



Headquarters Marine Corps

Command, Control,
Communications, and Computers (C4)
Information Assurance Division



Marine Corps Enterprise Information Assurance Directive

*011 Personally Identifiable
Information (PII)*

09 April 2009

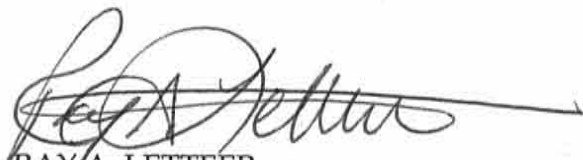
FOR OFFICIAL USE ONLY

FOREWORD

The Director C4/Marine Corps CIO and the Marine Corps Designated Accrediting Authority (DAA) issue's Marine Corps Enterprise Information Assurance Directives (EIAD). The EIAD series provides modules that guide the implementation of policy established in Marine Corps Order (MCO) 5239.2. The modules provide procedural, technical, administrative, and supplemental guidance for all information systems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the Marine Corps Enterprise Network (MCEN), other Marine Corps information systems, as well as contractor owned systems and networks. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing, and executing an element of the Marine Corps Information Assurance Program (MCIAP).

This module, *Personally Identifiable Information (PII)*, outlines the policy and initial procedures to properly protect user information residing on or across Marine Corps owned or operated networks and systems.

Reviewed and Approved by:



RAY A. LETTEER
MARINE CORPS DAA
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS,
INFORMATION ASSURANCE DIVISION



G. J. ALLEN
BRIGADIER GENERAL, U.S. MARINE CORPS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS

CONTENTS

SECTION 1.0 - INTRODUCTION	5
1.1 Purpose	5
1.2 Scope	5
1.3 Cancellation	5
1.4 Distribution.....	5
1.5 Recommendations.....	5
1.6 Effective Date.....	5
SECTION 2.0 - UNDERSTANDING PII	6
2.1 Background	6
2.2 Basics of Privacy	6
2.3 Personally Identifiable Information (PII)	8
2.4 Privacy Act.....	12
2.5 Privacy Act Statement	12
2.6 Systems of Records	13
2.7 E-Government Act of 2002.....	13
2.8 Federal Information Security Management Act (FISMA) of 2002	14
SECTION 3.0 - ROLES AND RESPONSIBILITIES	15
3.1 Director, Command, Control, Communications, and Computers (C4).....	15
3.2 Director of Administration and Resource Management (CMC AR)	15
3.3 CMC ARSF Privacy Act Manager.....	15
3.4 USMC Command Elements.....	16
3.5 Information Assurance Managers (IAMs).....	16
3.6 Program / System Managers	16
3.8 Individuals (Information Owners, Data Handlers, Data Users).....	17
SECTION 4.0 - HANDLING AND SAFEGUARDING PII	18
4.1 Handling PII	18
4.2 Portable Electronic Devices (PED) and Mobile Storage Devices	19
4.3 Remote Access	20
SECTION 5.0 - PII BREACH AND INCIDENT RESPONSE	21
5.1 Breach of PII.....	21
5.2 Penalties.....	22
5.3 Reporting Procedures.....	22
5.4 Reporting to External Individuals and Entities.....	26
5.5 Reporting Loss of Financial Data.....	26
5.6 Remediation.....	26

SECTION 6.0 - PII DISPOSAL	28
6.1 Paper	28
6.2 Computing Equipment	28
SECTION 7.0 - PRIVACY IMPACT ASSESSMENT (PIA)	29
7.1 Privacy Impact Assessment.....	29
7.2 PIA Roles and Responsibilities	31
SECTION 8.0 - RECURRING REQUIREMENTS	32
8.1 Training	32
8.2 Audit	32
8.3 Reporting.....	32
SECTION 9.0 - DEFINITIONS	33
SECTION 10.0 - REFERENCES	37
SECTION 11.0 - ACRONYM LIST	39

ENCLOSURES

ENCLOSURE A - PRIVACY ACT STATEMENT (PAS)	40
ENCLOSURE B - 12 EXCEPTIONS TO THE "NO DISCLOSURE WITHOUT CONSENT" RULE.....	42
ENCLOSURE C - PII COMPROMISE REPORT.....	45
ENCLOSURE D - PRIVACY IMPACT ASSESSMENT TEMPLATE.....	46
ENCLOSURE E - SECURITY CONTROLS	58

FIGURES

FIGURE 1: SEVEN PRINCIPLES OF PRIVACY.....	6
FIGURE 2: PRIVACY ACT AND PII.....	10
FIGURE 3: BREACH REPORTING FLOWCHART	23
FIGURE 4: PIA ROLES AND RESPONSIBILITIES.....	31

TABLES

TABLE 1: BREACH REPORT CHECKLIST	24
TABLE 2: BREACH REMEDIATION ACTIVITIES.....	26

SECTION 1.0 - INTRODUCTION

1.1 Purpose

This Enterprise Directive provides an understanding of Personally Identifiable Information (PII) and its importance within the Marine Corps. In response to recent events pointing out the loss or compromise of private information by other government agencies, the Marine Corps requires those collecting, maintaining, and handling PII to understand their responsibilities, balancing the need to maintain government records on individuals and protecting the individuals' right to privacy. The purpose of this Enterprise Information Assurance Directive (EIAD) for PII is to provide guidance related to the proper handling and protection of PII to prevent loss or compromise.

1.2 Scope

The standards identified in this document will be used as a resource by all Marine Corps organizations and departments that acquire, develop, use, and maintain information systems; by organizations and departments that handle PII in paper or electronic form; and by contracted third-parties who collect, use, or maintain PII on behalf of the Marine Corps. The procedures covered in this document apply to all information system assets.

1.3 Cancellation

This Directive cancels MARADMINs 344/07, 348/06, 431/07, 443/07, and 613/07, and 491/08.

1.4 Distribution

This document is approved for limited distribution to only those individuals possessing an official need to access this document. Access to Information Assurance Directives may be gained via the Headquarters Marine Corps C4 IA web page at: <https://hqdot.hqmc.usmc.mil/IA/Pages/Orders.asp>.

1.5 Recommendations

Recommendations for change or amendment to these standards may be submitted in writing through the HQMC C4 IA Identity Management (IdM) Branch at HQMC_C4IA_IDMGT@USMC.MIL. Recommendations will be evaluated and coordinated with the Marine Corps Privacy Office before taking the necessary action to change or amend this particular Directive.

1.6 Effective Date

This Information Assurance Directive is effective upon date of signature.

SECTION 2.0 - UNDERSTANDING PII

2.1 Background

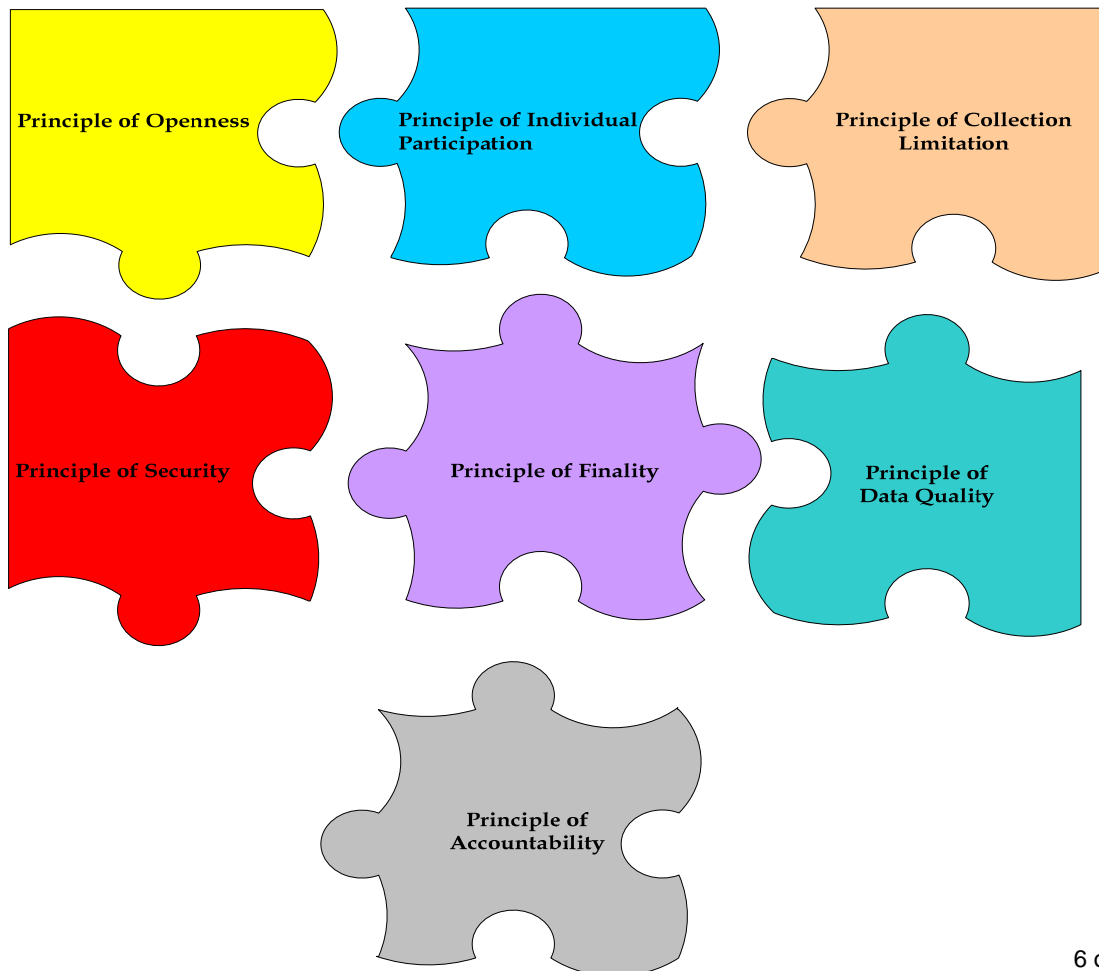
Due to a recent number of incidents where sensitive personal information has been lost or stolen (e.g., Department of Veteran Affairs, Department of State), the Secretary of the Navy has directed that personnel be made aware of their responsibilities regarding the safeguarding of PII, the rules for acquiring and using such information, and the penalties for violation of these rules.

Safeguarding PII is of major concern to the Marine Corps. The proper handling of personal information reduces the possibility of loss or compromise which can place an undue burden upon Marines, contractors, civil servants, and civilians and could cast the Marine Corps in an unfavorable light to the public.

2.2 Basics of Privacy

The concept of privacy is governed by seven basic principles:

Figure 1: Seven Principles of Privacy



The Principle of Openness: Record keeping systems and databases that hold personal data must be publicly known. This includes the main purpose and uses of the data.

The Principle of Individual Participation: Individuals shall have the right to view all information collected about them. Additionally, they should be able to correct or remove data that isn't accurate, relevant, or complete.

The Principle of Collection Limitation: Collection of personal data will be limited to lawful and fair means and with the knowledge or consent of the subject.

The Principle of Data Quality: Only data that is accurate, complete, and relevant to the purposes for which it is collected will be used.

The Principle of Finality: The use and disclosure of personal data will be limited to the purposes specified.

The Principle of Security: Personal information shall be protected from risks such as loss, unauthorized access, destruction, use, modification, or disclosure by means of reasonable security safeguards.

The Principle of Accountability: Record keepers will comply with fair information practices and will be accountable.

2.3 Personally Identifiable Information (PII)

This EIAD uses the definition of PII from OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which states, “information which can be used to distinguish or trace an individual's identity, such as their name, social security number (SSN), biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”

An *individual* refers to any human being, living or dead; including citizens, legal resident aliens, and non-citizens (visitors) of the United States; and employees, including contractors, of the Marine Corps.

To *distinguish* an individual is to identify that individual to a degree where it is possible to have an impact on their life, for example,

- Contacting the individual;
- Making decisions related to the individual’s rights or liberties;
- Granting the individual benefits;
- Imposing penalties on the individual; or
- Providing that information to third parties enabling them to do any of the same.

Examples of distinguishing data are full name combined with other PII elements such as SSN, date of birth, zip code, home address, biometric (images or template) data, etc. Data that does not identify a specific individual, such as a list of credit scores, would not be considered distinguishable data by itself.

To *trace* an individual is to have sufficient information to make a determination about a specific aspect of an individual’s activities or status, but without being able to distinguish the individual. For example, a log containing records of a computer user’s actions could be used to trace activities on the computer.

Information that is *linked* or *linkable* is not sufficient to distinguish an individual when considered separately, but could distinguish an individual when combined with a secondary information source. For example, suppose that two databases contain different PII elements but also share one or more common PII elements. An individual with access to both databases may be able to link information together and create more significant profiles of individuals, potentially distinguishing them. If the secondary information source is present on the same system or a closely related system, then the data is considered *linked*. If the secondary source is available to the general public or can be obtained with a moderate degree of effort, such as from an unrelated system within the organization, then the data is considered *linkable*.

Another example of linkable data: A background investigator has access to an individual's resume that contains information such as an e-mail address, school(s) attended, and degree(s) achieved. Using this information, the investigator may search social networking sites to find out more information about the individual, for example, if the person was identified in pictures while doing something illegal.

A final example of linked data: suppose you frequently buy concert tickets online. You have a profile on the ticket sales website and you have saved your credit card information in order to purchase tickets quickly. Your profile information and credit card information are stored in two different computer systems at the ticketing company but they are *linked* by your profile identification number. If someone compromised both computers, they could exploit this linked data to steal credit card information.

Only in extreme circumstances will name alone will be considered PII (i.e., if name can be attributed to only one person) for protection and reporting requirements.

2.3.1 PII Impact Categories

For DoD Information Assurance purposes and in accordance with reference (g), all PII electronic records shall be assigned an Impact Category (High or Moderate) as determined by the potential negative impact due to loss or unauthorized disclosure.

2.3.1.1 High Impact

High Impact PII is considered as any defense wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act.

High Impact PII may also be considered any compilation of electronic records, containing PII on less than 500 individuals, identified by the Information or Data Owner as requiring additional protection measures.

Example: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact.

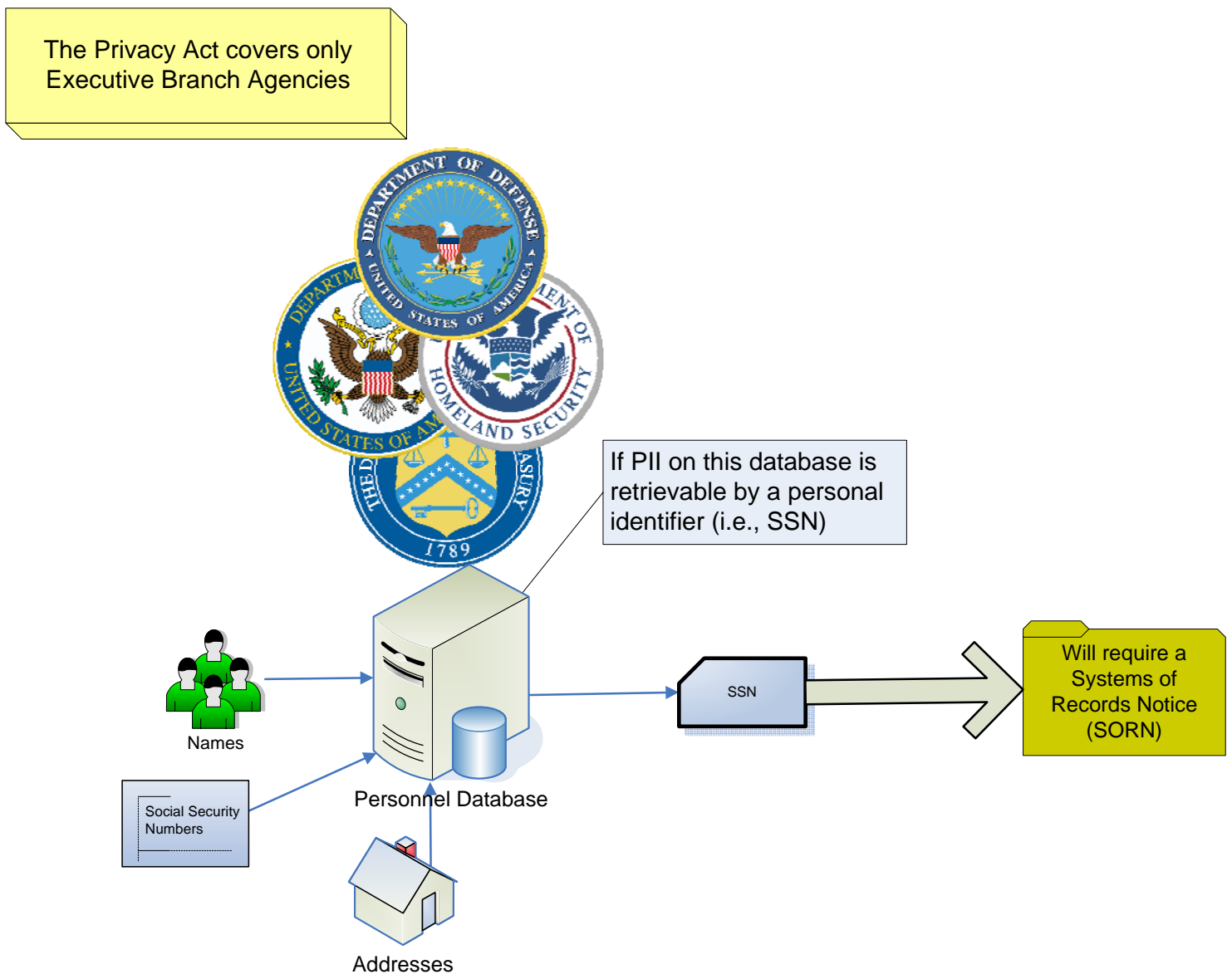
2.3.1.2 Moderate Impact

PII will be considered Moderate Impact if it does not meet the requirements of High Impact PII. Any collection of data storing less than 500 records on a single device, not requiring additional protection, will be considered Moderate PII.

2.3.2 Collecting PII

The Marine Corps collects personal information for several reasons; for hiring purposes, to pay, locate, and educate individuals, and to provide services. The Marine Corps must maintain a balance between maintaining official records for business and administrative purposes and protecting the individuals' right to privacy. When collecting this type of information, agencies must understand that while all information that falls under the Privacy Act is considered as PII, not all PII falls under the Privacy Act. This difference is vital in determining how PII is managed and reported.

Figure 2: Privacy Act and PII



PII that will eventually be placed in an IT/IS system or electronic collection and **retrieved through a personal identifier** is governed by the more rigorous standards of the Privacy Act of 1974, ref (a). If this is the case, Agencies may not collect personal data without first publishing a Privacy Act System of Records Notice (PASORN) in the Federal Register that announces the collection. To find out more information about PASORNs, please contact the USMC Privacy Act Manager at SMBHQMCPRIVACYACT@USMC.MIL.

2.3.3 Collecting PII from the Individual

To the greatest extent possible, collect information for systems of records directly from the individual to whom the record pertains. A Privacy Act Statement (PAS) must be provided when collecting information directly from the individual. The PAS must identify the PASORN that allows the collection of information and identify safeguards that are in place to prevent inadvertent disclosures.

2.3.4 Collecting PII from Third Parties

You may collect verifying information through other sources for security or employment suitability determinations; seeking other opinions, such as supervisor's comments on past performance or other evaluations; obtaining the necessary information directly from the individual would be exceptionally difficult or would result in unreasonable costs or delays; or, the individual requests or consents to contacting another person to obtain the information.

2.3.5 Collecting Social Security Information

Before requesting an individual to provide his or her SSN, the requesting agency shall inform that individual whether that disclosure is mandatory or voluntary, by what authority (statutory or other) the SSN is solicited under, and how it will be used. If a command requests an individual's SSN, though it is not required by Federal statute or is not for a System of Records in existence and operating prior to 1 January 1975, it must provide a PAS and make it clear that disclosure of the number is voluntary. Should the individual refuse to disclose their SSN, the activity must be prepared to identify the individual by alternate means. It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide their SSN.

Despite the widespread usage of the SSN as an identifier, Marine Corps activities are discouraged from collecting SSNs when another identifier would suffice. Further, the Department of Defense has put forth policy stating, "All DoD employees and contractors shall reduce or eliminate the use of SSNs wherever possible. Use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs." This DoD policy puts forth thirteen (13) acceptable uses

for collection of the SSN. All systems collecting SSNs must justify their legal authority to do so and what acceptable use the collection falls under. For more information on SSN limitations and reduction policy see reference (u).

2.3.6 Disclosure of PII

The Privacy Act forbids disclosure of personal information to those who are not entitled to view or access it. This is referred to as the “No Disclosure without Consent Rule.”

Disclosing personal information is punishable by a possible **misdemeanor charge** along with a **\$5000 fine**. As a general disclosure prohibition: “No agency shall disclose any record which is contained in a System of Records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” However, there are several exceptions to this rule. These exceptions are detailed in Enclosure (C). If you have any questions regarding the exceptions, contact the USMC Privacy Act Manager at SMBHQMCPRIVACYACT@USMC.MIL.

2.4 Privacy Act

The Privacy Act of 1974, Title 5, U.S.C. 552a (as amended) balances the Government’s need to maintain information about individuals with the requirement that agencies protect individuals’ right against unwarranted invasions of their privacy through limitations on the collection, maintenance, use, and disclosure of personal information.

The Privacy Act limits the collection and sharing of certain personal data for agencies falling under the Executive Branch. Executive Branch agencies include the various Departments, (Defense, Interior, Treasury, etc.) It further requires that those aforementioned agencies follow certain procedures when collecting personal information. Per the Privacy Act, all Executive Branch agencies must identify “Systems of Records” that allow the collection of information retrievable by a personal identifier. The Privacy Act applies only to US citizens and lawfully admitted aliens whose records are filed in a System of Records where those records are retrieved by a personal identifier.

For more information on the Marine Corps’ Privacy Act implementation, please see reference (i) or contact the USMC Privacy Act Manager at SMBHQMCPRIVACYACT@USMC.MIL.

2.5 Privacy Act Statement

When an individual is requested to provide personal information (name, date of birth, SSN, etc.), for inclusion into a System of Records, a Privacy Act Statement (PAS) must be provided to the individual, regardless of the method used to collect the information (e.g., paper or electronic forms, personal interviews, telephonic interviews, or other methods, etc.). The statement enables the individual to make an informed decision whether to

provide the information requested. A Privacy Act Statement identifies the authority for collecting the information, the purposes for collecting the data, identifies the routine uses of the data, and explains whether disclosure of the information is voluntary or mandatory. If the personal information solicited is not to be incorporated into a paper-based or electronic System of Records, the statement need not be provided. However, personal information obtained without a Privacy Act Statement shall not be incorporated into any System of Records. An example PAS is provided in Enclosure (A).

2.6 Systems of Records

A System of Records is defined as a group of any records under the control of any Executive branch agency from which information is retrieved using the name of the individual or by using some identifying number, symbol, or other identifying particular that is assigned to the individual. Reference (e) requires that DoD Components prepare system notices for systems of records containing personal information retrieved by name or personal identifier for publication in the Federal Register.

Privacy Act Systems of Records Notices (PASORN) inform the public as to what data is being collected, the purpose of collection, and the authority for doing so. The PASORN sets the rules for collecting, using, storing, sharing, and safeguarding personal data when records are retrievable by PII.

The Navy and Marine Corps maintain a list of PASORNs at <http://privacy.navy.mil>. The following are examples of Systems of Records identifiers:

N01740-1	Family Dependent Care Program
N01752-1	Family Advocacy Program System
N01770-2	Casualty Information Support System

To find out if your system or program requires a PASORN, contact the USMC Privacy Act Manager at SMBHQMCPRIVACYACT@USMC.MIL.

2.7 E-Government Act of 2002

The E-Government Act of 2002 requires that Federal agencies protect the collection of personal information in Federal Government information systems by requiring that agencies conduct Privacy Impact Assessments (PIA). This guidance directs agencies to conduct reviews of how privacy issues are considered when purchasing, modifying, or creating new Information Technology (IT) systems or when initiating new electronic collection of PII. A PIA is an analysis of how personal information is collected, stored, shared, and managed in Federal IT systems. The PIA addresses privacy factors for all new or significantly altered IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public. **The Marine Corps has extended this requirement to include all Federal employees and contractors.**

2.8 Federal Information Security Management Act (FISMA) of 2002

To help safeguard personally identifiable information, agencies must meet the requirements of FISMA and associated policies and guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). FISMA gives Congress permanent oversight of agency security matters and expands the information that agencies must submit to Congress, including plans for fixing security problems. FISMA requires all agencies to report security incidents to a Federal incident response center, and implement a comprehensive security program to protect the agency's information and information systems. Agency Inspectors General must independently evaluate the agency's program, and agencies must report annually to OMB and Congress on the effectiveness of their program. FISMA requires each agency to:

- Implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done.
- Notify and consult with the Federal information security incident center, law enforcement agencies and Inspectors General, and any office designated by the President for any incident involving a national security system or any other agency or office in accordance with law or as directed by the President.
- Implement reference (d) guidance and standards.

References (k) and (l) provide a framework for categorizing information and information systems, provide minimum security requirements and controls for incident handling and reporting. Enclosure (E) provides a list of DoD 8500.2 controls that help enforce protection of PII on IT systems.

FISMA guidance can be found on the DON CIO website at <http://www.doncio.navy.mil> while reporting templates are located at the Headquarters Marine Corps C4 IA Homepage at <https://hqdod.hqmc.usmc.mil/IA.asp>.

SECTION 3.0 - ROLES AND RESPONSIBILITIES

3.1 Director, Command, Control, Communications, and Computers (C4)

The Director, C4/DON Deputy CIO (Marine Corps) responsibilities include:

- Serving as the service PIA reviewing official.
- Ensuring that new or modified IT systems that collect, maintain, or disseminate PII and/or new electronic collections have a PIA performed by the office responsible for the IT system or collection.
- Verifying PIAs are completed in conjunction with developing, procuring, or modifying IT systems; and acquire appropriate coordination with the office submitting the request and the information assurance and privacy officials.
- Forwarding PIAs for IT systems and projects to DON CIO.
- Ensuring approved or summary PIAs are placed on the DON's public website.
- Providing information to the DON CIO, as necessary, to compile Congressional and OMB reports.
- Ensuring that PII transmitted in electronic form is protected, safeguarded, and any breach issues promptly reported.

3.2 Director of Administration and Resource Management (CMC AR)

The Director of Administration and Resource Management is the principal Privacy Act Officer for the Marine Corps.

3.3 CMC ARSF Privacy Act Manager

The Marine Corps Privacy Act Manager (MCPAM) oversees the administration of the Marine Corps Privacy Act program; reviews and resolves Privacy Act complaints; develops Marine Corps Privacy Act education, training and awareness programs; establishes, maintains, deletes, and approves Marine Corps PASORN; and, conducts staff assistance visits/program evaluations within the Marine Corps to review compliance with reference (a). Additionally, the MCPAM:

- Serves as the PA Coordinator for all HQMC components, except for Marine Corps Systems Command and the Marine Corps Combat Development Command.
- Provides Marine Corps input to Department of the Navy (DON) Privacy Act Officer for inclusion in the DON FISMA Report submission.
- Provides follow up assistance for PII breach reports.
- Serves on the DON PA Oversight Working Group.
- Reviews PIAs for Privacy Act impact.
- Makes the determination as to whether the new IT system requires a PASORN. If it does, determine whether an existing PASORN covers the collection or whether a new PASORN will have to be written and approved.
- As necessary, assists in creating and getting a new PASORN notice approved.

3.4 USMC Command Elements

USMC Commands shall be responsible for:

- Notifying individuals affected by a breach when notified to do so by USMC Privacy Act Manager and/or DON CIO.
- Reporting PII training numbers up to higher command element.

3.5 Information Assurance Managers (IAMs)

IAMs shall be responsible for:

- Reporting the number of individuals trained in accordance with Section 8.3.
- Establish logging and tracking procedures for High Impact PII records on mobile computing devices or portable media from workplaces.
- Verify, sign, and forward PIAs for systems under their cognizance to the Marine Corps Privacy Act Manager, in accordance with Section 7.0.

As a signatory on Marine Corps PIAs, IAMs hold a critical duty. IAMs must verify that the analysis contained in the PIA is valid, complete, and honest before signing the document. IAMs must also ensure that the security posture protects, and does not erode, privacy for the system. Any risks or deficiencies found in the PIA must be noted and sent to the PM for inclusion in the PIA.

3.6 Program / System Managers

System managers are responsible for overseeing the collection, maintenance, use, and dissemination of information for a system under their responsibility and ensuring that all personnel who have access are aware of their responsibilities for protecting PII. The system manager shall be responsible for:

- Appointing an IAM for the program/system, in accordance with reference (d).
- Establishing appropriate administrative, technical, and physical safeguards to ensure that information is protected from unauthorized alteration, destruction, or disclosure. See examples of privacy enhancing controls in Enclosure (E).
- Protecting the information from reasonably anticipated threats or hazards.
- Ensuring that all personnel who have access to the PII are properly trained on their responsibilities.
- Maintaining records of individuals belonging to other organizations that the system shares data.

3.8 Individuals (Information Owners, Data Handlers, Data Users)

An individual is classified as “a living person who is a citizen of the United States or an alien lawfully admitted for permanent residence.” The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are also categorized as individuals. Corporations, partnerships, sole proprietorships, professional groups, businesses (whether incorporated or unincorporated), and other commercial entities are not individuals.

Marine Corps employees/contractors are responsible for safeguarding the rights of others by:

- Ensuring that PII contained in a System of Records, to which they have access or are using to conduct official business, is protected so that the integrity, confidentiality, and security is preserved.
- Ensuring information contained in a Privacy Act System of Records is not transmitted by any means of communication, to any person or agency, except as authorized by this instruction or the specific PASORN.
- Ensuring unpublished official files that would fall under the provisions of reference (a) are not maintained.
- Safeguarding the privacy of individuals and confidentiality of PII contained in a System of Records.
- Properly marking all documents containing PII data as “For Official Use Only-Privacy Sensitive - Any misuse or unauthorized disclosure can result in both civil and criminal penalties.”
- Ensuring privacy sensitive information is not maintained in public folders. PII maintained in shared folders must, at a minimum, be protected with a strong password and access granted to **only** those with a business need to know.
- Reporting any unauthorized disclosure of PII as outlined in Section 5.0.
- Encrypting all email communications containing PII.

SECTION 4.0 - HANDLING AND SAFEGUARDING PII

Proper handling of personal information is critical in reducing the possibility of the loss or compromise. Recurring breaches and losses of PII have led to a growing concern among the public regarding the proper safeguarding and handling of their personal information. Public trust in the Marine Corps could potentially erode if proper steps are not taken to protect PII. The Marine Corps understands that proper education and training regarding the protection of PII serves to reduce future instances of breaches.

4.1 Handling PII

Individuals tasked with handling PII will do so in a manner that prevents the unauthorized disclosure of its contents. All Marine Corps personnel will employ the following procedures to ensure the proper handling of PII.

4.1.1 Marking and Storage Descriptions and Requirements

Marking and storage requirements apply to systems, applications, reports, all database types, portals, mobile data storage, individual workstations, and laptops. As stated above, all PII electronic records shall be assigned a High or Moderate PII Impact Category. PII data shall be protected at the FOUO level or higher unless specifically cleared for public release.

4.1.2 Paper Documents and Files

Documents containing PII will have a cover sheet stating "For Official Use Only". All documents containing PII will be marked "For Official Use Only" on each page. Documents containing PII will be shredded, burned, or chemically treated when no longer needed (see Section 6.0). An example of a paper document containing PII is a recall roster. Organizations are allowed to maintain recall rosters when collected information meets purpose statement listed in PASORN NM05000-2, Organizational Management and Locator System.

4.1.3 Computer Files/Folders

PII stored on network devices in shared folders shall be at minimum password protected.

- PII will **not** be stored in public folders or any other folders with unrestricted access.
- PII will **not** be maintained on personal computers/devices.
- PII will only be maintained on DoD owned, contracted or leased assets.

4.1.4 Websites

It is never permissible to post PII onto publicly accessible websites. Internal Marine Corps websites providing access to or holding PII shall be secured in a manner consistent

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

4.1.5 Email

Email containing any amount of PII or attachments containing PII must be digitally signed and encrypted using DoD approved PKI certificates.

The subject line of the e-mail **must** begin with “**FOUO:**”.

The body of the email shall contain a statement notifying the recipient to treat the email and its contents:

“FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE (FOUO). ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES.”

This statement will be applied to all email containing PII, even if it is encrypted.

4.2 Portable Electronic Devices (PED) and Mobile Storage Devices

For purposes of this directive, a Portable Electronic Device (PED) is a generic term used to describe any non-personally owned, non-stationary electronic device with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to; Personal Digital Assistants (PDA), Blackberries, palm tops, hand-held/laptop computers, web enabled cell phones, two-way pagers, wireless Email devices, and audio/video recording devices.

Any PED or removable storage device/media that processes or stores electronic records containing PII, shall be restricted to DoD owned, leased, or occupied workplaces. Authorized PED/mobile device users must ensure that any PII processed on the device is encrypted with FIPS 140-2 Level II validated mechanisms. It is understood that PED/mobile devices will be removed from DoD owned, leased, or occupied workplaces; however, commands shall ensure that removal is for official use only.

Under no circumstances will PII be allowed on personally owned devices.

When operational need requires moving PEDs from DoD owned, leased, or occupied workplaces, the PEDs containing personal information must be:

- Signed in and out with a supervising official designated in writing by senior leadership
- Configured to require certificate-based authentication for log on, where possible
- Set to implement screen lock, with a specified period of inactivity not exceeding 15 minutes, when possible
- 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, in the interim, WINZIP 9.0 or higher and above provides the required encryption protection using FIPS 140-2 Level II or FIPS-197 certified 258-bit Advanced Encryption Standard (AES) per reference (y). WINZIP passwords will conform to current strong password guidelines.

When creating a new encrypted file, be aware that the original file remains unchanged on the device. To maintain security of the protected information, the original, unencrypted file should be deleted.

4.3 Remote Access

Remote access to High Impact PII electronic records is highly discouraged. If the operational need arises, only DoD authorized devices shall be used for remote access. Additionally, remote access shall:

- Employ certificate-based authentication using a DoD authorized PKI certificate on DoD approved hardware token.
- Implement a screen lock with a specified period of inactivity not to exceed 15 minutes.
- Conform to IA Control Enclave and Computing Environment (ECRC)-1, Resource Control specified in reference (d).

The download and local or remote storage of PII records is prohibited unless approved in writing by the Marine Corps Enterprise Network (MCEN) Designated Accrediting Authority (DAA).

SECTION 5.0 - PII BREACH AND INCIDENT RESPONSE

5.1 Breach of PII

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:

- (1) 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 as a PII breach and must be reported.
- (2) 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.
- (3) 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 information on over 15,000 Marines. This is a PII breach and must be reported.
- (4) An **unencrypted** email 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.
- (5) An **encrypted** email containing 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.

Following the proper handling, marking, and protection procedures is crucial to mitigating a loss of information. A breach of PII can result in substantial harm, embarrassment, and inconvenience to the individuals and may lead to identity theft or other fraudulent use of the information. Because the Marine Corps maintains significant amounts of information, **there is a special duty to protect that information from loss and misuse.**

5.2 Penalties

A breach may have major implications for the individual(s) responsible for the loss/compromise that could result in disciplinary actions punishable under the UCMJ. Further, civil or criminal actions may be taken against the employee, and costly fines up to \$5000 per instance and jail time up to one year. Privacy violations that could lead to criminal penalties include collecting data without meeting the Federal Register publication requirement, sharing data with unauthorized individuals, acting under false pretenses, and facilitating those acting under false pretenses.

A breach also has severe ramifications for the agency as a whole. The Department of the Veterans Affairs received a report regarding a stolen laptop on May 3, 2006. The laptop contained 26.5 million records on active duty troops and veterans. On June 29, 2006 the FBI announced the stolen laptop had been recovered and that it appeared no one had accessed the personal data. Despite the FBI's announcement, class action law suit was filed against the VA. The class action law suit was settled for \$20 Million.

TJX Companies, Inc. estimated costs associated with the breach of 94 million customer records at \$256 million. The costs for TJX Companies, Inc include fixing the company's computer system and dealing with lawsuits, investigations, and other claims stemming from the breach. In addition to credit card numbers, personal information such as social security numbers and driver's license numbers from 451,000 customers were downloaded by the intruders. The breach was possible due to a non-secure wireless network in one of the stores.

5.3 Reporting Procedures

All breaches are to be reported to US-CERT within one hour of discovering an actual or suspected breach has occurred. The USMC PII Breach Report can be found at: <https://hqdot.hqmc.usmc.mil/PII.asp?page=PIIBreach> and in Enclosure (d).

Figure 3: Breach Reporting Flowchart

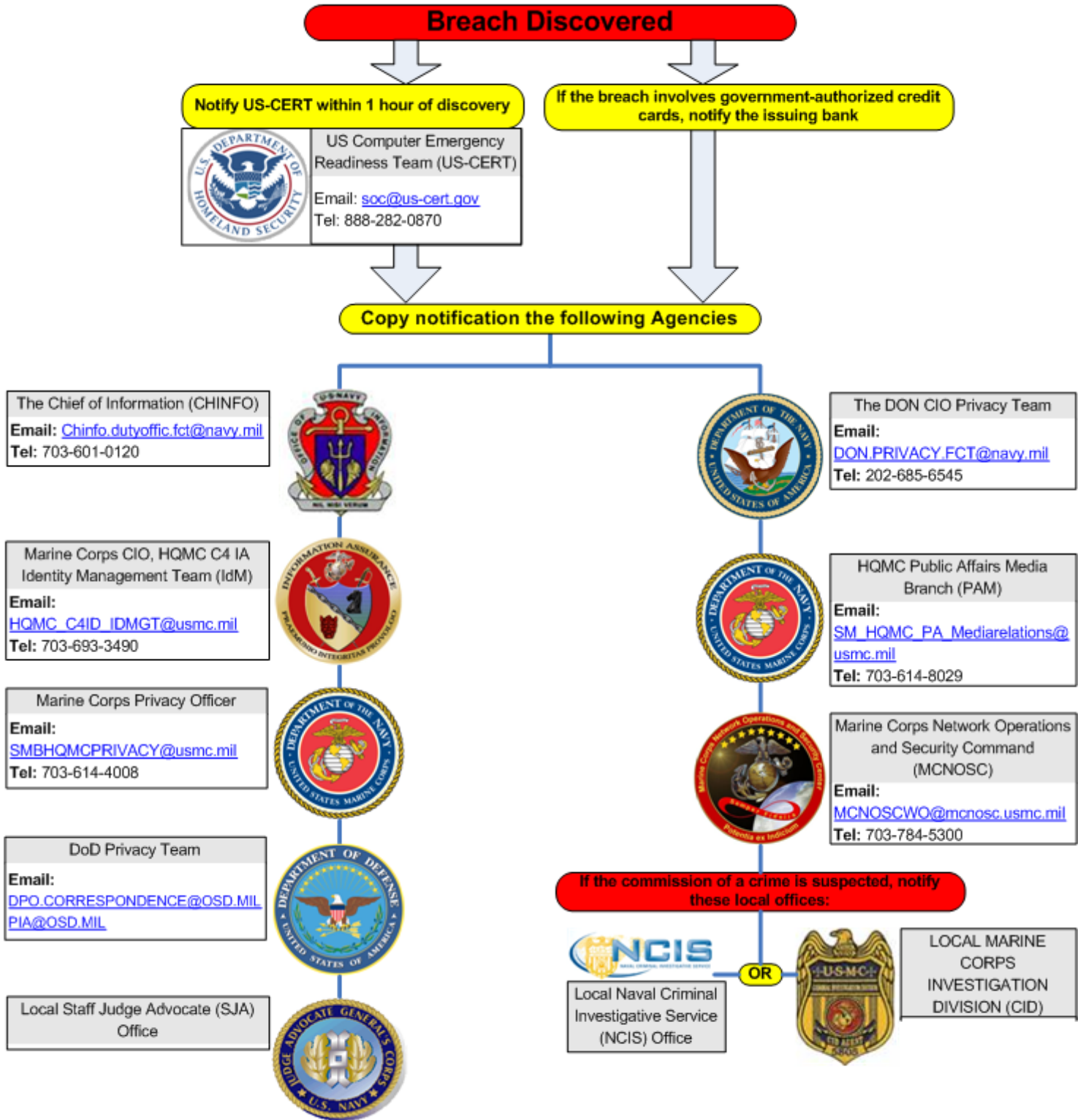


Table 1: Breach Report Checklist

WITHIN 1 HOUR		
<ul style="list-style-type: none"> Command will report actual or suspected breach using the PII Compromise Report Template 		
This report will be sent to the following offices and agencies:		
Agency	E-mail	Telephone
United States Computer Emergency Readiness Team (US-CERT)	SOC@US-CERT.GOV	(888) 282-0870
The Chief of Information (CHINFO)	CHINFO.DUTYOFFIC.FCT@NAVY.MIL	(703) 601-0120
DON CIO Privacy Team	DON.PRIVACY.FCT@NAVY.MIL	(703) 601-6882
Marine Corps CIO, HQMC C4 IA Identity Management (IdM) Team	HQMC_C4IA_IDMGT@USMC.MIL	(703) 693-3490
HQMC Public Media Affairs Media Branch	M_HQMC_PA_MEDIARELATIONS@USMC.MIL	(703) 614-8029
Marine Corps Privacy Act Manager	SMBHQMCPRIVACYACT@USMC.MIL	(703) 614-4008
Marine Corps Network Operations and Security Command (MCNOSC) Watch Officer	MCNOSCWO@MCNOSC.USMC.MIL	(703) 784-5300
DoD Privacy Team	DPO.CORRESPONDENCE@OSD.MIL PIA@OSD.MIL	
If commission of a crime is suspected, notify the appropriate local agencies:		
Local Naval Criminal Investigative Service (NCIS) Office	Local Staff Judge Advocate (SJA) Office	
<ul style="list-style-type: none"> Marine Corps units assigned to combatant commands or under the operational control of combined or Joint Force Commanders will issue an OPREP 3SIR to be submitted to the USMC Privacy Act Manager as a follow up to the initial compromise report. 		
<ul style="list-style-type: none"> All follow up actions by the reporting command will be coordinated through the USMC Privacy Act Manager. 		

WITHIN 24 HOURS		
<ul style="list-style-type: none"> • Commands will be notified by HQMC as to whether or not notification must be provided to the affected individuals. • Commands will file the 24 hour follow up report to the addresses listed above updating the report with any pertinent information (e.g., US-CERT Case number). 		
WITHIN 72 HOURS		
<ul style="list-style-type: none"> • Marine Corps units will issue a Naval Message to the aforementioned listed organizations within 72 hours of the initial report. • The report will contain, at a minimum, all of the information included in the PII report. • The Naval Message should be addressed to the following Plain Language Addresses (PLADS): <ul style="list-style-type: none"> ○ DON CIO WASHINGTON DC, ○ OGC WASHINGTON DC, ○ CMC WASHINGTON DC C4 IA, ○ CMC WASHINGTON DC PA, ○ ACC QUANTICO CWO, ○ CMCWASHINGTON DC AR. 		
WITHIN 10 DAYS		
<ul style="list-style-type: none"> • Command, when directed, must notify the affected individuals of the breach. • Commands will submit a report to the aforementioned list regarding the status of the command's plan to notify individuals whose information was compromised and will contain a description of the actions being taken to prevent future occurrences. 		
Notification will include at a minimum:		
PII elements involved in the breach (e.g., SSN, Date of Birth (DOB), addresses, etc.)	Circumstances surrounding the breach	Protective measures the individual can take
Notification must be either:		
1) Written letter. Sample notification letter may be found at: http://privacy.navy.mil .	2) Digitally signed email to each impacted individual.	
<ul style="list-style-type: none"> • Report lessons learned via email to the USMC Privacy Act Manager and HQMC C4 IA IdM team. 		
<ul style="list-style-type: none"> • If the command is unable to provide notification within the 10 day period, a report will be submitted to the USMC Privacy Act Manager and HQMC C4 IA IdM team providing justification as to the delay and a Plan of Action and Milestones (POA&M) outlining the steps that will be taken in order to complete the process. 		

5.4 Reporting to External Individuals and Entities

While commands will report all suspected or confirmed breaches within 24 hours of discovery, notifying external individuals shall be conducted after an assessment regarding the level of risk that results from the loss, theft, or compromise of the data. The HQMC Privacy Act Manager and DON CIO will assist in making a determination if a breach warrants notification.

5.5 Reporting Loss of Financial Data

If the breach involves the loss or suspected loss of a government authorized credit card or financial data associated with the card, immediately notify the issuing bank and the command government credit card manager.

5.6 Remediation

Remediation activities for PII breaches are varied and must be applied on a situation by situation basis. Below are suggested remediation activities for general breaches, please remember these are not a complete solution.

Table 2: Breach Remediation Activities

Breach Type	Activities
E-mail Breach	<ul style="list-style-type: none"> • Verify message was not properly encrypted and/or sent to parties without a need-to-know. • Send Recall Notice immediately • Request deletion and confirmation from all parties involved • Spillage CLINs are not required
PII Exposed to Internet	<ul style="list-style-type: none"> • Contact Webmaster and request: <ul style="list-style-type: none"> ○ Immediate removal of content ○ Contact Search Engines and request removal of indexed URLs (See below) ○ Ensure proper permissions and access controls are in place
Unauthorized Access (Hacking)	<ul style="list-style-type: none"> • Contact local Command IAM / G6 immediately
PED/Mobile Devices	<ul style="list-style-type: none"> • Contact local Command IAM / G6 immediately; or • Follow established procedures for lost/stolen equipment.

Below is a list of links that will aid in removing content from Search Engines:

- **Google** - <http://www.google.com/webmasters/tools/removals>
- **Yahoo** - <http://help.yahoo.com/l/us/yahoo/search/siteexplorer/delete/index.html>
- **MSN/Live** - <http://help.live.com/>
- **Microsoft SharePoint** - <http://support.microsoft.com/kb/837847>

SECTION 6.0 - PII DISPOSAL

Disposal requirements for PII are any means that prevents compromise of the data. Proper disposal is any means of destruction that renders documents or records (physical and electronic) unrecognizable and beyond reconstruction (e.g., burning, melting, chemical decomposition, pulping, pulverizing, shredding, mutilation, degaussing, and striping.) Marine Corps officials responsible for the collection and maintenance of documents containing PII are to immediately implement procedures to ensure documents containing PII are properly disposed. Additionally, officials will establish internal controls to ensure that periodic random checks are made to ensure proper disposal procedures are being followed. The following are acceptable means for disposing of PII in paper and electronic form.

6.1 Paper

The disposal method for paper is adequate if the information is left beyond reconstruction. Approved disposal methods include cross-cut shredding, burning or chemical decomposition. Documents containing PII will be marked **“FOR OFFICIAL USE ONLY”** when created and will **not** be disposed of in trash cans, recycling containers, etc. without first being shredded. Cross-cut shredding is the preferred method.

6.2 Computing Equipment

The disposal method is adequate if the information is left beyond reconstruction. Disposal methods include degaussing, physical destruction, and overwrite.

6.2.1 Degaussing

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.

6.2.2 Destruction

Destruction is defined as any procedure that renders paper, equipment, magnetic media, etc. unreadable and unusable along with the PII written on it. What remains may be handled and disposed of as unclassified waste material.

6.2.3 Overwrite

Under certain situations specified by the Marine Corps DAA, PII may be removed from computer hard drives through the use of approved overwrite software and procedures.

SECTION 7.0 – PRIVACY IMPACT ASSESSMENT (PIA)

7.1 Privacy Impact Assessment

Reference (b) requires all federal government agencies to conduct a PIA for all new or substantially changed technology that collects, maintains, or disseminates Personally Identifiable Information (PII). To achieve compliance with the mandate, the Marine Corps requires that **every** new or substantially changed technology initiative conduct a PIA. The PIA is a vital tool that evaluates possible privacy risks and the mitigation of those risks at the beginning of and throughout the development life cycle of a program or system. The transparency and analysis of privacy issues provided by a PIA demonstrates that the United States Marine Corps actively engages program managers and system owners on the mitigation of potential privacy risks.

The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. This involves making certain that privacy protections are built into the system from the initiation of development, not after the fact when they can be far more costly or could affect the viability of the project. Enclosure (E) provides example DIACAP controls that can be used to enhance the privacy protection of the system.

In accordance with Reference (f), the Marine Corps will conduct a PIA on **every IT system**. This includes both 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. **Every IT initiative must complete Section I of the DoD PIA**, reference (bb). The first section of the DoD PIA template determines if the system is processing PII and if further analysis is required. Those projects that are not processing PII will have the Program Manager and Information Assurance Manager sign the document and forward to HQMC C4 IA. Those systems processing PII must complete the remainder of the document and submit the PIA for the signatures of the Project Manager, Information Assurance Manager, Privacy Act Manager, Marine Corps DAA, and DON CIO. The PIA will be submitted as part of the Marine Corps C&A process (MCIAP).

PIAs pertaining to PORs are submitted as part of the overall C&A package to Marine Corps Systems Command (MARCORSYSCOM). Non-POR systems (e.g., a locally created Microsoft Access database) are submitted to their command IAM. If the Privacy Act Manager determines that a Privacy Act Systems of Record Notice (SORN) is required, the PIA will continue through the process, but the system and/or application will not be accredited until the SORN process is complete.

If it is determined that publishing a PIA may raise security concerns due to the sensitive nature of the system, a non-sensitive summary of the document may be prepared and

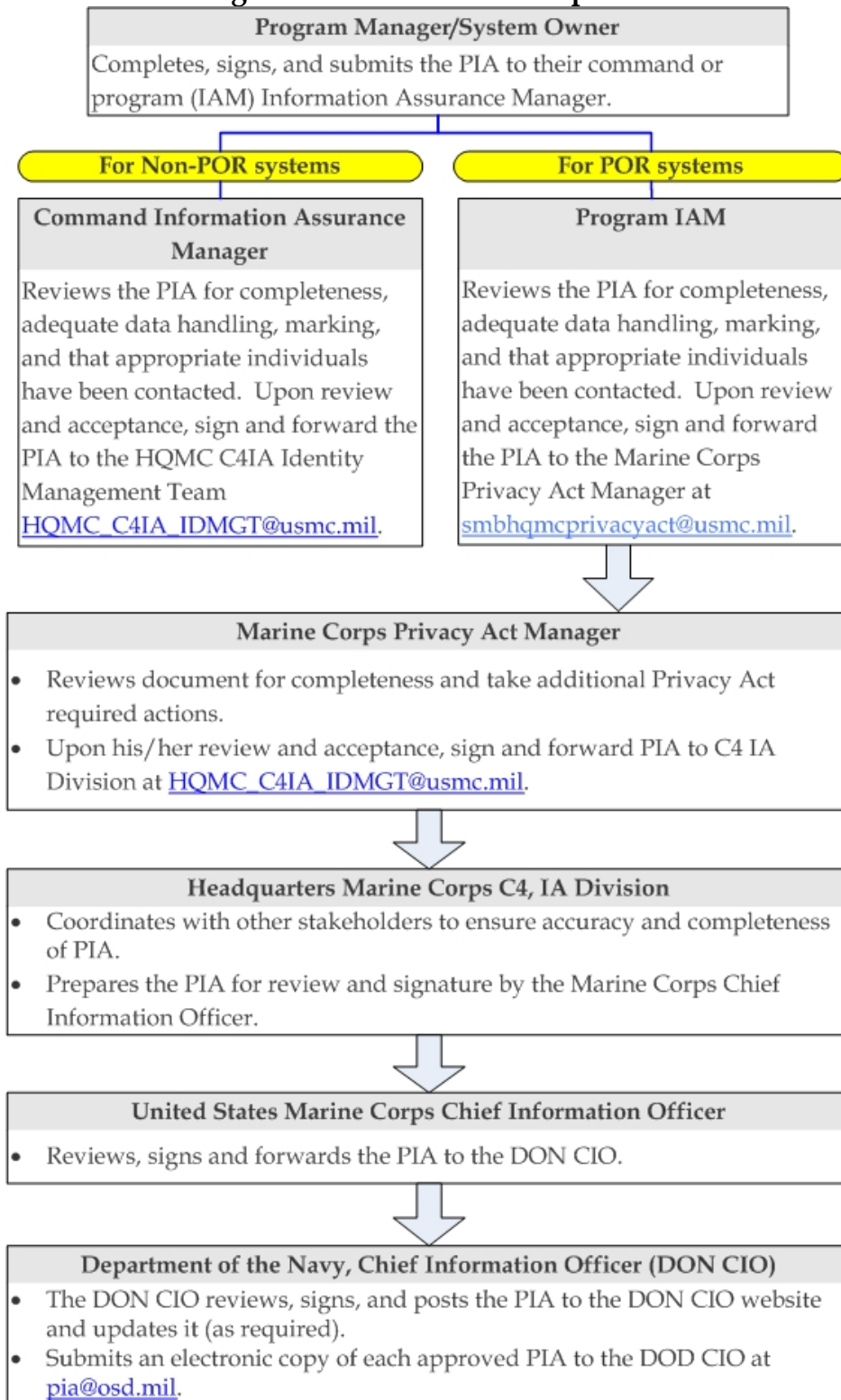
submitted for publication along with the original PIA. If a summary will not eliminate the security concerns, the PIA will not be posted, but will be maintained by the DON CIO for reference and reporting purposes.

All PIAs created by the Marine Corps will use the format located at <https://hqodod.hqmc.usmc.mil/pii.asp?page=PIImpact>. 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 at <http://www.doncio.navy.mil>.

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

7.2 PIA Roles and Responsibilities

Figure 4: PIA Roles and Responsibilities



SECTION 8.0 - RECURRING REQUIREMENTS

Safeguarding PII is a responsibility shared by all individuals responsible for administering operational, privacy, and security programs. As a result, the Marine Corps now requires all installations, commands, and activities to ensure all military, civilians, and contract personnel receive annual PII training. This training will instruct all personnel in the proper collection, protection, dissemination, and disposal of PII. PII training is an annual requirement.

8.1 Training

PII Training courseware can be found at the HQMC C4IA website by navigating to <https://hqodod.hqmc.usmc.mil/PII.asp> under the training tab. Deployed units may postpone annual training 60 days prior to departing CONUS and 60 days upon return to CONUS. All personnel will sign the certificate of completion at the end of the training course. Commands are responsible for providing access to training materials for individuals without network access.

8.2 Audit

Commands will ensure that all subordinate leadership and managers conduct compliance audits within their area(s) of responsibility, using the PII Compliance Checklist located at <https://hqodod.hqmc.usmc.mil/PII.asp>. Special areas of focus will be those dealing with PII on a regular basis such as personnel support, administration, human resources, security, medical, etc. Training certificates shall be kept on file as these are auditable documents. Any deficiencies found will be reported to the Commanding Officer (CO) or Officer-in-Charge (OIC) with a corrective action plan.

8.3 Reporting

Commands will report completion of training and compliance NLT the 10th day of each of the following months: November, February, May, and August using the PII Training Report template located at <https://hqodod.hqmc.usmc.mil/PII.asp>. Reports will be sent up through the chain of command with the MARFORs, MCCDC, and HQMC ARI consolidating subordinate reports and submitting to HQMC_C4IA_IdMGT@usmc.mil.

SECTION 9.0 - DEFINITIONS

Data Aggregation - Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

Disclosure - The transfer of any personal information from a System of Records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Distinguish - To distinguish an individual is to be able to identify that individual either directly or out of a group. Such distinguishable information could be used to contact that person or affect that person positively (e.g., granting benefits) or negatively (e.g., imposing penalties).

Electronic Collection of Information - Any collection of information enabled by IT.

Federal Contractors - The Contractor and its employees are considered agents of the Marine Corps when performing duties during the performance of the contract. Federal Contractors are considered "general public" for purposes of reporting.

Federal Personnel - Officers and employees of the U.S. Government, members of the uniformed services (including members of the reserve), individuals or survivors thereof, entitled to receive immediate or deferred retirement benefits under any retirement program of the U.S. Government (including survivor benefits).

Individual - Any human being, living or dead; including citizens, legal resident aliens, and non-citizens of the United States; and both employees and non-employees of the organization. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual.

Information System (IS) - Any telecommunication or computer-related equipment or interconnected systems or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

Information Technology (IT) - Any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management,

movement, control, display, switching, interchange, transmission, or reception of data or information.

Linkable - A record is linkable to an individual when it contains information that cannot distinguish an individual, but that may be matched or compared with other data elements from a source available to the general public or that is obtainable with moderate effort to distinguish at least one individual. For example, individuals might be identified in a database by home telephone number. The identities of some of the individuals could be determined by comparing this information to publicly available telephone directories.

Linked - A record is linked to an individual when it contains information that cannot distinguish an individual when considered separately, but which could distinguish an individual when combined with other data elements present on the same system or a closely related system. For example, an individual could be identified only by ID #12345 in one database, and another database on the same system could map that ID # to the individual's name and social security number. The records in the first database would be considered "linked" if users were likely to have access to both databases, or could obtain access with minimal effort.

Lost, Stolen, or Compromised Information - Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. Such incidents also are known as breaches.

Maintain - To hold or retain, collect, use, or disseminate records contained in a System of Records.

Major information system - Embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property, or other resources.

National Security Systems - As defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

Official Use - When officials and employees of a DoD Component have demonstrated a need for the use of any record or the information contained therein in the performance of their official duties.

Personally Identifiable Information (PII) - PII is defined in OMB Memorandum M-07-16 as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Personal Identifier - Information associated with a single individual and used to distinguish him or her from other individuals, e.g., name, SSN or other identifying number, symbols, or other identifying particular such as finger or voice print or photograph.

PII Impact Category - For DoD information assurance purposes and in accordance with DoD Instruction 8500.2 and FIPS 199, all PII electronic records shall be assigned an Impact Category (High or Moderate) according to the potential of a negative impact of loss or unauthorized disclosure.

Privacy Act Statements - When an individual is requested to furnish personal information about himself or herself for inclusion in a System of Records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory - A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act System of Records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

Privacy Impact Assessment (PIA) - Analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy policy in standardized machine-readable format - A statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

Record – Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.), about an individual that is maintained by a DoD Component. Information may include, but is not limited to an individual’s education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.

Remote Access – Enclave-level access for authorized users external to the enclave that is established through a controlled access point at the enclave boundary (i.e., remotely logging into a DoD network from outside your official workspace.)

System of Record – A group of any records under the control of any Executive branch agency from which information is retrieved using the name of the individual or by using some personal identifying number, symbol, or other identifying field that is assigned to the individual.

System of Records Notice (SORN) – Public notice of the existence and character of a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

Trace – To trace an individual is to be able to make a determination about a specific aspect of an individual’s activities or status, but without being able to distinguish the individual. For example, an individual’s computer activities might be tracked by a user ID or other identifier that does not reveal the individual’s identity yet allows someone to determine which of the recorded activities were performed by that individual.

SECTION 10.0 - REFERENCES

- (a) 5 U.S.C. 552a, "The Privacy Act of 1974."
- (b) E-Government Act of 2002
- (c) DoD 5200.1-R, DoD Information Security Program
- (d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (e) DoD 5400.11-R, 14 May 07, DoD Privacy Program
- (f) DoD Instruction 5400.16, "Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- (g) DoD Memorandum, DoD Guidance on Protecting PII
- (h) DEPSECDEF Memorandum "Notifying Individuals When Personal Information is Lost, Stolen or Compromised"
- (i) SECNAV Instruction 5211.5E, "Department of the Navy (DON) Privacy Program," December 28, 2005
- (j) Section 3541 of title 44, United States Code, *Federal Information Security Management Act of 2000* (FISMA)
- (k) Federal Information Processing Standards (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems
- (l) National Institute of Standards and Technology (NIST) Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- (m) OMB M-06-16 Protection of Sensitive Agency Information, 23 June 2006
- (n) OMB M-06-19 Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, 12 July 2006
- (o) OMB Memo, M-03-22: "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", 26 September 2003
- (p) OMB Memo 22 May 07: Safeguarding against and responding to the breach of PII

- (q) ALNAV 057/07, "Safeguarding PII from Unauthorized Disclosure."
- (r) GENADMIN, "DON Privacy Impact Assessment Guidance, DON CIO Msg DTG 081547ZFeb07.
- (s) GENADMIN, "DON PII Breach Reporting Guidance", DON CIO Msg DTG 301540ZNov06
- (t) GENADMIN, " Safeguarding Personally Identifiable Information", DON CIO Msg 171952ZApr07
- (u) DoD Instruction 1000.hh "Social Security Number (SSN) Reduction"
- (v) GENADMIN, "Protecting Personally Identifiable Information on DON Shared Drives and Application Based Portals ", DON CIO Msg 201839Z NOV 08
- (w) GENADMIN, "DON Policy Updates for Personal Electronic Devices Security and Application of Email Signature and Encryption", DON CIO Msg 032009Z OCT 08
- (x) GENADMIN, "DON Security Guidance for Personal Electronic Devices," DON CIO Msg 202041Z AUG 07
- (y) MARADMIN 732/07 DATA AT REST ENCRYPTION FOR MOBILE COMPUTING DEVICES AND REMOVABLE STORAGE MEDIA
- (z) NIST Special Publication 800-88: Guidelines for Media Sanitation, September 2006
- (aa) National Industrial Security Program Operating Manual (NISPOM), February 2006
- (bb) Department of Defense (DD) Form 2930, Privacy Impact Assessment November 11, 2008 - <https://hqodod.hqmc.usmc.mil/PII.asp>

SECTION 11.0 - ACRONYM LIST

C&A	Certification and Accreditation
C4 IA	Command, Control, Communications, and Computers, Information Assurance Division
CO	Commanding Officer
DAA	Designated Accrediting Authority
DITPR	DoD IT Portfolio Registry
DOB	Date of Birth
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of the Navy, Chief Information Officer
E.O.	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
HQMC	Headquarters, United States Marine Corps
IA	Information Assurance
IAM	Information Assurance Manager
IS	Information System
IT	Information Technology
MARCORSYSCOM	Marine Corps Systems Command
MCEN	Marine Corps Enterprise Network
MCNOSC	Marine Corps Network Operations and Security Center
MCPAM	Marine Corps Privacy Act Manager
NIST	National Institute of Standards and Technology
OIC	Officer in Charge
OMB	Office of Management and Budget
PA	Privacy Act
PAS	Privacy Act Statement
PASORN	Privacy Act Systems of Records Notice
PED	Portable Electronic Device
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POR	Program of Record
SFTP	Secure File Transfer Protocol
SSL	Secure Socket Layer
SSN	Social Security Number
USC	United States Code
USMC	United States Marine Corps
VPN	Virtual Private Network

ENCLOSURE A - PRIVACY ACT STATEMENT (PAS)

- 1) Identify the PA systems of record notice where you are going to store the information (<http://www.defenselink.mil/privacy/notices/> and <http://privacy.navy.mil> contains a list of PA systems).
- 2) Fill in the following areas: AUTHORITY AND PURPOSE. Under AUTHORITY, please list the Federal law or Executive Order that appears in the systems notice. Under PURPOSE, copy the same information that is contained in the systems notice under Purpose.
- 3) Under ROUTINE USES, address who within and outside the organization will have access to the information. Do not cite "BLANKET ROUTINE USES APPLY".
- 4) Under DISCLOSURE, cite whether or not the disclosure of information is "Voluntary" or "Mandatory". Mandatory is appropriate when a Federal Law or E.O. of the President specifically imposes a requirement to furnish the information and provides a penalty for failure to do so. Voluntary is appropriate if furnishing the information is a condition for granting a benefit or privilege voluntarily sought by the individual.

Most statements will read as follows: DISCLOSURE: Voluntary. However, failure to provide the requested information may result in _____. (This could include not being considered for a position, not being notified in case of an emergency, not being granted a clearance, etc.).

Caveat: Military members are required, by law to provide recall roster info.

ENCLOSURE A (CONT) - PRIVACY ACT STATEMENT (PAS)

GENERAL PURPOSE PRIVACY ACT STATEMENT	
PART A - IDENTIFICATION OF REQUIREMENT	
1. REQUIRING DOCUMENT (Describe - SECNAVINST, OPNAVNOTE, SECNAV ltr, etc.)	2. SPONSOR CODE
3. DESCRIPTIVE TITLE OF REQUIREMENT (Form title, report title, etc.)	
PART B - INFORMATION TO BE FURNISHED TO INDIVIDUAL	
1. AUTHORITY	
2. PRINCIPLE PURPOSE(S)	
3. ROUTINE USE(S)	
4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL NOT PROVIDING INFORMATION	
PART C - IDENTIFICATION OF FORM/REPORT/OTHER REQUIREMENT	
1. FORM NO./REPORT CONTROL SYMBOL/OTHER IDENTIFICATION	PRIVACY ACT STATEMENT

OPNAV 5211/12 (MAR 1992)

ENCLOSURE B - 12 EXCEPTIONS TO THE "NO DISCLOSURE WITHOUT CONSENT" RULE

Note that, with the exception of (b)(2), disclosures under the following exceptions are permissive, but not mandatory.

5 U.S.C. § 552a(b)(1) - refers to those officers and employees of the Agency which maintains the record who have a need for the record in the performance of their duties. This "need to know" exception authorizes the intra-agency disclosure of a record for necessary, official purposes. Any disclosure made pursuant to this exception DOES NOT require an entry on the Accounting Disclosure Form in the applicable record.

5 U.S.C. § 552a(b)(2) - required under 5 U.S.C. §552, as amended. The Privacy Act will never prohibit a disclosure that the FOIA actually requires.

This is the one exception request that will not be processed by the Privacy Act System of Records Manager (records custodian). Any request citing to 5 U.S.C. § 552a(b)(2) will be processed as a FOIA request and will be handled and coordinated by the command's FOIA Coordinator. Any disclosure made pursuant to this exception DOES NOT require an entry on the Accounting Disclosure Form in the applicable record.

5 U.S.C. § 552a(b)(3) - requires Federal Register publication of "each routine use of the records contained in the system, including the categories of users and the purpose of such use." "Routine use" means with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(4) - to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13. Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(5) - to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(6) - to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(7) - to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record. However, unlike the other exception disclosures, accountings disclosures made pursuant to this exception are not to be made available for viewing by the subject of the record.

5 U.S.C. § 552a(b)(8) - to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification of disclosure is transmitted to the last known address of the subject individual.

In addition to the above notification requirement, any disclosure made pursuant to this exception ALSO requires an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(9) - to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee of any such joint committee.

This exception DOES NOT authorize the disclosure of a Privacy Act protected record to an individual Member of Congress acting on his/her own behalf or on behalf of a constituent.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(10) - to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(11) - pursuant to the order of a court of competent. Essentially, the Privacy Act "cannot be used to block the normal course of court proceedings, including court-ordered discovery." However, it should be noted that the Court of Appeals for the District of Columbia

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

5 U.S.C. § 552a(b)(12) - to a consumer reporting agency in accordance with section 3711(e) of Title 31. This disclosure exception was added by the Debt Collection Act of 1982. It authorized agencies to disclose bad-debt information to credit bureaus, but only after the agency has completed a series of due process steps designed to validate the debt and to offer the individual an opportunity to repay it.

Any disclosure made pursuant to this exception DOES require an entry on the Accounting Disclosure Form in the applicable record, which must be made available for viewing to the subject of the record, upon request.

ENCLOSURE C - PII COMPROMISE REPORT

**REPORT OF THEFT/ LOSS/ COMPROMISE OF
PERSONALLY IDENTIFIABLE INFORMATION (PII)**

COMPLETE REPORT WITH ALL INFORMATION KNOWN AT THE TIME OF SUBMISSION, INDICATING IF THE REPORT IS THE INITIAL OR FOLLOW-UP REPORT.

- **QUESTIONS 1 THROUGH 4 ARE REQUIRED FOR THE INITIAL REPORT.**
- **QUESTIONS 5 AND 6 ARE NOT REQUIRED FOR THE INITIAL REPORT BUT MUST BE COMPLETED AS PART OF THE FOLLOW-UP REPORT.**

- INITIAL REPORT WITHIN ONE HOUR OF DISCOVERY OF THEFT/LOSS/COMPROMISE**
- FOLLOW-UP REPORT WITHIN 24 HOURS OF DISCOVERY OF THEFT/LOSS/COMPROMISE**

SERVICE: United States Marine Corps	COMMAND:
DATE / TIME OF INCIDENT:	
US-CERT NUMBER:	NOTE: US-CERT NUMBER WILL NOT BE AVAILABLE FOR INITIAL SUBMISSION, PLEASE INCLUDE NUMER AS PART OF THE FOLLOW UP.

1. TOTAL NUMBER OF INDIVIDUALS WHO'S PII WAS INVOLVED:

- Percentage of Total Military:
- Percentage of Total Civilian:
- Percentage of Total Contractor:
- Percentage of Total Private Citizen:

2. PROVIDE A DESCRIPTION OF THE INCIDENT TO INCLUDE THE CIRCUMSTANCE OF THE COMPROMISE. (Do NOT INCLUDE INDIVIDUAL'S NAMES)

3. LIST THE SPECIFIC DATA ELEMENTS LOST, STOLEN OR COMPROMISED. (NOTE: THIS IS A LIST OF GENERIC DATA ELEMENTS (E.G. NAME, DATE OF BIRTH, HOME ADDRESS, TELEPHONE, SSN,). DO NOT INCLUDE A LIST OF THE SPECIFIC DATA COMPROMISED).

4. WERE ANY SAFEGUARDS IN PLACE TO PROTECT THE DATA?

- No
- Yes

List the safeguards (i.e. encryption, password protection).

5. HAS NOTIFICATION BEEN MADE TO THE INDIVIDUALS AFFECTED?

- No. When will notification start?
- Yes. Detail method of notification:

6. WHAT REMEDIAL EFFORTS WILL BE MADE TO MITIGATE FUTURE COMPROMISES?

ENCLOSURE D - PRIVACY IMPACT ASSESSMENT TEMPLATE



PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

DoD Component Name:

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as “electronic collection” for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel * and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* “Federal personnel” are referred to in the DoD IT Portfolio Repository (DITPR) as “Federal employees.”

b. If “No,” ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes Enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

- No

d. Does the DoD information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes Enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at:
<http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

No

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a System of Records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a System of Records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive or instruction implementing the statute within the DoD Component should be identified.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component. Specify

Other DoD Components. Specify

Other Federal Agencies. Specify

State and Local Agencies. Specify

Contractor (enter name and describe the language in the contract that safeguards PII.) Specify

Other (e.g., commercial providers, colleges). Specify

i. Do individuals have the opportunity to object to the collection of their PII?

Yes **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) **What PII will be collected?** Indicate all individual PII or PII groupings that apply in the table below.

<input type="checkbox"/> Name	<input type="checkbox"/> Other Names Used	<input type="checkbox"/> Social Security Number (SSN)
<input type="checkbox"/> Truncated SSN	<input type="checkbox"/> Driver's License	<input type="checkbox"/> Other ID Number
<input type="checkbox"/> Citizenship	<input type="checkbox"/> Legal Status	<input type="checkbox"/> Gender
<input type="checkbox"/> Race/Ethnicity	<input type="checkbox"/> Birth Date	<input type="checkbox"/> Place of Birth
<input type="checkbox"/> Personal Cell Telephone Number	<input type="checkbox"/> Home Telephone Number	<input type="checkbox"/> Personal Email Address
<input type="checkbox"/> Mailing/Home Address	<input type="checkbox"/> Religious Preference	<input type="checkbox"/> Security Clearance
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Mother's Middle Name	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Marital Status	<input type="checkbox"/> Biometrics	<input type="checkbox"/> Child Information
<input type="checkbox"/> Financial Information	<input type="checkbox"/> Medical Information	<input type="checkbox"/> Disability Information
<input type="checkbox"/> Law Enforcement Information	<input type="checkbox"/> Employment Information	<input type="checkbox"/> Military Records
<input type="checkbox"/> Emergency Contact	<input type="checkbox"/> Education Information	<input type="checkbox"/> Other

If "Other," specify or explain any PII grouping selected.

(2) **What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?**

Describe.

(3) **How will the information be collected?** Indicate all that apply.

- Paper Format
- Telephone Interview
- Email
- Information Sharing from System to System
- Other (Describe)
- Face-to-Face Contact
- Fax
- Web Site

(4) **Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?**

Describe

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

Yes

No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in the DoD information system or electronic collection? Indicate all that apply.

Users Developers System Administrators Contractors

Other (Describe)

d. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

Security Guards
Identification Badges

Cipher Locks

Combination Locks
Closed Circuit Television

Key Cards

Safes

Other (Describe)

(2) Technical Controls. Indicate all that apply.

- User Identification
- Password
- Intrusion Detection System (IDS)
- Encryption
- External Certificate Authority (CA) Certificate
- Common Access Card (CAC)
- Other (Describe)
- Biometrics
- Firewall
- Virtual Private Network (VPN)
- DoD Public Key Infrastructure Certificates

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Access to PII
- Encryption of Backups Containing Sensitive Data
- Backups Secured Off-site
- Other (Describe)

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

- Authorization to Operate (ATO) Date Granted:
- Interim Authorization to Operate (IATO) Date Granted:
- Denial of Authorization to Operate (DATO) Date Granted:
- Interim Authorization to Test (IATT) Date Granted:

No, this DoD Information system does not require certification and accreditation.

f. How do information handling practices at each stage of the “information life cycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals’ privacy?

Describe.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe:

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Other Official (to be used at Component discretion)

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Other Official (to be used at Component discretion)

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Component Senior Information Assurance Officer or Designee

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Component Privacy Officer

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Component CIO (Reviewing Official)

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

ENCLOSURE E - SECURITY CONTROLS

In addition to the PII-specific protection measures described earlier in this section, many types of technical and operational security controls are available to safeguard the confidentiality of PII. These controls are often already available on a system to protect other types of data processed, stored, or transmitted by the system. The security controls listed in *Department of Defense Instruction 8500.2, Information Assurance Implementation*, address general protections of data and systems. The items listed below are some of the DoDI 8500.2 controls that can be used to help safeguard the confidentiality of PII. Note that some of these controls may not be in the recommended set of security controls for the baselines identified in DoDI 8500.2 (e.g., a control might only be recommended for MAC I system). In addition to the controls listed below, DoDI 8500.2 contains many other controls that can be used to help protect PII, such as incident response controls.

- **Access Enforcement (CFA-1, ECAN-1, EBRU-1, PRNK-1, ECCD-1, ECSD-2).** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways. One example is implementing role-based access control and configuring it so that each user can access only the pieces of data necessary for the user's role. Another example is only permitting users to access PII through an application that tightly restricts their access to the PII, instead of permitting users to directly access the databases or files containing PII.⁴⁴ Encrypting stored information is also an option for implementing access enforcement.⁴⁵ OMB M-07-16 specifies that Federal agencies must "encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing".
- **Separation of Duties (ECLP-1).** Organizations can enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.
- **Least Privilege (ECLP-1).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII data, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.
- **Remote Access (EBRP-1, EBRU-1).** Organizations can choose to prohibit or strictly limit remote access to PII. If remote access is permitted, the organization can ensure that the communications are encrypted.
- **Access Control for Mobile Devices (ECWN-1).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities). Some organizations choose to forbid all telework and remote access involving higher-impact instances of PII so that the information will not leave the organization's physical boundaries. If access is permitted, the organization can ensure that the devices are properly secured and

regularly scan the devices to verify their security status (e.g., antivirus software enabled and up-to-date, operating system fully patched).

- **Auditable Events (ECAR-3).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
- **Audit Monitoring, Analysis, and Reporting (ECAT-1, E3.3.9).** Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
- **User Identification and Authentication (IAIA-1).** Users can be uniquely identified and authenticated before accessing PII.⁴⁶ The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole. OMB M-07-16 specifies that Federal agencies must “allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access,” and also must “use a ‘time-out’ function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity.”
- **Media Access (PEDI-1, PEPF-1).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.
- **Media Marking (ECML-1).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. The organization could exempt specific types of media or output from labeling so long as it remains within a secure environment. Examples of labeling are cover sheets on printouts and paper labels on digital media.
- **Media Storage (PESS-1, ECCR-1).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.
- **Media Transport (NIST MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization’s controlled areas. Examples of protective measures are encrypting stored information and locking the media in a container.
- **Media Sanitization (PECS-1, PEDD-1).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.⁴⁷ An example is degaussing a hard drive—applying a magnetic field to the drive to render it unusable.
- **Transmission Confidentiality (ECCT-1).** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.
- **Transmission Integrity (ECTM-1).** Organizations can protect the integrity of transmitted PII. This is most often accomplished by ensuring the data is not tampered with during transmission by using encryption, intrusion detection systems, firewalls, etc.