UNITED STATES MARINE CORPS
MARINE CORPS BASE HAWAII
BOX 63002, KANEOHE BAY HAWAII 96863-3002

BaseO 5211
MP&A
2 Feb 2012

BASE ORDER 5211

From: Commanding Officer, Marine Corps Base (MCB) Hawaii
To: Distribution List

Subj: PRIVACY ACT GUIDANCE

Ref: (a) SECNAVINST 5211.5E
(b) SECNAVINST 5210.8D
(c) SECNAV M-5210.1
(d) DODI 5400.16
(e) MCO 5210.11E
(f) Enterprise Cybersecurity Directive 011 v2.0
(g) Marine Corps Enterprise IA Dir 011

Encl: (1) Privacy Act Coordinator Duties
(2) Unit Systems of Records Program Manager Duties
(3) Directorate Systems of Records Program Manager Duties
(4) Unit/Directorate Information Systems Coordinator (ISC) Duties
(5) USMC PII Compliance Report
(6) Handling/Use, Transporting, and Disposal of Personally Identifiable Information (PII)/Privacy Act Information (PAI)
(7) Rules of Access
(8) USMC PII Compliance Checklist
(9) Department of the Navy (DON) Loss of Compromise of PII Breach Reporting Form
(10) DON Loss or Compromise of PII After Action Reporting Form
(11) Sample Notification Letter
(12) Marine Corps Systems of Records Notices

1. Situation. The Privacy Act of 1974 (Public Law 93-579) and the references above have affected the manner in which personal information concerning individuals is acquired, maintained, stored, and disclosed by Department of Defense (DoD) agencies. Because an individual's privacy may be jeopardized by misuse of data contained in government record systems, Congress established civil liabilities and criminal penalties as safeguards against willful misuse of personal information by federal employees. All levels of command must be aware of mandatory procedures under current regulations for the safeguarding and proper disposal of personal information.

2. Mission. To implement policies and procedures set forth in the references, and enclosures, that govern the administration of the

Privacy Act of 1974 for the proper safeguard and disposal of PII and PAI, and to reduce the potential for data compromise.

3. Execution

a. Commander's Intent and Tasks

(1) Commander's Intent. To ensure all military members, civilian employees, and contractors collecting, maintaining, and handling PII understand their responsibilities to properly protect Privacy Act data; and to require privacy management practices and procedures be employed to prevent loss or compromise.

(2) Tasks

(a) Commanding Officers

1. Conduct a thorough review of all directives, instructions, and policies to ensure procedures are in place that minimize the opportunities for loss or compromise of PII and PAI.

2. Ensure that all military, civilian, and contract personnel within their respective commands receive annual PII training. The base commander is overall responsible for this annual training, and subordinate commanders and directors are directly responsible for annual PII training of all personnel within their authority. PII training is an annual requirement and can be found at: https://hqdod.hqmc.usmc.mil/PII.asp?page=2008Standdown. In addition, the Unit Privacy Act Coordinator will provide overview training to command personnel on the proper collection, protection, dissemination, storage, and disposal of PII with the assistance of the Base Privacy Act Coordinator.

3. Appoint, in writing, a Unit Privacy Act Coordinator. The appointed person is recommended to be a Staff Sergeant/GS-07 or above. See enclosure (1) for a complete list of the Privacy Act Coordinator duties.

4. Appoint, in writing, a Unit Systems of Records Program Manager. The appointed person is recommended to be a Sergeant/GS-05 or above. This appointee may also simultaneously act as the Records Manager. See enclosure (2) for a list of the unit Systems of Records Program Manager's duties.

5. Appoint a Unit ISC. The ISC appointed will be a Sergeant/GS-05 or above. See enclosure (4) for a complete list of ISC duties. In addition to those duties outlined in enclosure (4), the ISC's are responsible for reporting a consolidated listing of the number of individuals who have completed the annual PII training in accordance with reference (g) to the Base Privacy Act Coordinator and

Information Assurance Manager using the USMC Compliance Report, enclosure (5).

6. Provide a copy of all appointment letters to the Base Privacy Act Coordinator.

7. Ensure all personnel employ the procedures detailed in enclosure (6) for the proper handling, transport, and disposal of PII/PAI.

(b) Base Directorates

1. Base Directorates will ensure that all military, civilian, and contract personnel under their authority, or within their work section, receive and complete annual PII training. Annual PII training can be found at: https://hqdod.hqmc.usmc.mil/PII.asp?page=2008Standdown. The Headquarters Battalion (HQBN) Privacy Act Coordinator will provide overview training to command personnel on the proper collection, protection, dissemination, storage, and disposal of PII with the assistance of the Base Privacy Act Coordinator. Base Directorate ISC's are responsible for reporting PII training completion numbers, quarterly, to the HQBN ISC. The HQBN ISC will forward all training statistics to the Base Privacy Act Coordinator and the Information Assurance Manager.

2. Appoint, in writing, a Directorate Systems of Records Program Manager. The person appointed is recommended to be a Sergeant/GS-05 or above. See enclosure (3) for a complete list of Directorate Systems of Records Program Manager's Duties.

3. Appoint a Directorate ISC. The person appointed is recommended to be a Sergeant/GS-05 or above. See enclosure (4) for a complete list of ISC duties.

4. Provide a copy of all appointment letters to the Base Privacy Act Coordinator.

(c) Director, Installations, Environment and Logistics. Ensure that the MCB Hawaii Recycling Center adheres to the policies and procedures outlined in the references, to safeguard against the receipt of improperly disposed PII/PAI from MCB Hawaii, tenant units and organizations.

(d) Base Inspector. Assist the Base Security Manager in the conduct of quarterly inspections of the MCB Hawaii Recycling Center to ensure that proper procedures are followed regarding the receipt of properly disposed PII/PAI material from MCB Hawaii, tenant units and organizations. Ensure the USMC PII Compliance Checklists are completed in accordance with reference (g).

(3) Base Adjutant

(a) As the designated base representative, the Base Adjutant will perform the additional duty of Base Privacy Act Coordinator. This appointment will be in writing and shall be guided in the performance of duties in accordance with the references and this Order.

(b) Ensure proper procedures are adhered to regarding access and notification, timelines, denial authority, disclosure and accounting for all PII/PAI and Privacy Act Requests, see enclosure (7). In the matter of denials (in whole or in part), the MCB Hawaii Staff Judge Advocate's office will assist to ensure legal compliance.

(c) Conduct internal inspections of Directorates using the USMC PII Compliance Checklist, enclosure (8). These inspections will be random and unannounced.

b. Reporting PII Violations/Breaches. Upon discovery of a violation or breach, all military, DoD and contractor personnel are required to immediately notify the Base Security Manager and the Base Privacy Act Coordinator. The Base Privacy Act Coordinator will ensure the commanding officer of the responsible unit is notified of the violation.

c. PII Breach Reporting Steps. Upon being notified, the Base Privacy Act Coordinator will collaborate with the Base Cyber Security Manager, the Base Security Manager and the responsible unit to guide the reporting and after action processes. See enclosures (9) through (11) contain required forms and a sample notification letter. For a detailed list of steps can be found at: https://hqdod.hqmc.usmc.mil/PII.asp?page=PIIBreach. A visual summation of the process is outlined below in Figure 1-1.

Responsible Organization	Time Frame	Action	Resources
Discovering Command		Breach discovered	
Discovering Commands	Within one hour	Breach reported to DON CIO and U.S. Computer Emergency Readiness Team	DON CIO Message DTG 291652Z FEB 08; OPNAV Form 5211/13/td>
DON CIO	Within 24 hours	Individual notification determination made; command notified whether individual notifications required	DoD Risk Analysis Methodology
US-CERT		Assign US-CERT number	
DON CIO	Within	Forward breach report to	

	48 hours	the DoD Privacy and Civil Liberties Office	
Accountable Command	Within 10 days	If required, signed letter sent to each affected individual	Sample notification letter
Accountable Command	Within 30 days	days After action report sent to DON CIO	OPNAV Form 5211/14

Figure 1-1. Department of the Navy Breach Reporting Process.

4. Administration and Logistics. This directive can be found at: http://www.mcbh.usmc.mil/g1/adjutant/Borders.htm.

5. Command and Signal

a. Command. This Order is applicable to MCB Hawaii.

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

BRIAN ANNICHIARICO

DISTRIBUTION: A

Privacy Act Coordinator Duties

1. Serve as principal point of contact on Privacy Act (PA) matters and Subject Matter Expert on the contents and requirements of the references and this Order.

2. Ensure no official files are maintained on individuals that are retrieved by name or other personal identifiers without first ensuring that a system of records notice exists that permits such collection. See enclosure (12) for a list of Privacy Act Systems of Records Notices. Please visit the DON Privacy Act website for a complete list of PA System of Record Notices: http://dpclo.defense.gov/privacy/SORNs/SORNs.html

3. Work closely with their PA systems manager to ensure they are properly trained with regard to collecting, maintaining, and disseminating information in a PA system of records notice.

4. Provide overview training to unit personnel on the provisions of reference (a) and this Order.

5. Review internal directives, forms, practices, and procedures, including those having PA implications and where PA statements are used or PII is solicited.

6. Maintain liaison with records management officials, as appropriate.

7. Provide guidance on handling PA requests; scope of PA exemptions; and fees, if any, that may be collected.

8. Conduct staff assistance visits or program evaluations within the unit and lower echelon organizations to ensure compliance with the PA.

9. Process PA complaints.

10. Ensure protocols are in place to avoid instances of loss of PII. Should a loss occur, take immediate action to apprise affected individuals of how to ensure their identity has not been compromised.

Unit Systems of Records Program Manager Duties

1. Review annually each PA system of records notice under their cognizance to determine if the records are up to date, used in matching programs, and ensure compliance with reference (g). See enclosure (12) for a list of Privacy Act Systems of Records Notices. Please visit the DON Privacy Act website for a complete list of PA Systems of Records Notices: http://dpclo.defense.gov/privacy/SORNs/SORNs.html

2. Report annually, by 1 January, to the Base Privacy Act Coordinator a list of all PA systems of records within the unit.

3. Ensure that records are maintained in accordance with the identified PA system of records notice, and maintain a list of all PA systems of records for each section within the unit that maintain collections.

4. Work closely with unit sections to ensure that all personnel who have access to PA systems of records are properly trained on their responsibilities under the PA.

5. Provide PII training statistics to the Base Privacy Act Coordinator using the USMC PII Compliance Report, enclosure (5), no later than (NLT) the 1st day of November, February, May and August.

6. Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction or disclosure.

7. Protect the records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

8. Ensure that no illegal files are maintained. Illegal files are files not authorized under an approved System of Records Notice, enclosure (12).

9. Ensure only those DoD/DON officials with a “need to know” in the official performance of their duties has access to information contained in a system of records.

10. Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PII contained in a system of records.

11. Using enclosure (8), oversee the unit self-inspection program and conduct semi-annual self-inspections. The Base Privacy Act Coordinator will oversee the Base Directorates for inspection purposes. Report semi-annually on 1 January and 1 July the summarized inspection results to the Base Privacy Act Coordinator.

12. Work with Computer Information Systems Directorate personnel to identify any new information systems being developed that contain PII.

13. Complete and maintain a disclosure accounting form for all disclosures made without the consent of the record subject, except those made within DoD or under the Freedom of Information Act (FOIA).

14. Stop collecting any category or item of information about individuals that is no longer justified, and when feasible remove the information from existing records.

15. Ensure that records are kept in accordance with retention and disposal requirements set forth in reference (c).

16. Take reasonable steps to ensure the accuracy, relevance, timeliness, and completeness of a record before disclosing the record to anyone outside the Federal Government.

Directorate Systems of Records Program Manager Duties

1. Review annually each PA system of records notice under their cognizance to determine if the records are up to date and/or used in matching programs and to ensure they are in compliance with reference (g). See enclosure (12) for a list of Privacy Act Systems of Records Notices. Please visit the DON Privacy Act website for a complete list of PA Systems of Records Notices: http://www.defenselink.mil/privacy/notices/usmc

2. Annually, by 1 January, provide a complete list of all PA Systems of Records notices under their cognizance to the Base Privacy Act Coordinator.

3. Collect, consolidate, and report PII statistics of all personnel trained to the HQBN ISC using the USMC PII Compliance Report, enclosure (8), NLT than the 15th day of October, January, April and July.

4. Maintain all signed PII training certificates.

5. Establish appropriate administrative, technical, and physical safeguards to ensure the records in every system of records are protected from unauthorized alteration, destruction or disclosure.

6. Semi-annually conduct self-inspections using the USMC PII Compliance Checklist, enclosure (8). Provide a copy of the self-inspection results to the Base Privacy Act Coordinator.

7. Protect records from reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

8. Ensure that no illegal files are maintained. Illegal files are files not authorized under an approved System of Records Notice, enclosure (12).

9. Ensure only those DoD/DON officials with a “need to know” in the official performance of their duties has access to information contained in a system of records.

10. Ensure safeguards are in place to protect the privacy of individuals and confidentiality of PII contained in a system of records.

Unit/Directorate ISC Duties

These duties only reflect responsibilities relating to the Privacy Act.

1. Establish logging and tracking procedures for high impact PII records on mobile computing devices or portable media when occupational need requires moving from DoD owned, leased, or occupied workplaces.

2. Analyze how personal information is collected, stored, shared, and managed in Federal IT Systems. This analysis is called a Privacy Impact Assessment (PIA).

3. Verify, sign, and forward via the Base Information Assurance Manager and Base Privacy Act Coordinator, PIAs for systems under their cognizance to the Marine Corps Privacy Act Manager, in accordance with reference (d).

4. Sign in and out Portable Electronic Devices (PED) and Mobile Storage Devices for personnel within their section when removed from DoD owned, leased or occupied workplaces.

5. Assist the Base Information Assurance Manager in investigating and reporting actual or suspected PII violations to the Privacy Act Officer for further reporting to HQMC.

6. Ensure annual PII training is completed for all personnel. Consolidate PII training statistics of all personnel from the unit. For HQBN, this includes reporting for the Base Directorates.

USMC PII COMPLIANCE REPORT

This form is an internal document and is to be used by command leadership to report compliance with USMC PII Training. Each Command will route completed reports via chain of command with MARFORS, MCCDC, and HQMC Departments consolidating subordinate reports and submitting to HQMC C4 IA (hqmc_c4ia_idmgt@usmc.mil).

For additional guidance and information go to the USMC PII website at https://hqdod.hqmc.usmc.mil/pii.asp.

Date:

Command:

Reporting Official:

Phase 1 - All Hands Meeting

Topics covered during the All Hands Meeting (check all that apply):

- ☐ Handling
- ☐ Marking
- ☐ Safeguarding
- ☐ Access
- ☐ Disposal
- ☐ Breach Reporting Procedures
- ☐ Other, Please Specify

Comments:

Phase 2 - Training

Number of military, government civilians, and contractors completing USMC PII Training

Number of military, government civilians, and contractors completing Supplemental PII Training

Comments:

Phase 3 - Compliance

Number of Compliance Checks completed by Command

Comments:

Handling/Use, Transporting, and Disposal of PII/PAI

1. Handling/Use Procedures

a. Full social security numbers (SSNs) shall not be included as part of any printed personnel reports, rosters, award certificates, correspondence, or local forms, etc., unless required under the provisions of reference (a). The only authorized SSN derivative that may be used is the last four digits.

b. All personnel will adhere to the "no disclosure without consent of the record subject" rule of the Privacy Act and ensure that any "non-consensual" disclosure complies with the specific exception criteria set forth in reference (a), sections (b)(1) through (b)(12) and the Privacy Act system of records notice governing records collection. Further, personnel will also ensure that all DoD personnel requesting access to Privacy Act data have demonstrated a valid "official need to know in order to conduct agency business" before such information is shared per section (b)(1) of reference (a).

c. Printed documents that contain PII/PAI are to be protected with a cover sheet marked “For Official Use Only”.

d. All documents that contain PII/PAI are to be marked as “For Official Use Only” on each page, per reference (a).

e. All CD/DVDs that contain PII/PAI are to be marked as “For Official Use Only - Privacy Act Sensitive”.

f. Organizations are allowed to maintain recall rosters when collected information meets purpose statement listed in PASORN NM05000-2, Organizational Management and Locator System.

g. All personnel are required to password-protect PII/PAI maintained on network shared drives.

h. Access to all files, folders, and e-mail that contain PII/PAI shall be restricted to individuals with an official need-to-know requirement. PII/PAI will not be stored in public folders or any other folders with unrestricted access.

i. Government furnished external hard drives are authorized to store or work with PII/PAI documents and information. These external hard drives must be equipped with data at rest encryption security software (e.g. Guardian Edge). Hard drives that contain PII/PAI will be marked “For Official Use Only”. Personal computers or personal external hard drives are not authorized to store PII in any form.

j. In no case is it ever permissible to post PII/PAI to publicly accessible websites. Internal Marine Corps websites providing access to or holding PII/PAI shall be secured in a manner consistent with

current encryption and authentication mechanisms, i.e. Secure Socket Layer and Public Key Infrastructure (PKI). Further, access shall be limited to only those individuals with a business need to know.

k. Personnel will ensure the subject line of all e-mails that contain PII/PAI begin with “FOUO”.

l. All e-mail that contains PII/PAI must be digitally signed and encrypted using DoD approved PKI certificates.

m. Personnel will include the following text within the body of any e-mail, even when encrypted, that contains PII/PAI:
“FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE (FOUO). ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.”

n. Personnel will not send PII/PAI, in any form, to a commercial e-mail account.

o. Data files containing PII/PAI requiring movement from one system to another through or across the NMCI network shall be encrypted, password protected and transported using secure File Transfer Protocol or Virtual Private Network.

p. PII/PAI will not be stored on PEDs and Mobile Storage Devices unless encrypted and password protected.

q. When operational need requires moving PEDs from the confines of MCB Hawaii, the PEDs containing personal information must be:

1. Signed in and out with the designated representative.

2. Configured to require certificate-based authentication for log on, where possible.

3. Set to implement screen lock, with a specified period of inactivity not exceeding 15 minutes, when possible.

4. Have all PII stored or created on PEDs encrypted. At a minimum, encryption methods will be NIST-certified, FIPS 140-2 or current. Until DoN approves an enterprise encryption method for data at rest, WINZIP 9.0 or higher and above provides the required encryption protection using FPIS 140-2 Level II or FIPS-197 certified 258-bit Advanced Encryption Standard. WINZIP passwords will conform to current password guidelines.

r. Individuals who handle PII/PAI must complete Privacy Act training prior to gaining access to Privacy Act records. Web-based basic Privacy Act training packages are available on the DoN Privacy Act Office website at www.privacy.navy.mil.

2. Transporting Procedures

a. All personnel tasked with transporting records containing PII/PIA will transport data in a manner that prevents disclosure of the contents.

b. A cover sheet stating "For Official Use Only" must be used on all documents containing PII/PAI.

3. Disposal Procedures

a. Printed documents may be disposed of by burning, chemical decomposition, pulping, cross-cut shredding, or mutilation to preclude recognition or reconstruction of personal information.

b. All CD/DVDs that contain PII/PIA are to be shredded when no longer needed. These CD/DVDs will not be disposed of in a trash can unless the aforementioned has occurred.

c. Information on magnetic tapes or other magnetic medium will be disposed of by using a method adequate enough for the information to be left beyond reconstruction. Disposal methods include degaussing, physical destruction or overwrite.

d. Placing documents containing PII/PAI in recycle bins is insufficient to meet disposal requirement detailed in reference (d) since recycling facilities typically bale the intact paper for transport to commercial paper mills.

e. If disposing of large quantities of PII/PAI through the use of MCB Hawaii Recycling Center, ensure proper destruction; i.e., shredding, etc., takes place prior to this bulk transfer. The MCB Hawaii Recycling Center is not a "secured" area and is not responsible for the proper destruction of Privacy Act material.

4. Privacy Impact Assessment

a. MCB Hawaii will conduct a PIA on every IT system, Programs of Record (POR) and non-POR, as well as locally created systems to include, but not limited to databases, local websites and limited use applications hosted at the command, per reference (d).

b. All PIAs created by the Marine Corps will use the format located at: https://hqdod.hqmc.usmc.mil/pii.asp?page=PIImpact with further guidance available at: http://www.doncio.navy.mil/contentview.aspx?id=862.

c. Completed PIAs are to be submitted through the Marine Corps Privacy Office, Headquarters Marine Corps C4 IA Division, and the DON CIO for posting to the DON CIO website.

d. For assistance on creating a PIA, please contact HQMC_C4IA_IDMGT@usmc.mil.

Rules of Access

1. Request for access must be submitted to:

Commanding Officer (Attn: Base Adjutant)
Box 63002
MCB Hawaii Kaneohe Bay, HI 96863-3002

or faxed to 808-257-3290. If faxing a request, do not assume it was received but follow-up with a phone call to the office. For questions, please call 808-257-8812.

2. Individuals desiring to review records pertaining to them are urged to submit their requests by mail or in person 10 days before the desired review date. Every effort will be made to provide access more rapidly when necessary; however, records ordinarily cannot be made available for review on the day of the request. When the request is to provide the individual's records directly to an authorized representative other than the parent of a minor or legal guardian, a notarized authorization signed within the past 45 days is required, specifying the records to be released. Additionally, an indication of when and where records may be reviewed will be provided.

3. Requests must provide information needed to locate and identify the record(s); i.e., full name, last four of SSN, etc.

4. When records are ready for review, in person, the custodian will require presentation of identification (ID) before access is granted. Acceptable forms of ID are the U.S. Uniformed Services issued ID, state issued driver's license, or other officially issued forms of ID.

5. When a request is made by mail or other written form, verification of identity will be obtained by requiring the individual to provide certain minimal identifying data, such as date of birth and some item of information in the record which only the concerned individual would likely know. Individuals requesting access by telephone must provide adequate verification. In most cases, information will not be released over the phone and verification will have to be made in person or writing.

6. Individuals may be accompanied by a person of their own choosing when reviewing the record(s) requested, however, the custodian will not discuss the record(s) in the presence of the third party without the written authorization of the individual to whom the record(s) pertain.

7. On request, copies of the record(s) will be provided at cost. Ensure, as the requestor, a statement of willingness to pay all fees or those up to a specified amount is provided or provide a justification to support a fee waiver. Agreements to pay fees are considered to be up to $250.00, unless another amount is specified.

The fee schedule is provided in enclosure (3) of SECNAVINST 5720.42F. If you seek a fee waiver, provide a justification for such a waiver.

8. To protect the personal privacy of others, all records from which an individual has requested copies and release of material, will be reviewed by the custodian before being copied and/or released. In the event information, which would infringe upon the personal privacy of another, is contained in the record, a copy of the record will be made deleting such information, and provided to the requesting individual.

9. A medical record will not be released to the individual if, in the judgment of a physician, the information contained therein could have an adverse effect on the individual's physical or mental well-being. In this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician.

10. Requests under the FOIA may be made by any “person,” including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments. The FOIA does not require Federal agencies to answer questions, render opinions, or provide subjective evaluations. Requesters must ask for existing records. The procedures for filing a request are detailed at the following MCB Hawaii website and available to the general public: http://www.mcbh.usmc.mil/g1/adjutant/adj_foia2.htm.

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?

   Number of systems requiring PIAs

USMC PII COMPLIANCE CHECKLIST

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

MSG/DONCIO 291652ZFEB 2008

DEPARTMENT OF THE NAVY (DON)
LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)
BREACH REPORTING FORM

This form is intended to provide information regarding the INITIAL REPORT of a loss or suspected loss of PII (i.e., a breach). As additional breach information becomes available, this form can be submitted as often as necessary as a SUPPLEMENTAL REPORT. Select the report type from the drop down menu above. **DO NOT DELAY** submission due to lack of information.

US-CERT Number: _____ Today's Date: _____

(In most cases, the US-CERT number will not be available for inclusion in the initial report. Please provide in supplemental report, when available.)

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:

5. Component *(BUMED Activities should Select CNO)*:

6. Organization/Branch/Unit Office:

LOSS OF PII/BREACH INFORMATION

7. Date of Breach: _____ 8. Breach Discovery Date: _____ 9. Breach Discovery Time: _____

(The one hour reporting requirement to notify US-CERT begins at the Date and Time command became aware of the breach. Use military format for time (i.e. 0930, 1455))

10. Individuals Affected by Breach:

Government Civilians:		Government Contractors:		Military (Active):	
Military (Reserve):		Military (Dependent):		Military (Retired):	
Members of the Public:		Other:		If Other, Specify:	

Total Number of Individuals Affected by Breach: 0

11. Type of PII Lost *(e.g., SSNs, Financial Data, Medical Data, etc)*:

12. Brief Description of the breach. Do not include specific names or PII of personnel whose information was lost or compromised.

DATA STORAGE/COLLECTION MEDIA TYPE INFORMATION

13. Data Storage/Collection/Media Type involved in Breach:	14. If Other or More Than One Type, Specify:

15. If the Breach Involved Hardware or Equipment, was the equipment (Check All That Apply):

☐ Personally Owned ☐ Government Owned ☐ Contractor Owned

☐ Encrypted ☐ Password Protected ☐ PK Enabled

16. If the Breach Involved a Government Credit Card, was the Issuing Bank Notified: ☐ Yes ☐ No ☐ N/A

17. What was the Cause of the Breach?

18. If Other, Specify:

ORGANIZATION DESIGNATED OFFICIAL	
19. Name:	20. Title:
21. Phone Number:	22. E-mail Address:

Individual Notifications:

Based on information provided in this report, a risk analysis will be conducted by the DON CIO Privacy Office. If the analysis leads to the determination of a high risk potential for identity theft, this report's Organization Designated Official will be contacted within 24 hours and provided with additional guidance regarding the requirement for notifying individuals.

SENIOR OFFICIAL SIGNING NOTIFICATION LETTERS (IF APPLICABLE) (Usually the Commanding Officer)	
23. Name:	24. Title:
25. Phone Number:	26. E-mail Address:

Submit **Initial Report** for **SECNAV/NAVY Breaches**

Submit **Initial Report** for **MARINE CORPS Breaches**

Submit **Initial Report** for **BUMED Breaches**

Submit **Supplemental Report** for **SECNAV/NAVY Breaches**

Submit **Supplemental Report** for MARINE CORPS **Breaches**

Submit **Supplemental Report** for BUMED **Breaches**

If this form will not work with your version of Adobe Acrobat, please follow the procedure in DON CIO WASHINGTON DC 291652Z FEB 08 LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORTING PROCESS or MARINE CORPS ENTERPRISE INFORMATION ASSURANCE DIRECTIVE 011

MSG/DONCIO 291652ZFEB 2008

DEPARTMENT OF THE NAVY (DON)
LOSS OR COMPROMISE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)
AFTER ACTION REPORTING FORM

This form is intended to provide additional breach information and the status of follow-up actions as information becomes available. It may be used multiple times, as requred.

US-CERT Number: _____ Today's Date: _____

(Please provide when available.)

PERSON MAKING INITIAL REPORT

1. Name:	2. Title:
3. Phone Number:	4. E-mail Address:

5. Component (BUMED Activities should Select CNO):

6. Organization/Branch/Unit Office:

ADDITIONAL BREACH INFORMATION AND STATUS OF FOLLOW-UP ACTIONS

7. If it was previously determined that individual notifications were required, provide status of notifications. If not complete, indicate estimated completion date.

8. Provide actions taken to prevent reoccurrence.:

9. Provide lessons learned.:

10. If breach occurred on a IT system, provide system name.:

_____

11. If a paper document or e-mail, was it marked correctly?

☐ Yes ☐ No ☐ N/A

Submit for **SECNAV/NAVY Breaches**

Submit for **MARINE CORPS Breaches**

Submit for BUMED **Breaches**

Enclsoure (10)

5211 Ser
<Date>

<First Name Last Name>
<Street Address>
<City, State Zip Code>

Dear Sir/Madam:

This letter is to notify you of the potential compromise of your Personally Identifiable Information (PII). Specifically, (activity's name) at (location) reported on (date of report) that (describe what was lost, misplaced, etc.).

While there is no evidence to suggest personal data has been misused, it is the Department of the Navy policy to apprise individuals who may have had personal data compromised. We recommend you visit the Federal Trade Commission's web site at: http://www.ftc.gov/bcp/edu/microsites/idtheft/ for guidance on protective action.

We take this potential data compromise very seriously and continue to strive to protect and secure your PII. Should you have any questions or concerns, please contact (POC and phone number).

We regret this unfortunate development and any inconvenience or undue concerns this may cause. Additional security measures have been implemented to prevent further losses and we are adopting new protocols to ensure all PII is protected.

Sincerely,

<CO>

Marine Corps Systems of Records Notices

M01040-1	Marine Corps Total Force Retention System Records
M01040-2	Marine Corps Total Force System (MCTFS) Records
M01070-6	Marine Corps Official Military Personnel Files
M01080-1	Total Force Administration System Secure Personnel Accountability (TFAS SPA)
M01080-2	U.S. Marine Corps Manpower Personnel Analysis Records
M01133-3	Marine Corps Recruiting Information Support System (MCRISS)
M01754-4	Marine For Life Program
M01754-5	Marine Corps Family Readiness Mass Communication
M01754-6	Exceptional Family Member Program Records
M05100-6	Camp Lejeune Historic Drinking Water Notification Registry
M06320-1	Marine Corps Total Information Management Records
M05420-2	Marine Corps Aircrew Performance Qualification Records
MHD00001	Biographical Files
MHD00006	Register/Lineal Lists
MIL00001	Assignment and Occupancy of Family Housing Records
MIL00002	Unaccompanied Personnel Housing Registration System
MIL00005	Passenger Transportation Program
MIL00012	Licensing Procedures for Military Motor Vehicles
MIL00013	Individual Uniform Clothing Records
MIL00014	Exchange Privilege Authorization Log
MIL00015	Housing Referral Services Records System
MIL00016	Depot Maintenance Management Subsystem (DMMS)
MIL00017	Transportation Data Financial Management System (TDFMS)
MIL00018	Organization Clothing Control File
MIL00022	Delinquent Clothing Alteration List
MJA00002	General Correspondence Files for Legal Administration
MJA00003	Magistrate Court Case Files
MJA00004	In Hands of Civil Authorities Case Files
MJA00005	Financial Assistance/Indebtedness/Credit Inquiry Files
MJA00009	Marine Corps Command Legal Files
MJA00010	Unit Punishment Book
MJA00012	Individual Accounts of Mail Order Clothing (bill file)
MJA00016	Judge Advocate Division "D" Files
MJA00017	JA Division, HQMC Correspondence Control Files
MJA00018	Performance File
MMC00002	Working Files, Inspection Division
MMC00004	Adjutant Services Section Discharge Working Files

MMC00008	Message Release/Pickup Authorization File
MMC00009	Narrative Biographical Data with Photos
MMC00010	Marine Corps Marathon Automated Support System
MMN00005	Marine Corps Education Program
MMN00010	Personnel Services Working Files
MMN00011	Source Data Automated Fitness Report System (SDAFRS)
MMN00013	Personnel Management Working Files
MMN00019	Drug/Alcohol Abuse Reporting Program
MMN00027	Marine Corps Military Personnel Access Files
MMN00034	Personnel Procurement Working Files
MMN00035	Truth Teller/Static Listings
MMN00041	Non-Appropriated Fund (NAF) Employee File
MMN00043	Marine Corps Recreation Property Records and Facilities
MMN00044	Central Registry System Discrimination and Sexual Harassment Database (CRS/DASH)
MMN00046	Recruit Incident System
MMN00048	Performance Evaluation Review Board
MMN00049	Manpower Management Information System
MMN00050	Drill Instructor Evaluation Files System
MMN00051	Individual Recruiter Training Record
MMT00002	Marine Corps Institute Correspondence Training Records System
MRS00003	Marine Corps Reserve HIV Program