UNITED STATES MARINE CORPS
MARINE CORPS INSTALLATIONS EAST
PSC BOX 20005
CAMP LEJEUNE NC 28542-0005

MCIEASTO 5211.5
G-6
05 MAR 2012

MARINE CORPS INSTALLATIONS EAST ORDER 5211.5

From: Commanding General
To: Distribution List

Subj: PERSONALLY IDENTIFIABLE INFORMATION (PII)

Ref: (a) MC EIAD 011 PII, "Marine Corps Enterprise Information Assurance Directive 011 PII" 09 Apr 09
(b) ALNAV 070/07 of 4 Oct 07, "Department of the Navy (DON) Personally Identifiable Information (PII) Annual Training Policy"
(c) Federal Information Security Management Act (FISMA) of 2002
(d) DTM 07-015-USD (P&R), "DoD Social Security Number (SSN) Reduction Plan"
(e) The Privacy Act of 1974, as amended
(f) MARADMIN 491/08, Interim Guidance for Handling, Safeguarding and Reporting Breaches of PII
(g) SECNAVINST 5211.5E, "Department of the Navy (DON) Privacy Program," 28 Dec 05

Encl: (1) USMC PII Compliance Checklist

Reports Required: I. Federal Information Security Management Act (FISMA) Report (Report Control Symbol DD Form 5211-05).
II. PII Breach Report (Report Control Symbol MCIEAST-5211.5-01)
III. Privacy Impact Assessment Report (Report Control Symbol DD Form 2930)

1. Situation. The loss or compromise of PII is a significant risk to military and civilian personnel within Marine Corps Installations East (MCIEAST). PII is any information about an individual which can be used to distinguish or trace their identity, such as name, social security number (SSN), date and place of birth, mother's maiden name, biometric records, etc. This information must be safeguarded no matter the media.

2. Mission. This Order provides guidance on the collection, safeguarding, and maintenance of PII for all subordinate commands and personnel within MCIEAST's Area of Responsibility (AOR) in accordance with the references. Additionally, this policy ensures MCIEAST personnel understand the importance of the proper handling of PII; providing guidance, training, procedures and controls to effectively protect PII and reduce the risk for fraud and identity theft, in accordance with references (a) through (g).

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All personnel shall comply fully with the requirements of the references in order to safeguard PII.

(2) Concept of Operations

(a) Only information reasonably necessary to accomplish a purpose or mission required by higher authority will be kept on any individual.

(b) As defined in reference (a), PII is any information that can be used to distinguish or trace an individual's identity such as their name, SSN, date and place of birth, mother's maiden name, biometric records, and any other information that is linked or linkable to a specific individual in any format to include electronic or paper.

(c) Per reference (c), a record is identified as all books, papers, maps, photographs, machine readable materials or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law.

b. Subordinate Element Missions

(1) Assistant Chief of Staff (AC/S), G-6 shall:

(a) appoint in writing the MCIEAST PII Coordinator;

(b) ensure proper handling of PII at the MCIEAST HQ level in accordance with the references;

(c) periodically review MCIEAST procedures to ensure

compliance with the references;

(d) assist commands in establishing internal controls that apply to their system environment(s);

(e) submit the bi-annual Federal Information Security Management Act (FISMA) Report to the Department of the Navy (DON) Chief Information Officer;

(f) direct command PII Managers to conduct unannounced internal inspections to ensure that PII is being handled properly with respect to training, retention, transmission, and disposal. Additional focus shall be placed on organizations handling PII on a routine basis, utilizing enclosure (1).

(g) Report PII Breaches within one hour of discovery to the U.S. Computer Emergency Response Team (U.S. CERT) using the PII Breach Report. The report must contain all preliminary information known at the time the incident was reported. All subsequent new or updated information will be submitted to U.S. CERT for inclusion into the initial report as soon as it becomes available;

(h) assist Program Managers/Information Technology (IT) System Owners with the completion of Privacy Impact Assessments (PIA) for their new or substantially changed system of records (SOR) IT systems;

(i) ensure PIAs are documented and completed; Identify any Department of Defense (DoD) information system(s) that will collect, maintain, use, and/or disseminate PII;

(j) ensure that completed PIAs are forwarded to Headquarters Marine Corps (HQMC) via the MCIEAST PA Officer per SOR registration requirements;

(k) retain PIA documentation for future inspections; and

(l) ensure PII Managers are compliant the SSN use reduction initiative per reference (d).

(2) MCIEAST Commanders shall:

(a) appoint in writing a PII Officer to oversee the administration of this program;

(b) ensure proper handling of PII at the command level in accordance with the references;

(c) periodically review command procedures to ensure compliance with the references;

(d) ensure the PII Officer complies with section (3) of this Order; and

(e) facilitate fulfillment of training requirements per references (b) and (f). Personnel that handle or may potentially handle PII must receive PII training annually. Individual auditable records of completion will be maintained by the command training officer or the contracting officer representative (COR) in the case of contractor personnel.

(3) Command PII Officer shall:

(a) appoint in writing a PII Manager;

(b) ensure proper handling of PII in accordance with the references;

(c) periodically review procedures to ensure compliance with the references;

(d) establish internal controls that apply to their AOR. Internal controls may be different for each program and each type of record;

(e) submit the bi-annual FISMA Report to MCIEAST G-6 CSD;

(f) conduct unannounced internal inspections on areas that handle or process PII;

(g) report PII breaches within one hour of notification of an incident by completing an OPNAV Form 5211/13 DON Loss or Compromise of PII Breach Reporting Form;

(h) complete a PIA and submit it to HQMC for processing; forward a copy to the MCIEAST G-6, and retain documentation for future inspections;

(i) ensure proper disposal procedures are followed per paragraph 3c(2); and

(j) identify any DoD information system(s) that will collect, maintain, use, and/or disseminate PII.

1. Complete a PIA on all new and substantially changed IT systems of record;

2. maintain a listing of all current systems, publish a bulletin, and conduct a review annually for future inspections; and

3. submit the completed PIA to MCIEAST G-6 Cyber Security Manager per reference (b).

(k) Review the PIA for any information systems that use SSN's. Per reference (d), review the system and justify use of the SSN's. Future phases of the Reduction of SSN Plan will require additional actions.

c. Coordinating Instructions

(1) Acceptable Use. Proper safeguarding of PII is critical to reducing the possibility of the loss or compromise of sensitive information. Per reference (d), PII shall only be viewed by persons with an official need to know. Need to know typically constitutes individuals that collect and handle PII as a specific aspect of their job function.

(a) Paper Documents. Documents that contain PII can include, but are not limited to, recall rosters, sensitive health information, and security clearance information. When handling documents of this nature the individual shall:

1. mark each page containing PII "For Official Use Only (FOUO)";

2. use a PA cover sheet (DD 2923);

3. ensure that the documents are only accessible to individuals with an official need to know per reference (d);

4. when unattended, ensure documents are, at a minimum, locked securely in a drawer or file cabinet; and

5. properly dispose of all PII according to paragraph 3c(2) below.

(b) Electronic Files. The potential loss of PII stored in electronic files can be particularly damaging due to the accessibility, portability, and potential volume that can exist.

1. Electronically stored PII shall be maintained only on official DoD computing assets, be password protected, and be accessible only to individuals with an official need to know (including all shared and public folders).

2. Websites will be secured in a manner consistent with current encryption and authentication mechanisms such as Secure Sockets Layer and Public Key Infrastructure (PKI).

3. Remote access shall employ certificate-based authentication using a DoD authorized PKI certificate on a DoD approved hardware token.

(c) E-mail. The most common breach of PII in the United States Marine Corps occurs by e-mail. When transmitting an e-mail that contains PII the individual shall:

1. digitally sign and encrypt using DoD approved PKI certificates;

2. include "FOUO:" in the subject line; and

3. place the statement "FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES" in the body of the e-mail.

(d) Portable Electronic Devices (PED) and Mobile Storage Devices (MSD). Any PED or MSD that processes or stores electronic records containing PII shall:

1. be restricted to DoD authorized workplaces;

2. be removed from DoD workplaces only when being used for official business; and

3. be encrypted using data-in-transit and data-at-rest.

(2) Maintenance and Disposal

(a) Proper disposal. Any means of destruction that renders documents or records, physical or electronic, unrecognizable and beyond reconstruction.

(b) Paper. Documents shall never be disposed of in trash cans or recycling containers without first cross-cut shredding.

(c) Computing Equipment. Disposal methods include:

1. Degaussing - Causes a total loss of all data stored on the media by passing the device through a very powerful magnetic field, which renders the media inoperable.

2. Destruction - Causes electronic data unreadable and unusable by means of catastrophic forces; any remnants may be handled and disposed of as unclassified waste material.

3. Overwrite - PII may be removed from computer hard drives through the use of approved overwrite software and procedures.

(3) Breach and Incident Response

(a) As defined in reference (d) section (6), a breach of PII occurs when it is lost, stolen, released, or viewed without proper need, improperly distributed, or incorrectly disposed. Any potential compromise of PII, including loss of control, constitutes a breach.

(b) Federal reporting requirements established in reference (a) require all incidents involving PII to be reported to the Federal Incident Response Center within one hour of discovery.

(4) Penalties

(a) Penalties will be determined based on the severity of the offense. The term removal may apply to different situations (e.g., certain duties, a building, network access, etc.). Per reference (g), the recommendations are:

1. The penalty for a first-time offense ranges from reprimand to removal depending on the severity and circumstances of the compromise.

2. The penalty for a second offense ranges from a 14 day suspension to removal depending on the severity and circumstances of the compromise.

3. The penalty for a third offense ranges from a 30 day suspension to removal depending on the severity and circumstances of the compromise.

(b) Reference (e), section (e) as amended explains the applicable criminal penalties.

4. Administration and Logistics

a. Recommendations concerning this Order shall be forwarded to the MCIEAST G-6 Cyber Security Manager at DSN: 751-7050 or Comm: (910) 451-7050 Email: MCIEAST_G6_CSD@USMC.MIL.

b. PII training is available in multiple forms including online, small group, and mass training.

5. Command and Signal

a. Command. This Order is applicable to MCIEAST to include all service members, contractors, civilians, and foreign nationals utilizing any MCIEAST computing enclaves.

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

T. A. GORRY

DISTRIBUTION: A

FOR OFFICIAL USE ONLY

USMC PII COMPLIANCE CHECKLIST

This form is an internal document and is to be used by command leadership to assess the level of compliance in the handling of Personally Identifiable Information (PII) as delineated by law and or specific DoD, DON, and Marine Corps policy. Where deficiencies are noted, the command should take immediate corrective action. For additional guidance and information go to the USMC PII website at https://hqdod.hqmc.usmc.mil/pii.asp or contact Marine Corps Privacy Act Officer at smbhqmcprivacyact@usmc.mil or the Marine Corps C4 IA Identity Management Team at usmc_c4ia_idm@usmc.mil.

This Spot Check form is an auditable record and will be kept on file for three years.

Date:

Section 1 Administrative

The name of your Major Subordinate Command (MSC) / MARFORCOM Privacy Act Coordinator is

The name of the individual assigned to conduct this spot check is

1. The MSC / MARFORCOM Privacy Act Coordinator has been identified in writing with clear roles and responsibilities identified.
   ☐ Yes ☐ No
2. The MSC / MARFORCOM has an implementing Privacy Act instruction per SECNAV 5211.5E.
   ☐ Yes Site document: ☐ No
3. The chain of command has a clear understanding of the Marine Corps reporting policy when a breach of personally identifiable information occurs and ensures affected personnel have been contacted in no more than 10 calendar days from discovery of the breach.
   ☐ Yes ☐ No
4. How many PII incidents were reported in the past 12 months?
5. Of the number of reported incidents, was notification made to the affected individuals within 10 calendar days from the date of discovery?
   ☐ Yes ☐ No ☐ N/A, no incidents reported
6. Has the command disseminated guidance to its personnel on how to properly mark email, messages, letters, etc., that contains PII prior to transmission?
   ☐ Yes ☐ No
7. Has the command taken action to eliminate or reduce the need for the use of SSNs?
   ☐ Yes ☐ No

Section 2 Paper Records

1. At random, spot check 10% of trash containers within your organization to ensure that if they contain PII that they are secure from unauthorized access by individuals who do not have a need to know.
   Number of containers checked Number of container containing PII not secured

USMC PII COMPLIANCE CHECKLIST

2. If command does not shred all documents containing PII before being placed in a recycle container, at random spot check 10 % of recycle containers within your organization to ensure that no PII has been placed inside.

   Number of containers checked Number of containers containing PII

3. Do all forms that collect PII directly from the individual contain a Privacy Act Statement?

   ☐ Yes ☐ No

4. Does the command ensure that disposal of paper records follow the DON Records Retention Schedule set forth in SECNAV M 5210.1?

   ☐ Yes ☐ No

5. For bulletin boards / read boards that disseminate command information to all hands or to select groups, check for the presence of PII. PII should only be available to individuals with an official need to know.

   Number of boards checked Number of examples of where PII was found

Section 3 - Electronic Records and Hardware

1. A check in /check out log with written procedures for all laptops and portable electronic equipment has been created and implemented for all such devices that are transported outside a secure government space.

   ☐ Yes ☐ No

2. At random, spot check 10% of the command's Personal Electronic Devices (PEDs) to ensure time out function is enabled and each device is password protected.

   Number of devices checked
   Number of devices not in compliance
   ☐ N/A - command has no PEDs

3. At random, spot check 10% of the commands laptops and thumb drives for documents containing PII information. Of those select documents, identify if those are either encrypted or password protected.

   Number of documents containing PII
   Number of documents not encrypted or password protected
   ☐ N/A - command has no laptops or thumb drives

4. Does the command ensure all files on hard drives are routinely reviewed and whenever possible, purged of unnecessary PII?

   ☐ Yes ☐ No

5. For commands using shared drives, check 25 % of shared drives for files containing PII.

   Number of files checked
   Number of files containing PII
   ☐ N/A - command does not utilize shared drives

6. For DITPR DON registered systems that contain PII, has there been a PIA submitted for approval?

USMC PII COMPLIANCE CHECKLIST

Number of systems requiring PIAs

Number of systems with PIAs submitted

Section 4 - Websites

1. Does the command have procedures established to ensure PII is not inadvertently posted on a public or restricted access website?

   ☐ Yes ☐ No

2. Are command sponsored websites properly registered in the DefenseLINK Locator?

   Number of sites Number properly registered

3. Spot check 25% of command web sites for PII available to individuals not having an official need to know.

   Number of sites checked Number of records with PII

Section 5 - Training

Is there documentation on file certifying that all military, government civilians, and contractor personnel have completed USMC PII Training?

☐ Yes ☐ No

Is there documentation on file certifying that your personnel have completed Supplemental PII Training?

☐ Yes ☐ No