UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

IN REPLY REFER TO:
1000
G-6
1 APR 2015

POLICY LETTER 7-15

From: Commanding General, I Marine Expeditionary Force
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE (I MEF) USER ACCOUNT MANAGEMENT POLICY

Ref: (a) CJCSI 6510.01F
(b) CMC WASHINGTON DC 232110Z Dec 13 (MARADMIN 690/13)
(c) TECOM QUANTICO VA 111819Z Jun 13 (MARADMIN 288/13)

Encl: (1) Memorandum I MEF Annual Cyber Awareness User Account Management

1. Purpose. I MEF places a high degree of emphasis on its cybersecurity posture. A major component of organizational cybersecurity is effective and diligent management of access control to organizational resources. To ensure effective management of I MEF user accounts, Information Assurance and Information Systems Management personnel run a monthly scan of user accounts to identify and remediate inactivity thresholds.

2. Information

a. Reference (a), section (26), paragraph (r) mandates that system administrators will disable accounts that have not been used in a 30-day period and that Information Systems Security Officers (ISSOs) will validate disabled accounts and determine if they should be deleted.

b. Reference (b), section (3) states that Annual Cyber Awareness Training is valid for one year from the date of the user's last Cyber Awareness training certificate date. Users without valid cyber awareness training are not authorized access on the Marine Corps Enterprise Network Non-classified Internet Protocol Router Network (MCEN N) or the Marine Corps Enterprise Network Secret Internet Protocol Router Network (MCEN S).

3. Scope

a. 30/60/90-Day Account Management Process

(1) 30-Days of Inactivity. User accounts flagged as being inactive for 30 days will be disabled by I MEF administrators.

(2) 60-Days of Inactivity. When user account inactivity exceeds 60 days, the I MEF G-6 Helpdesk will send the user's Information Systems Coordinator (ISC) a notification of the user's account status. The account will be moved to an Inactive User folder.

(3) 90-Days of Inactivity. User accounts flagged as being inactive for 90 days will be deleted by I MEF administrators.

(4) Identification of Account Exceptions. User sections or units are responsible for identifying deployed or Temporary Additional Duty (TAD)

personnel. User accounts that have been identified as deployed or TAD will be placed in an Inactive User folder which will prevent erroneous account disabling or deletion.

b. Cyber Awareness Account Management Process

(1) Cyber Awareness Certificate Expiration:

(a) Cyber awareness and 30/60/90-day account management tasks will be directly administered by I MEF administrators on both the I MEF Secure Internet Protocol Router Network (SIPRNet) domain and the Combined Enterprise Regional Information Exchange (CENTRIXS) enclaves. Since Marine Air Ground Task Force (MAGTF) Information Technology Support Center West (MITSC West) directly manages the MCEN N enclave, all account management requests will be submitted to MITSC West administrators utilizing a Remedy Service Request.

(b) I MEF administrators must ensure that user accounts are set to expire 365 days from the course completion date of the last cyber awareness completion certificate on file with the user's System Authorization Access Request (SAAR).

(c) User accounts will be disabled when cyber awareness training certificates are expired. User accounts will continue to be disabled until a valid cyber awareness certificate is provided. Disabled accounts will be managed utilizing the 30/60/90-day account management process unless the user is deployed, TAD, or otherwise flagged as an exception.

(2) Cyber Awareness Training for Other Uniformed Personnel and International Officers Serving with the Marine Corps:

(a) All non-Marine Department of Defense (DoD) uniformed personnel and International Officers serving with the Marine Corps in a Permanent Change of Station (PCS) status, Permanent Change of Assignment (PCA) status or in a TAD status who require access to the MCEN N or MCEN S must have a valid Cyber Awareness certificate before access is granted. User account SAAR requests without a valid accompanying Cyber Awareness certificate will not be processed for user account creation.

(b) Annual Cyber Awareness training can be conducted on the MarineNet training portal, the Total Workforce Management System (TWMS) portal or via the Defense Information Systems Agency (DISA) portal.

(c) Foreign National users are required to complete the following additional documentation prior to receiving user access to SIPR releasable (REL) resources:

1. Nondisclosure Agreement.

2. Supplemental Training form.

3. Acceptable Use Policy. In addition, the Foreign Disclosure Officer must have a copy of the user's Delegation of Disclosure letter on file.

c. Common Access Card (CAC) Authentication

(1) MCEN N user accounts must utilize a Defense Enrollment Eligibility Reporting System (DEERS) CAC in order to access the MCEN N environment.

(2) MCEN S user accounts must utilize a SIPRNet token CAC in order to access the MCEN S environment.

(3) Generally, username and password authentication to MCEN resources is not authorized unless there is an administrative requirement to waive CAC enforcement. Requests to waive CAC enforcement can be submitted to the I MEF G-6 Helpdesk at DSN 365-9199, or commercial at 760-725-9199 or the I MEF G-6 ISMO Chief at DSN 365-1545 or commercial at 760-725-1545.

d. All I MEF administrative privileged account personnel are responsible for timely and complete compliance with this Policy Letter.

e. Failure to comply with this policy may result in removal of privileged access.

f. This Policy Letter is applicable to I MEF Command Element (CE), I Marine Expeditionary Force Headquarters Group (I MHG) units, and 11th, 13th, and 15th Marine Expeditionary Unit (MEUs).

4. Certification

a. Points of contact are the I MEF G6 Helpdesk at DSN 365-9199, or commercial at 760-725-9199 or the I MEF G-6 ISMO Chief at DSN 365-1545 or commercial at 760-725-1545.

b. This Policy Letter is effective the date signed.

M. J. GOUGH
Chief of Staff

Distribution: I/II

UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U.S. MARINE CORPS FORCES PACIFIC
BOX 555300
CAMP PENDLETON, CALIFORNIA 92055-5300

IN REPLY REFER TO:
5500
ISMO
16 Sep 14

MEMORANDUM

From: G-6 Information Systems Management Officer, I Marine Expeditionary Force
To: Distribution List

Subj: I MARINE EXPEDITIONARY FORCE ANNUAL CYBER AWARENESS USER ACCOUNT MANAGEMENT

Ref: (a) CJCSI 6510.01F
(b) MARADMIN 690/13

1. Purpose. The purpose of this memorandum is to provide situational awareness regarding the need for First Marine Expeditionary Force (I MEF) G-6 and I Marine Headquarters Group (I MHG) Major Subordinate Elements (MSEs) S-6 to establish a defined course of action regarding the creation and management of I MEF Secure Internet Protocol Router Network (SIPRNet) and Non-Secure Internet Protocol Router Network (NIPRNet) user accounts.

2. Background. MARADMIN 690/13 section 3 states that Annual Cyber Awareness Training is valid for one year or 365 days from the date of the last training. Users without valid cyber awareness training are not authorized access on the MCEN SIPRNet or NIPRNet network.

3. Course of Action.

In order to assure annual cyber awareness compliance the Microsoft Active Directory User Account creation process must ensure that the user account is set to expire 365 days from the course completion date of the last cyber awareness completion certificate on file with the user's System Authorization Access Request (SAAR).

Although I MEF G-6 has historically created and managed user accounts for MSE units, select units have been provided appropriate Administrator-level access to Create, Delete, and otherwise manage their user accounts. These units are required to maintain and manage user accounts, SAAR forms, and logon

privileges in accordance with all existing policies, procedures and guidelines.

In order to facilitate user account management processes and SAAR record keeping requirements, I MEF G-6 requests a valid user roster from S-6 personnel so that MSE personnel SAARs can be transferred from I MEF G-6 to the local commands.

In addition to user account disabling when cyber awareness training certificates are invalid, user accounts will continue to be disabled after 30 consecutive days of inactivity and deleted after 90 consecutive days of inactivity (unless deployed, TAD, or otherwise flagged as an exception) in accordance with CJCSI 6510.01F.

It is recommended that User Account management personnel maintain a user account management log that will allow for timely and proactive notification when a user's cyber awareness certificate will expire. Users must submit a valid Cyber M (Marines) or Cyber C (Civilians and Contractors) certificate of completion prior to account enablement. Annual cyber awareness certification requirements can be met on the MarineNet Distance Learning website.

9/17/2014

X Patrick S. Miller

CAPTAIN / USMC
I MEF G-6 ISMO
Signed by: MILLER.PATRICK.SHAWN.1141845159