. Marine Air Ground Task Force Training Command (MAGTFTC), Marine Corps Air Ground Combat Center (MCAGCC) continues employing information technology (IT) to support the warfighter as there continues to be an increase on the dependence of network IT-based Command and Control Systems to process and transfer daily administrative and operational information. Consequently, internal and external threats to these systems increase the likelihood that a successful attack will occur as our adversaries continue to become more technically and tactically sophisticated which may degrade or disrupt daily administrative and operational tasks. Therefore, it is incumbent upon every IT user to be an active member of MAGTFTC, MCAGCC Cybersecurity.

b. This Order formally establishes the MAGTFTC, MCAGCC Cybersecurity and defines the responsibilities for protecting our information infrastructure. This directive augments the references and delineates responsibilities for local units, organizations, and users.

c. 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 MAGTFTC, MCAGCC Information System Security Manager (ISSM).

2. Cancellation. CCO 5239.2C.

3. Mission

a. Implement Cybersecurity on Communications and Information Systems (CIS) and IT resources procured, developed, operated, maintained, or managed at MAGTFTC, MCAGCC.

b. 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 U.S. 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) Commanding Officers, Assistant Chiefs of Staff (AC/S), Division Directors, and Special Staff Officers

(a) 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 AC/S Communications Directorate 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) MCEN Users. All information system (IS) 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.

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. Coordinating Instructions

(1) Prohibited Activities. 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 user-configurable 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 Communications Directorate. 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/Adjutant-Office/Orders/.

6. Command and Signal

a. Command. This Order is applicable to all MAGTFTC, MCAGCC special staff sections, units, tenant commands, and organizations aboard the Combat Center.

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

R. MARTINEZ
Chief of Staff

DISTRIBUTION: A