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:
1040
CG

POLICY LETTER 01-10

From: Commanding General
To: Distribution List

Subj: SAFEGUARDING OF PERSONALLY IDENTIFIABLE INFORMATION

Ref: (a) Marine Corps Enterprise Information Assurance Directive 011
(b) DISA Personally Identifiable Information(PII)Training
(c) DON CIO msg dtd 181430Z MAY 09 Department of the Navy Privacy Impact Assessment (PIA) Guidance
(d) MARADMIN 162/10, Safeguarding Personally Identifiable Information

1. Situation. This policy letter provides guidance regarding the safeguarding of PII in order to ensure compliance with the references.

2. Mission. Ensure PII is properly handled and procedures are established to mitigate the risk of a PII breach within I Marine Expeditionary Force (I MEF).

3. Execution.

a. Commander's Intent. Reinforce Department of Defense (DOD) and United States Marine Corps (USMC) policies applicable to the handling and storage of PII and take aggressive action to prevent its unauthorized disclosure.

b. Concept of Operations. All I MEF personnel must be familiar with PII safeguarding methods and practices. In conjunction with the references, this policy letter provides specific guidance intended to reduce the risk of a PII breach or mishap.

c. Tasks.

(1) AC/S, G-6

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

(b) Conduct shared drive scans to indentify stored PII that is not in compliance with DoD and Marine Corps policy.

(c) Coordinate I MEF reporting requirements in accordance with the references.

(d) Provide support for PII training requirements.

(2) I MEF Staff and MSCs

(a) Designate staff/organization leads to remove/modify PII information from respective public information repositories.

(b) Ensure personnel follow guidelines regarding storage and distribution of PII within your organizations.

d. Coordinating Instructions

(1) Review staff/organization public information repositories (shared drives, SharePoint Portal, etc…) to ensure PII is stored in accordance with this policy.

(2) Remove all files (documents, spreadsheets, databases, etc…) containing PII that are no longer required.

(3) Ensure files that are still required, which contain PII are password protected.

(4) Files containing PII that are emailed will be password protected and the email itself will be encrypted.

(5) Naval messages and E-mails containing PII will be digitally signed and encrypted.

(6) A PII breach must be reported immediately to the I MEF G-6 Information Assurance Manager during working hours or I MHG CDO during non-working hours. A breach of PII occurs when PII is lost, stolen, released without proper need, improperly distributed, or incorrectly disposed. 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 and for an other than 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 ONE recruit stored on the laptop is considered a PII breach and must be reported.

(b) An officer loads his command's fitness reports onto a thumb drive to work on over the weekend. On his way to the car, the thumb drive falls out of his pocket and is lost. The officer's command consists of over 300 Marines. Upon realizing it was lost, the officer retraces his steps and finds the thumb drive two days later. Despite finding the thumb drive, the data was in an uncontrolled environment. This is a PII breach and must be reported.

(c) A backup tape of a large database that holds payroll information is unaccounted for. A search for the tape turns up evidence that a former employee stole the tape. The tape contains PII for more than 15,000 Marines. Regardless of the reason, since the tape is missing, this is a PII breach and must be reported.

(d) An unencrypted email containing PII is sent to a group of watch officers who have an authorized reason to view the information. Since the email was unencrypted, this is a PII breach and must be reported.

(e) An encrypted email containing PII is sent to a group of watch officers who do not have an authorized reason to view the information. Although the email was encrypted, since they did not have a justifiable need to have access to the information, this is a PII breach and must be reported.

(7) All personnel complete annual PII and Information Assurance training on an annual basis no later than the last day of the last month of each calendar year via MarineNet or http://iase.disa.mil/eta/.

4. Administration and Logistics. Points of contact regarding this policy letter are the G-6 Information Assurance section at DSN 361-3397 or the AC/S G-6 at DSN 361-9666.

5. Command and Signal. This policy letter is applicable to all I MEF units and is effective as of the date signed.

J. F. DUNFORD, JR.

DISTRIBUTION: I,II