



UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NC 28542-0080

5510

G-6

APR 30 2020

II MARINE EXPEDITIONARY FORCE POLICY LETTER 3-20

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

Subj: II MARINE EXPEDITIONARY FORCE (II MEF) POLICY ON
PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) SECNAVINST 5211.5F, dtd 20 May 2019
(b) Department of Defense Instruction 1000.30, 1 Aug 2012
(c) Marine Corps Enterprise Cybersecurity Directive 011
Personally Identifiable Information (PII) Version 4.0,
dtd 30 Apr 2013
(d) SECNAV Manual 5210.1, dtd 23 Sep 2019

Encl: (1) II MEF Cyber Smart Pak for Removable Media

1. Situation. This policy letter provides additional guidance on the implementation of references (a) through (d) to prevent the disclosure of PII. Reference (c) defines PII as any information that can be used to distinguish or trace an individual's identity such as his or her name, Social Security Number (SSN), date and place of birth (DOB/POB), mother's maiden name, biometric records, and any other information that is linked or linkable to a specified individual. Recurring breaches and losses of PII are concerning to all commanders. Therefore, it is essential that all users understand the following precautions for proper safeguarding and handling of personal information.

a. Rosters containing a military member's name and telephone number alone are not considered PII, but the addition of any other information, such as Social Security Number (SSN), spouse's name, addresses, date of birth, mother's maiden name, financial, credit, and medical data, etc., constitutes PII.

b. A full SSN is automatically PII and the use of the last four digits of a SSN is authorized only when absolutely necessary. Refrain from using any SSN if possible when creating rosters.

c. The Electronic Data Interchange Personal Identifier (EDIPI) also known as the Department of Defense Identification Number (DOD ID Number) has been incorporated by the Department of Defense (DOD) to alleviate the use of SSNs. The DOD considers any breach containing DOD ID Numbers alone to be low risk and is viewed as being no more significant than the knowledge of an individual's name. A breach report is necessary

II MEF POLICY LETTER 3-20

only when the DOD ID Number is associated with other PII elements listed above in paragraph 1(a). The DOD ID Number is considered internal government-related PII by the DOD and should be handled in accordance with references (a) through (d).

2. Mission. To ensure PII is properly handled to prevent the unauthorized disclosure of PII.

3. Execution

a. Commander's Intent. To reinforce DOD and Marine Corps policies on the appropriate handling, storage and receipt/transfer of PII.

b. Concept of Operations. Leaders are responsible for ensuring personnel adhere to the guidelines and practices outlined in references (a) through (d) to ensure the proper safeguard of PII.

c. Task

(1) Assistant Chief of Staff, G-6

(a) Provide technical assistance as required to identify PII on shared drives.

(b) Coordinate II MEF reporting requirements in accordance with references (a) through (d).

(c) Provide support for PII training requirements.

(2) Commanding Generals, 2d Marine Division, 2d Marine Aircraft Wing, 2d Marine Logistics Group, and Commanding Officers 22nd, 24th, and 26th Marine Expeditionary Unit, Marine Expeditionary Force Information Group

(a) Designate a section lead that is responsible for identifying, removing, and maintaining access restrictions of PII on public information repositories.

(b) Ensure personnel follow rules on the storage and distribution of PII.

(c) Coordinate efforts of all subordinate units.

d. Coordinating Instructions

(1) Review public information repositories (shared drives, SharePoint Portal, etc.) to ensure PII is stored in accordance with references (a), (c) and (d).

(2) Remove all files (documents, spreadsheets, databases, etc.) containing PII in accordance with references (a), (c) and (d).

II MEF POLICY LETTER 3-20

(3) All paper files containing PII will have a Privacy Act Data Cover Sheet.

(4) Electronic files containing PII will have access restrictions or will be password-protected in order to permit only appropriate personnel access in accordance with reference (c).

(5) Files containing PII that are e-mailed will be restricted on a need-to-know basis and the e-mail itself will be digitally signed and encrypted in accordance with reference (c). The subject line must begin with "FOUO" and the body will contain the statement "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE (FOUO). ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES."

(6) The scanning of files containing PII is not authorized unless sufficient encryption and access restriction measures are implemented on information systems.

(7) PII shall not be on personally-owned computers or devices. PII will only be stored on Department of Defense owned, contracted, or leased equipment. BITLOCKER encryption will be utilized with removable storage device/media in accordance with enclosure (1).

(8) All commands reporting a suspected or confirmed PII breach must follow the reporting procedures outlined in reference (c). The command Information Systems Security Officer (ISSO) or Information Systems Security Manager (ISSM) will submit the report and immediately notify the II MEF G-6 ISSM. A breach of PII occurs when PII is lost, stolen, improperly distributed, incorrectly disposed, or wrongly released without proper need to, improperly distributed, or disposed of incorrectly. In accordance with reference (c), a breach is defined as an actual or possible loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to PII, whether physical or electronic where one or more individuals could be adversely affected. The following scenarios are examples of PII breaches:

(a) A recruiter has just completed an enlistment package and goes to lunch. He leaves his laptop in his vehicle and enters the establishment to eat. Upon returning, he discovers the car has been broken into and the laptop stolen. The enlistment information collected on the single recruit stored on the laptop is considered as a PII breach and must be reported.


(b) An unencrypted e-mail containing PII is sent to a group of Watch Officers who have a business-need to view the information. This is a PII breach and must be reported.

II MEF POLICY LETTER 3-20

(c) An encrypted e-mail containing the PII is sent to a group of Watch Officers who do not have a business-need to view the information. This is a PII breach and must be reported.

(9) All personnel are required to have Cyber Awareness Training completed during the fiscal year, and it is valid for one year from the date of the last training.

4. Administration and Logistics. Point of contact for this matter is the II MEF G-6 Information Systems Security Manager at (910) 450-7815 or (910) 450-7814.


R. S. MORGAN
Chief of Staff

DISTRIBUTION: A

II MEF Computers will either be a WEAPON for the MAGTF, or a WEAPON for the adversary.



Every User is expected to not only use this weapon to conduct maneuver warfare, but use it to defend the Command and Control Capabilities of the Commander



VIGILANCE IS KEY IN CYBER WARFARE

CYBERSECURITY MISSION:

Apply proven security principles to the Marine Corps Enterprise Network and its interfacing components in order to maintain **CONFIDENTIALITY, INTEGRITY** and **AVAILABILITY** for the network and its data as a whole

IF THERE IS A QUESTION...



....THERE IS NO QUESTION.

CONTACT YOUR LOCAL CYBERSECURITY PERSONNEL

II MEF G-6 Cyber (910) 450-8789



II MEF G-6
CYBER SMART PAK



YOU

ARE THE FIRST LINE OF DEFENSE.

HOLD THE LINE

Preparation

Cyberspace Operations Chief:
MGySgt Travers
Comm 910-450-7815

DCO Chief:
GySgt Gariepy
Comm 910-450-5789

Suspected Phishing:
suspicious@usmc.mil

Identification

General signs of POTENTIAL compromise

Several leads might hint that the system could be compromised by a Virus:

- Antivirus raising an alert or unable to update its signatures.
- Unusually slow computer.
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected time.
- Unusual network activity.
- The computer reboots without reason.
- Some applications are crashing, unexpectedly.
- Pop-up windows are appearing while browsing on the web. (sometimes even without browsing).

General signs of POTENTIAL Phishing Email

Phishing emails are the primary means of social engineering to gain access into a network.

- Email appears to be official, but does not have a digital signature.

Identification

POTENTIAL Phishing (Cont.)

- Poor grammar or uncommon misspellings.
- Urgent language in Subject Line.
- Questionable "From" email address.

Potential Spillage

Understanding that UNCLASSIFIED networks are expected to operate in a suspect state, classified information spillage potentially releases information to adversaries, even if contained locally.

- Look for obvious classification markings.
- Is the information about Troop Movement, DV Travel, Operational Information?
- Is Personally Identifiable Information included?

Containment/Remediation

POTENTIAL Compromise/Virus/Malware

In a potential compromise, time is critical in identifying and possibly containing the event.

- Do NOT turn workstation off, or unplug from the network.
- Identify what actions were taken just before the indication took place.
- Contact your local Helpdesk and notify of symptoms, indicators, and actions taken just prior to symptoms.
- BE PATIENT – Most indicators of compromise are common Operating System faults. Virus alerts typically notify you that the virus was PREVENTED. Follow-on actions prevent further infection.

Containment/Remediation

POTENTIAL Phishing

Notification of Phishing attacks is timely to mitigate other users from being victims.

- DO NOT click on links or open attachments.
- Open new email and "Drag and Drop" the suspect email into new email to add as attachment.
- Send the email to: Suspicious@usmc.mil
- SELF-REPORT!!! If you fell victim to a suspicious email, notify your helpdesk. This is time sensitive, as potential for compromise is highly increased.

POTENTIAL Spillage

Timely reporting and sanitization of classified information spillages prevents possible compromise from adversary.

- DO NOT Forward email
- DO NOT reply to email, as this can further spread classified information and alert potential adversary
- Gather basic information:
 - Who sent email
 - Subject of message
 - Approximately how many recipients
 - Identify possible spillage to outside agencies
- Contact your local Helpdesk to notify of potential spillage and relay any information gathered.
- BE PATIENT – If this is an actual spillage, your workstation will need to be sanitized, which DOES NOT MEAN you will lose all of your files.

YOU ARE THE FIRST LINE OF DEFENSE