Headquarters Marine Corps
Command, Control,
Communications and Computers (C4)
Cybersecurity Division

United States Marine Corps Enterprise Cybersecurity Directive

011 Personally Identifiable Information
Version 2.0

30 November 2011

FOR OFFICIAL USE ONLY

This page intentionally left blank

FOREWORD

The Marine Corps Senior Information Assurance Official (SIAO) issues Marine Corps Enterprise Cyber Security Directives (ECSDs). The ECSD series provides modules that guide the implementation of policy direction 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) as well as other Marine Corps information systems. 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). The Marine Corps ECSD series will be the authoritative source for implementation of cybersecurity policy direction.

This module, Personally Identifiable Information (PII), outlines the policy and procedures for the collection, safeguarding, and maintenance of all PII across the Marine Corps.

Reviewed and Approved by:

K. J. NALLY
BRIGADIER GENERAL, U.S. MARINE CORPS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS

R. A. LETTEER
MARINE CORPS SENIOR INFORMATION ASSURANCE OFFICIAL
CHIEF, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS, CYBERSECURITY DIVISION

DOCUMENT CONFIGURATION CONTROL

Version	**Release Date**	**Summary of Changes**
Version 1.0	August 4, 2003	Original published version
Version 2.0	November 30, 2011	Updated from the original version.

Table of Contents

LIST OF FIGURES

EXECUTIVE SUMMARY

This ECSD provides techniques and procedures for the collection, safeguarding, and maintenance of PII in accordance with Federal, Department of Defense (DoD), Department of the Navy (DON), and Marine Corps policy. This document serves as a foundation for network infrastructure components to use in developing and implementing their Information Technology (IT) security programs. It incorporates procedures in use by security personnel throughout the Marine Corps as well as other federal entities that have previously established network security foundations.

PII is any information that can be used to distinguish or trace an individual's identity such as their name, Social Security Number (SSN), date and place of birth (DOB/POB), mother's maiden name, biometric records, and any other information that is linked or linkable to a specific individual. The protection of PII is a top Marine Corps priority that was further emphasized by the August 23, 2011 Commandant of the Marine Corps (CMC) White Letter NO. 2-11, "*Cyber Awareness and Accountability*," which addresses compliance with PII policies and command accountability for those who have compromised PII.

This document addresses how to maintain compliance when PII is present, specifically regarding the proper collection, safeguarding, and maintenance of PII. Additionally, this document has been amended to incorporate policy for the reduction of SSN use across the Marine Corps. For policy or procedural clarification email: HQMC_C4CY_IDMGT@usmc.mil.

SECTION 1.0: INTRODUCTION

1.1 BACKGROUND

This Marine Corps ECSD 011, PII, provides direction for the secure use and protection of PII throughout the Marine Corps, to include all subordinate commands, bases, and organizations.

1.2 PURPOSE

MCO 5239.2 formally establishes the MCIAP and defines the responsibilities for protecting the Marine Corps information infrastructure as well as delineating directives, instructions, and guidance governing DoD Information Assurance (IA). Marine Corps ECSD 011, details guidance on the collection, safeguarding, and maintenance of PII. The Marine Corps recognizes its responsibility to balance the need to maintain government records while protecting individuals' privacy. This ECSD shall provide individuals with the necessary tools for compliance when managing PII and ways to mitigate its loss or compromise. It will also supplement guidance outlined in Secretary of the Navy (SECNAV) Instruction 5211.5E, "DON Privacy Program," (reference (a)) and DoD 5400.11-R, "DoD Privacy Program," (reference (b)).

1.3 APPLICABILITY AND, SCOPE

1.3.1 Applicability

This ECSD applies to:

- Marine Corps components, organizations, and personnel (government and non-government employees) that operate aboard Marine Corps facilities and/or access Marine Corps Information Technology (IT) systems. This includes any networks that process Marine Corps data whether stand alone, contractor provided, or directly connected to the MCEN.

- Marine Corps military personnel who are subject to disciplinary action under the Uniform Code of Military Justice and or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this policy manual. Civilian and contractor employees are subject to criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this policy.

1.3.2 Scope

Per MCO 5400.52, DON Deputy Chief Information Officer Marine Corps Roles and Responsibilities, Headquarters, Marine Corps (HQMC) Command, Control, Communications, and Computers (C4) is responsible for all networks and networked systems within the Marine Corps. The MCEN is defined as the Marine Corps' network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate in accordance with section 1.3.1.

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 (IS)/ IT 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.

1.3.3 Objectives

To ensure that the Marine Corps:

- Is compliant with all laws, regulations, and policies governing the management of PII, including but not limited to: PII in IT systems, reduction of SSN use, incident reporting when a breach of PII occurs, and collection of PII as it relates to section 552a of title 5 United States Code, the Privacy Act of 1974, as amended (reference (c)).

- Personnel using Marine Corps information systems receive PII handling and security training commensurate with their duties and responsibilities.

- PII security-related technology efforts are responsive to Marine Corps requirements.

- Encourages interoperability between DON enclaves and DoD agencies, as required.

- Meets compliance with this ECSD and other DoD/SECNAV PII policies, instructions, and directives by implementing an aggressive PII security program.

1.3.4 Action

This policy will be reviewed on a semi-annual basis. This ECSD takes precedence over all previous Marine Corps messages, instructions, and policies concerning PII.

- All Marine Corps Commands shall implement this ECSD within their organizations.

- All operating activities shall budget for and execute the actions necessary to comply with this ECSD.

1.4 CANCELLATION

This ECSD cancels Marine Administrative Message (MARADMINs) 344/07, 348/06, 431/07, 443/07, 613/07, and 491/08. It also replaces Enterprise Information Assurance Directive (EIAD) 011, PII, dated April 9, 2009.

1.5 DISTRIBUTION

This document is approved for limited distribution to only those individuals possessing DoD Public Key Infrastructure (PKI) certificates and an official need to access this document. Access to ECSDs may be gained via the HQMC C4, Cybersecurity (CY) web page at:

https://hqdod.hqmc.usmc.mil/Orders.asp

1.6 STRUCTURE

This ECSD is organized into six major sections; PII, Collecting PII, Safeguarding PII, PII Breach and Incident Response, Maintenance and Disposal of PII, and Compliance and Recurring Requirements.

1.7 RECOMMENDATIONS

Recommendations for change or amendment to these standards may be submitted in writing through the HQMC C4 CY Identity Management Branch at: HQMC_C4CY_IDMGT@USMC.MIL.

Recommendations will be evaluated and coordinated as necessary before taking action to change or amend this ECSD.

1.8 EFFECTIVE DATE

This ECSD is effective upon publication.

SECTION 2.0: RESPONSIBILITIES

2.1 DIRECTOR, C4

Director, C4/DON Deputy Chief Information Officer [Marine Corps] (CIO) will:

- Establish policy for the collection, safeguarding, and maintenance of PII.

- Interpret Federal and DoD guidance and establish Marine Corps strategy for reduction of SSN's across the Enterprise.

- Serve as the Service reviewing official for all Privacy Impact Assessments (PIA); coordinating with the Marine Corps Privacy Act (PA) Manager, the Department of the Navy CIO (DON CIO), and ensuring compliance with the E-Government Act of 2002 (reference (d)).

- Coordinate with DON CIO to ensure approved and summary PIAs are available on the DON CIO public website.

- Ensure that all breaches of PII are coordinated with DON CIO, as necessary, and processed according to Federal guidance.

- Assist DON CIO, as necessary, to ensure compliance with all Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB), and Congressional reporting requirements.

2.2 DIRECTOR OF CMC ADMINISTRATION AND RESOURCE MANAGEMENT (ARI)

The Director of CMC ARI will:

- Serve as the principal PA Officer for the Marine Corps.

- Oversee the Marine Corps PA program and ensure compliance with (reference (c)).

- Assign a Marine Corps PA Manager.

2.2.1 CMC Administration and Resource Management Security Division and Freedom of Information Act (ARI-SF FOIA) PA Manager

As directed by the Director, CMC ARI, the CMC ARI-SF PA Manager will:

- Review and resolve PA complaints.

- Develop Marine Corps PA education, training, and awareness programs.

- Approve and manage PA Systems of Record Notices (PASORN).

- Serve as the PA Coordinator for all HQMC components (exceptions: Marine Corps Systems Command, Marine Corps Combat Development Command, and Marine Corps Recruiting Command).

- Provide FISMA reporting requirements as needed to the DON PA officer.

- Review all PIAs for PA impact.

- Manage the PASORN, OMB number, and Federal Register notice process for all IT systems.

- Provide assistance for PII breach reports as requested.

2.3 MARINE CORPS TRAINING AND EDUCATION COMMAND (TECOM)

TECOM will:

- Provide PII training numbers via MarineNet as requested by HQMC C4 CY and as specified in Section 8.1, of this ECSD.

2.4 COMMANDING GENERALS, COMMANDING OFFICERS (CG/CO)

Marine Corps CGs, COs will:

- Comply with DoD, DON, and Marine Corps policy for the collection, safeguarding, and maintenance of PII.

- Reduce the use of the SSN, to the greatest extent practicable, as specified in Section 4.5.

- Ensure all personnel are compliant with annual training requirements in accordance with Section 8.1 of this ECSD.

- Ensure the appropriate assigned personnel are completing PII spot checks in accordance with Section 8.2 of this ECSD.

- Report all breaches of PII and make notifications to affected person(s) in accordance with Section 6.0 of this ECSD.

2.5 PROGRAM MANAGERS (PM) AND SYSTEM OWNERS (SO)

PM's and SO's will:

- Oversee the full lifecycle of collection, maintenance, use, and dissemination of all systems and information under their responsibility.

- Ensure that all personnel, who have access to PII, are properly trained on their responsibilities.

- Appoint an Cybersecurity Manager (CSM)/Information Assurance Manager (IAM) for the program or system in accordance with DoD Instruction 8500.2, "IA Implementation," (reference (e)).

- Establish appropriate administrative, technical, and physical safeguards to ensure that information is protected from unauthorized alteration, destruction, or disclosure in accordance with (reference (e)).

- Protect information from reasonably anticipated threats or hazards.

- Reduce the use of the SSN to the greatest extent practicable and in accordance with Section 4.5 of this ECSD.

2.6 CSM'S/IAM'S

CSM's/IAM's will:

- Verify, sign, and forward PIAs, in coordination with the Program Manager (PM), to HQMC C4 CY in accordance with Section 4.3.1 of this ECSD.

- Reduce the use of the SSN to the greatest extent practicable and in accordance with Section 4.5 of this ECSD.

- Advocate PII policies and procedures as specified by this ECSD.

2.7 INFORMATION OWNERS, DATA HANDLERS, DATA USERS

All Information Owners, Data Handlers and Data Users will:

- Follow all guidance for collecting, handling, safeguarding, and disposing of PII as specified by this ECSD.

- Complete annual PII training as outlined in sub-section 8.1 of this ECSD.

- Report any breach of PII as outlined in Section 6.0 of this ECSD.

- Identify processes to reduce the use of the SSN to the greatest extent practicable and as outlined in Section 4.5 of this ECSD.

SECTION 3.0: PII

The protection of PII is a top Marine Corps priority that helps ensure the privacy and safety of all Marines, Civilian Marines, and contractor personnel. CMC White Letter 2-11, "Cyber Awareness and Accountability," (reference (f), addresses compliance with PII policies and Command accountability for those who have compromised PII. Commanders shall implement necessary procedures to manage their individual Privacy programs while implementing all aspects of this ECSD.

As defined in reference (b), PII is any information that can be used to distinguish or trace an individual's identity such as the name, SSN, DOB/POB, mother's maiden name, biometric records, and any other information that is linked or linkable to a specified individual. The following sub-sections further detail the different types of PII elements and their categorization.

3.1 PII IMPACT CATEGORIES

DoD CIO Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information," (reference (g)), designates that all PII electronic records be assigned an impact category of high or moderate as determined by the potential negative impact due to loss or unauthorized disclosure. This ECSD expands on reference (g) and assigns specific types of PII to these categories.

3.1.1 High Impact PII

High impact PII is any DoD-wide, organizational (e.g., unit or office), or program or project level electronic or paper records containing PII stored on a single device or accessible through a single application or service, whether or not the compilation is subject to reference (c). High impact PII is any information that can positively distinguish an individual and have an adverse affect on their personal life if compromised. These elements include, but are not limited to, any of the following when presented with the name: SSN, medical information, and financial information.

High impact PII can also include the combination of multiple elements, that when presented together, can positively distinguish an individual and adversely affect them in their personal life if compromised. These elements include but are not limited to: name, date of birth, family member's names, home address, personal email address, and personal cell phone number.

If high impact PII is compromised the responsible command shall notify the affected individual(s) regarding the potential breach. This process is further outlined in Section 6.0.

3.1.2 Moderate Impact PII

Moderate impact PII contains elements that identify an individual in their work environment including, but not limited to: work address, work phone, email address, pay grade, and rank. Moderate Impact PII that is compromised is not required to be reported and generally is information that is releasable to the public.

SECTION 4.0: COLLECTING PII

The Marine Corps collects personal information for several reasons to include hiring purposes, to pay, locate, and educate individuals, and to provide services. Federal law mandates strict guidelines when information is collected from individuals. Individuals collecting PII shall be in compliance with Section 4.0 of this ECSD and references (a), (b), (c) and (d). Reference (c) only applies to Executive Branch agencies and does not encompass all PII elements and requirements covered by this ECSD.

4.1 PRIVACY ACT OF 1974 / SYSTEMS OF RECORDS NOTICE

Reference (c) requires all Executive Branch Agencies to have a completed PASORN for any electronic system or application that retrieves information using the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. If a PASORN is required, it must be published in the Federal Register for a 30-day public comment period announcing the collection. A PASORN informs the public regarding the data elements being collected, the purpose of the 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 a personal identifier.

The DON maintains a list of all PASORNs at http://privacy.navy.mil. If an individual is unaware if their system or program requires a PASORN, contact the Marine Corps PA Manager at SMBHQMCPRIVACYACT@USMC.MIL.

4.2 COLLECTING PII FROM AN INDIVIDUAL (PRIVACY ACT STATEMENT)

When an individual is requested to provide personal information (e.g., name, date of birth, SSN) 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).

A PAS enables an individual to make an informed decision on whether to provide the information being requested by identifying the authority for collecting the information, the purpose for collecting the data, identifying the routine uses of the data, and explaining whether disclosure of the information is voluntary or mandatory. If the personal information solicited will not be incorporated into a paper-based or electronic System of Records, a PAS is not required. Personal information obtained without a PAS shall not be incorporated into any System of Records. An example PAS is provided at Enclosure A.

4.3 SYSTEM COMPLIANCE: PRIVACY IMPACT ASSESSMENT

Reference (d) requires all federal government agencies to conduct a PIA for all new or substantially changed IS/IT systems that collect, maintain, or disseminate PII. A PIA allows for the evaluation and mitigation of possible privacy risks throughout the lifecycle of a program or system. PIAs provide accountability for the information being collected and maintained in the Marine Corps.

In accordance with DoD Instruction 5400.16, “Privacy Impact Assessment (PIA) Guidance,” (reference (h)) and reference (d), all system owners/PMs will conduct a PIA on every IT system under their responsibility including: Programs of Record (POR), non-POR, and locally created systems (e.g., databases, local websites, and limited use applications hosted at the command).

4.3.1 Processing a PIA

Every IT initiative shall at a minimum have a completed Section 1 of DD Form 2930, “PIA,” (reference (i)), which is used to determine if the system processes PII and if further analysis is required.

If the initiative does not process PII, the PM and IAM shall sign Section 4 of Reference (h) and email it to HQMC C4 CY at HQMC_C4CY_IDMGT@usmc.mil.

If the initiative does process PII, reference (i) shall be completed and submitted to HQMC C4 CY. A complete PIA shall contain the following signatures: PM, IAM, PA Manager, MCEN Authorizing Official (AO)/Marine Corps Designated Accrediting Authority (DAA), and DON CIO. The PIA will be submitted as part of the Marine Corps Certification & Accreditation (C&A) process.

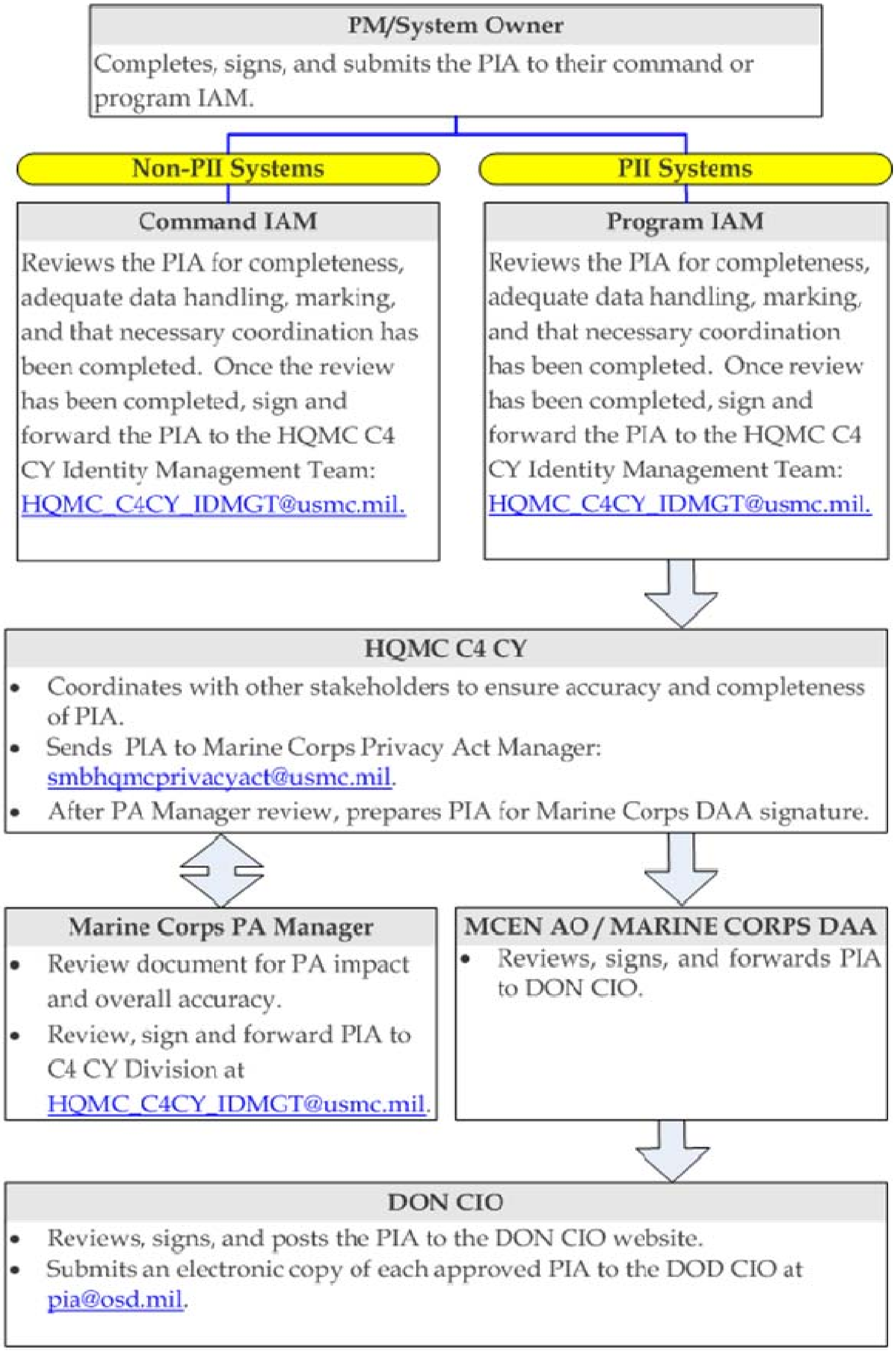
PIAs pertaining to a POR are submitted as part of the overall C&A package to Marine Corps Systems Command (MARCORSYSCOM) and to the MCEN C&A Team, as per Marine Corps EIAD/ECSD 018, Marine Corps Certification and Accreditation Process (MCCAP). Non-POR systems (e.g., a locally created Microsoft Access database) are submitted to their command IAM. If the PA Manager determines that a PA Systems of Record Notice (SORN) is required, the PIA shall be completed; however an IT initiative will not be accredited until a PASORN is completed.

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

All final PIAs will be posted on the DON CIO website at: http://www.doncio.navy.mil. For assistance with completing a PIA, contact HQMC_C4CY_IDMGT@usmc.mil.

Figure 1 provides an overview of PIA roles and responsibilities.

Figure 1: PIA Roles and Responsibilities



PM/System Owner

Completes, signs, and submits the PIA to their command or program IAM.

Non-PII Systems

PII Systems

Command IAM

Reviews the PIA for completeness, adequate data handling, marking, and that necessary coordination has been completed. Once the review has been completed, sign and forward the PIA to the HQMC C4 CY Identity Management Team: HQMC_C4CY_IDMGT@usmc.mil.

Program IAM

Reviews the PIA for completeness, adequate data handling, marking, and that necessary coordination has been completed. Once review has been completed, sign and forward the PIA to the HQMC C4 CY Identity Management Team: HQMC_C4CY_IDMGT@usmc.mil.

HQMC C4 CY

- Coordinates with other stakeholders to ensure accuracy and completeness of PIA.
- Sends PIA to Marine Corps Privacy Act Manager: smbhqmcprivacyact@usmc.mil.
- After PA Manager review, prepares PIA for Marine Corps DAA signature.

Marine Corps PA Manager

- Review document for PA impact and overall accuracy.
- Review, sign and forward PIA to C4 CY Division at HQMC_C4CY_IDMGT@usmc.mil.

MCEN AO / MARINE CORPS DAA

- Reviews, signs, and forwards PIA to DON CIO.

DON CIO

- Reviews, signs, and posts the PIA to the DON CIO website.
- Submits an electronic copy of each approved PIA to the DOD CIO at pia@osd.mil.

4.4 COLLECTING SOCIAL SECURITY NUMBERS

The process for collecting, handling, and maintaining the SSN is regulated by Federal, DoD, and Marine Corps policy. All individuals should be aware of their rights when disclosing their SSN. It is unlawful for any Federal, State, or local government agency to deny an individual a right, benefit, or privilege provided by law because an individual refuses to provide their SSN unless a statute, executive order, regulation, or policy requires the SSN be furnished (reference (b)). When collecting, maintaining, or requesting the SSN from an individual the responsible manager will:

- Inform the individual whether the disclosure is voluntary or mandatory, by what authority the SSN is being collected, and how it will be used.

- Ensure the collection is compliant with one of the 12 acceptable uses for SSN collection as identified in Office of the Undersecretary of Defense (OUSD) (P&R) Directive Type Memorandum 07-015 “DoD Social Security Number Reduction Plan”(reference (j).

- Use other identifiers in lieu of the SSN to the greatest extent practicable.

- Ensure the collection meets the requirements in accordance with Section 4.0 of this ECSD (i.e., PASORN, PIA, and PAS).

- Ensure the SSN is properly safeguarded in accordance with Section 5.0 of this ECSD.

- Be compliant with the DON CIO/Marine Corps SSN Reduction Plan described in Section 4.5 of this ECSD.

4.5 SSN REDUCTION PLAN

The Marine Corps, working with DON CIO, developed a three-phased SSN reduction plan. The plan addresses the reduction of SSNs in all Marine Corps forms, IT Systems, and implements the use of the Electronic Data Interchange Personal Identifier (EDI-PI), hereafter known as the DoD ID Number. In all cases collection of the SSN shall be minimized to the greatest extent practicable. Individuals that collect, maintain, use, or disseminate the SSN shall continuously review the use of the SSN and determine if it can be eliminated, restricted, or concealed.

4.5.1 Reduction of SSN in all Forms (Phase One)

Phase One of the SSN reduction plan requires Forms Management Officials to review and justify SSN collection for all forms per MARADMIN 646/10, “Department of the Navy Social Security Reduction Plan for Forms Phase One,” (reference (k)). The review requires justification for the collection of the SSN using SECNAV Form 5213-1, “SSN Reduction Review,” (reference (l)). This effort is on-going and Commands shall continue to reduce the use of the SSN in all forms to the maximum extent practicable.

4.5.2 Reduction of SSN in all IT Systems (Phase Two)

Phase Two of the SSN reduction plan requires PMs and assigned Functional Area Managers (FAMs) to review and justify SSN collection for all DoD IT Portfolio Registry (DITPR-DON) registered systems. PMs/FAMs shall complete and upload reference (l) to the PIA/PA tab in DITPR-DON and answer all SSN related questions.

Email HQMC_C4CY_IDMGT@USMC.MIL if PMs and FAMs are having trouble accessing DITPR-DON This effort is on-going and Commands shall continue to reduce the use of the SSN in all IT systems to the maximum extent practicable

4.5.3 Implementation of the DOD ID Number (Phase Three)

Phase Three of the SSN reduction plan requires transition to the EDI-PI per ALNAV 0XX/11, “Department of the Navy Social Security Number Reduction Plan Phase Three” (reference (m)) and USD(P&R) memorandum, “Updated Plan for the Removal of Social Security Numbers from Department of Defense Identification Cards,” (reference (n)).

The EDI-PI, commonly referred to as the DoD ID number, shall be used as a substitute for the SSN to the greatest extent practicable in all forms and IT systems when resources are available and/or interfacing systems implement the use of the number. To ensure that sensitive information is not accessible due to knowledge of the DoD ID number the following guidelines will be followed:

- Presence or knowledge of an individual’s DoD ID number alone shall be considered as no more significant than presence or knowledge of an individual’s unique name; it does not constitute any level of authority to act on that individual’s behalf.

- An individual’s DoD ID number and name shall be treated as a single factor in authentication transactions. A second authentication factor shall always be provided in addition to the DoD ID number and/or name.

- The DoD ID number shall only be used for DoD business purposes. This may include transactions with entities outside of the Department as long as individuals are acting on behalf or in support of the DoD.

- The DoD ID number shall not be shared with other federal agencies unless both the DoD and the recipient agency agree upon a memorandum of understanding (MOU). All MOU’s shall be submitted to HQMC_C4CY_IDMGT@USMC.MIL for approval. HQMC C4 CY will share the MOU with DON CIO, which will also submit the MOU to DoD.

4.6 COLLECTING PII FROM THIRD PARTIES

When possible, all PII shall be collected directly from the individual. However, in cases where this is not practicable PII may be collected from third parties when:

- 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.

- The individual requests or consents to contacting another person to obtain the information.

4.7 DISCLOSURE OF PII

reference (c) forbids disclosure of personal information to those who are not entitled to view or access it; this concept is referred to as the "No Disclosure without Consent" Rule. Disclosing personal information is punishable by a 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 Record 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 (reference (b)). However, there are several exceptions to this rule; these exceptions are detailed in Enclosure B. If you have any questions regarding these exceptions, contact the Marine Corps Privacy Act Manager at SMBHQMCPRIVACYACT@USMC.MIL

SECTION 5.0: SAFEGUARDING PII

Proper safeguarding of PII is critical to reducing the possibility of the loss or compromise of sensitive information that can adversely impact the integrity of the Marine Corps and its personnel. PII shall only be viewed by persons with an "official need to know." These are individuals that collect and handle PII as a specific aspect of their job function. No other individuals shall be able to access or view an individual's personal information without having an official need for that information. If information is viewed or accessed by individuals without an official need to know a PII breach has occurred and should be reported based on the process outlined in sub-section 6.1. This section outlines how to successfully safeguard PII in both electronic and paper forms.

5.1 PAPER DOCUMENTS

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

- Mark each page containing PII "For Official Use Only (FOUO)."
- Ensure the document has a cover sheet stating, "FOUO."
- Ensure the document is only accessible to individuals with an official need to know.
- Ensure documents are not easily accessible and at a minimum locked securely.
- Properly dispose of all PII in accordance with the guidelines in sub-section 7.1.

5.2 ELECTRONIC FILES

The potential loss of PII stored in electronic files can have a catastrophic impact due to the accessibility, portability, and potential volume that can exist. Some of the Department's largest PII breaches have included the loss of improperly managed laptops or Compact Disk (CDs) that have contained thousands of records. PII shall never be permissible on personal computers or devices. All PII shall only be maintained on official DoD assets.

Per General Administrative Messages (GENADMIN), "Protecting Personally Identifiable Information on DON Shared Drives and Application Based Portals," reference (o), when PII is being stored on shared drives, portals, or other network devices the information will:

- At a minimum be password protected.
- Only be accessible to individuals with an official need to know (this includes all shared/public folders maintained in Microsoft Outlook).

5.3 WEBSITES

OSD Memorandum 13798-10, “Social Security Numbers Exposed on Public Facing and Open Government Websites,” reference (p) mandates that full and partial SSNs shall not be posted on any public facing or open government website in any form; this includes all high impact PII elements, as identified in sub-section 3.1.1. All internal Marine Corps websites providing access to or holding PII, at a minimum, will be:

- Secured in a manner consistent with current encryption and authentication mechanisms, i.e. Secure Socket Layer (SSL) and PKI.

- Limited to only those individuals with an official need to know.

5.4 EMAIL

The most common breach of PII in the Marine Corps occurs by email. The majority of these incidents occur due to lack of awareness by the sender or recipient that PII is contained within the email. When transmitting an email that contains PII the individual, at a minimum, will:

- Digitally sign and encrypt using DoD approved PKI certificates.

- Include “FOUO:” in the subject line.

- Place the statement “FOR OFFICIAL USE ONLY (FOUO) - PRIVACY SENSITIVE. ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES,” in the body of the email.

5.5 PORTABLE ELECTRONIC DEVICES AND MOBILE STORAGE DEVICES

Any Portable Electronic Device (PED) or mobile storage device that processes or stores electronic records containing PII will:

- Be restricted to only DoD authorized workplaces.

- Only be removed from DoD workplaces when being used for official use.

- At a minimum, encrypt data transmissions, data-in-transit (DIT) and data-at-rest (DAR) per MARADMIN 732/07, “Data at Rest Encryption for Mobile Computing Devices and Removable Storage Media,” (reference (q). The validated encryption module must be implemented in accordance with the Cryptographic Module Validation Program per Federal Information Processing Standards (FIPS) Publication 140-2 reference (t).

5.5.1. Removal of Portable Electronic Devices or Mobile Storage Devices

When operational need requires moving PEDs or removable storage device/media PEDs from DoD authorized workplaces, the device containing PII will:

- Be signed in and out with a supervising official designated in writing by senior leadership.
- Be configured to require certificate-based authentication for log on, when possible.
- Implement a screen lock with a specified period of inactivity not to exceed 15 minutes.
- Further guidance on portable electronic devices can be found in ECSD 005: PEDs reference (u).

5.6 REMOTE ACCESS

Remote access to high impact PII electronic records is highly discouraged. The download or remote storage of PII records is prohibited unless approved in writing by the MCEN AO/Marine Corps DAA.

Only authorized DoD devices shall be used for remote access. Any remote access solution will:

- 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 (ECRC)-1, Resource Control as specified in reference (e).

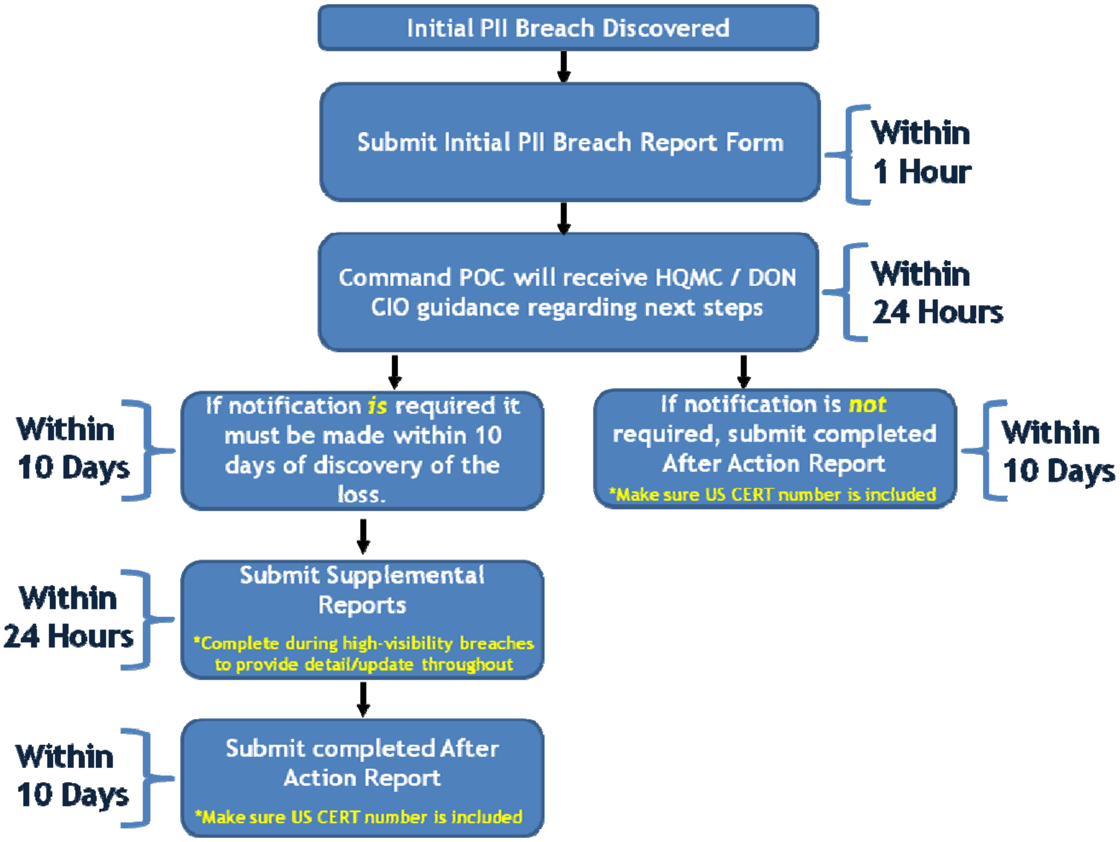
SECTION 6.0: PII BREACH AND INCIDENT RESPONSE

A breach of PII can occur when PII is lost, stolen, released or viewed without proper need, improperly distributed, or incorrectly disposed. Anytime PII is potentially compromised, it constitutes a PII Breach. The most common breaches of PII in the Marine Corps include: sending unencrypted email, loss/theft of laptops, misplacing paper documents, and inappropriate information dissemination to individuals without an official need to know.

Federal reporting requirements established by the FISMA Act of 2002 and updated procedures established in OMB memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," (Reference (v)) require all incidents involving PII to be reported to the Federal incident response center [United States Computer Emergency Readiness Team (US-CERT)] within one hour of discovery.

To meet Federal, DON, and Marine Corps policy each time a breach of PII occurs an official breach report shall be processed in accordance with the procedures described in this section. Figure 2 provides an overview of the PII breach reporting process:

Figure 2: PII Breach Reporting Process


Initial PII Breach Discovered
Submit Initial PII Breach Report Form
Within 1 Hour
Command POC will receive HQMC / DON CIO guidance regarding next steps
Within 24 Hours
Within 10 Days
If notification is required it must be made within 10 days of discovery of the loss.
If notification is not required, submit completed After Action Report
*Make sure US CERT number is included
Within 10 Days
Within 24 Hours
Submit Supplemental Reports
*Complete during high-visibility breaches to provide detail/update throughout
Within 10 Days
Submit completed After Action Report
*Make sure US CERT number is included

6.1 REPORTING PROCEDURES

As outlined in Figure 2 above, when a PII breach has occurred an initial report shall be submitted within one hour of discovery of the incident using OPNAV Form 5211/13, "DON Loss or Compromise of PII Breach Reporting Form," reference (w). Reference (w) has been automated to submit to all necessary agencies/offices (e.g., US CERT, HQMC, and DON CIO). The initial report can be submitted by selecting the "Submit Initial Report for Marine Corps Breaches" option at the bottom of the form.

Once the initial report has been submitted HQMC C4 CY shall provide guidance notifying the reporting command of next steps. HQMC C4 CY shall make the determination to the reporting command if notification is or is not required to the affected person(s). Typically, notification is required when high impact PII elements are exposed in an uncontrolled manner. Figure 3 provides examples of both notification scenarios.

Figure 3: Examples of PII Breaches

These breaches may or may not require written notification to the affected person(s).

Written notification **is** required	• A laptop was stolen that contained a Marine's name and SSN. The laptop was not DAR encrypted. • An email was sent unencrypted, outside of the DoD network that contained Marine names and sensitive health information. • A file was stolen that contained a Marine's home address, family members' names and cell-phone numbers, and personal email addresses.
Written notification **is not** required	• A laptop was stolen that contained a Marine's name and SSN. The laptop was DAR encrypted. • An email was sent unencrypted that contained Marines' names and sensitive health information – however the email stayed within the DoD network and was only sent to Trusted Agents of that information.

All breach reports submitted require the reporting command to complete OPNAV Form 5211/14, "DON Loss or Compromise of PII After Action Reporting Form," reference (x), within 10 days of the initial notification. Reference (x) must include the US CERT number to officially close the incident. The US CERT number can be retrieved by emailing (soc@us-cert.gov) or calling US CERT (888-282-0870) if it has not been provided to the reporting Command.

All breach reporting forms and procedures can be found at: https://hqdod.hqmc.usmc.mil/PII.asp.

6.1.1 Procedures when Notification to the Affected Person(s) is required.

If notification is required to the affected person(s) it shall be made by the reporting command within 10 days of discovery of the incident to the home address or via digitally signed email to the affected individual(s). A sample notification letter along with other PII resources can be found on the HQMC C4 CY PII website at: https://hqdod.hqmc.usmc.mil/PII.asp.

If additional information has been discovered a supplemental report should be submitted by selecting the supplemental tab in Reference (u) and resubmitting. Once notification has been made the reporting command shall submit Reference (v) with the confirmation of the date notification was made, the US CERT number, and lessons learned.

6.1.2 Procedures when Notification to the Affected Person(s) is not required.

If notification is not required to the affected person(s) the reporting command shall submit Reference (v) with the US CERT number and lessons learned to officially close the incident.

6.2 PENALTIES

A breach of PII may have major implications for the individual(s) responsible for the loss or compromise of the information and may lead to disciplinary actions punishable under the Uniform Code of Military Justice. Further civil or criminal actions may be taken against the employee, and 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. The CMC further emphasized Command accountability for those individuals responsible for PII breaches in Reference (f). Local Commanders are encouraged to evaluate their PII programs and set forth appropriate disciplinary actions.

6.3 REPORTING TO EXTERNAL INDIVIDUALS AND ENTITIES

While commands will report all suspected or confirmed breaches within one hour 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 C4 CY PII lead, in coordination with DON CIO, will make a final determination if a breach warrants additional notification(s).

6.4 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. If the loss involves personal bank information the individual should notify their bank and follow their local procedures.

6.5 REMEDIATION

The steps to remediate a PII breach vary based on the severity and type of breach. HQMC C4 CY will evaluate the risk factors of the PII breach and determine whether or not notification is necessary. Figure 4 provides a list of remediation activities for some of the most common PII breaches.

Figure 4: Breach Remediation Activities

Breach Type	Activities
E-mail Breach	• Verify message was not properly encrypted and/or sent to parties without a need-to-know • Send Recall Notice immediately • Request deletion and confirmation of deletion from all parties involved
PII Exposed to Internet	• Contact the Webmaster and request immediate removal of content • Follow guidance below to request removal of indexed URLs from Search Engines
Unauthorized Access (Hacking)	• Contact local Command IAM / G6 immediately
Loss of PED/Mobile Devices	• Contact local Command IAM / G6 immediately • Follow established procedures for lost/stolen equipment

The following links 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
- Microsoft SharePoint - http://support.microsoft.com/kb/837847

SECTION 7.0: MAINTENANCE AND DISPOSAL OF PERSONALLY IDENTIFIABLE INFORMATION

Proper disposal of PII 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 references (a) and (b). Marine Corps officials responsible for the collection and maintenance of documents containing PII shall implement procedures to ensure documents are properly disposed. PII shall never be disposed of in trash cans or recycling containers, such occurrences would constitute a breach of PII. All records shall be retained in accordance with SECNAV M 5210.1, "Department of the Navy Records Management Manual," reference (y).

Officials shall conduct compliance spot checks, as outlined in sub-section 8.2 to ensure that proper disposal procedures are being followed. This section provides acceptable means of disposing PII in paper and electronic form.

7.1 PAPER

Proper disposal of paper containing PII is any method that leaves the information beyond reconstruction including cross-cut shredding, burning or chemical decomposition. Cross-cut shredding is the most common and recommended method.

7.2 COMPUTING EQUIPMENT

The Proper disposal of computing equipment is any method that leaves the information beyond reconstruction. Disposal methods include degaussing, destruction, and overwrite.

SECTION 8.0: COMPLIANCE AND RECURRING REQUIREMENTS

All individuals have a responsibility to be in compliance with annual training and audit requirements. The Marine Corps requires all Marines, Civilian Marines, and contractor personnel to complete annual PII training. This training will instruct all personnel in the collection, safeguarding, and maintenance of PII. Additionally, to ensure that PII is being continuously managed appropriately semi-annual spot checks are required per ALNAV 070/07, ”DON PII Annual Training Policy,” reference (z).

8.1 TRAINING AND REPORTING

All Marines, Civilian Marines, and contractor personnel shall take required Annual PII Training via MarineNet by registering for the following course:

- Marine Corps Personally Identifiable Information (PII) Annual Training - PII0090000

TECOM shall provide PII training numbers, via MarineNet, for all Marines, Civilian Marines, and contractor personnel to HQMC C4 CY No Later Than (NLT) the tenth day of each of the following months: November, February, May, and August. HQMC C4 CY shall coordinate with TECOM regarding the format training numbers will be provided in.

8.2 AUDIT (SPOT CHECKS)

Commands will ensure that all subordinate leadership and managers conduct compliance spot checks (audits) semi-annually within their area of responsibility. An internal spot check form is provided at Enclosure C. Spot checks provide awareness and oversight to ensure compliance with current policies and procedures for the management of PII. Special areas of focus should be those dealing with PII on a regular basis (e.g., personnel support, administration, human resources, security, and medical). Any deficiencies found shall be reported to the Commanding Officer (CO) or Officer-in-Charge (OIC) with a corrective action plan. This duty shall be assigned at the local command level.

SECTION 9.0: ACRONYMS

ARI	Administration and Resource Management Division
ARI-SF	Administration and Resource Management Division Security
C&A	Certification and Accreditation
C4	Command, Control, Communications, and Computers
CD	Compact Disk
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CMC	Commandant of the Marine Corps
CG	Commanding General
CO	Commanding Officer
CSM	Cybersecurity Manager
CY	Cybersecurity Division
DAR	Data-at-Rest
DIT	Data-in-Transit
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
ECSD	Enterprise Cybersecurity Directive
EDIPI	Electronic Data Interchange Personal Identifier
E.O.	Executive Order
FAM	Function Area Manager
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GENADMIN	General Administrative Messages
HQMC	Headquarters, United States Marine Corps
IA	Information Assurance
IAM	Information Assurance Manager
IS	Information System
IT	Information Technology

MARADMIN	Marine Administrative Message
MARCORSYSCOM	Marine Corps Systems Command
MCCAP	Marine Corps Certification and Accreditation Process
MCIAP	Marine Corps Information Assurance Program
MCEN	Marine Corps Enterprise Network
MOU	Memorandum of Understanding
NLT	No Later Than
OIC	Officer in Charge
OMB	Office of Management and Budget
OUSD	Office of the Undersecretary of Defense
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
PM	Program Manager
POA&M	Plan of Action and Milestones
POR	Program of Record
SECNAV	Secretary of the Navy
SORN	Systems of Records Notice
SSL	Secure Socket Layer
SSN	Social Security Number
TECOM	Training and Education Command
US-CERT	United States Computer Emergency Readiness Team
USMC	United States Marine Corps

SECTION 10.0: REFERENCES

10.1 PUBLICATIONS

This appendix provides a list of relevant statutes, regulations, directives, and other guidance applicable to IT security and critical infrastructure protection (CIP). It includes those cited in this document as well as other items that concerned personnel might need to understand. Although it is not a comprehensive collection of IT security-related references and authorities, it is sufficiently detailed to facilitate the reader’s use of this document and to understand other IT security-related documentation.

a) SECNAV Instruction 5211.5E, *“Department of the Navy (DON) Privacy Program,”* December 28, 2005.

b) DoD 5400.11-R, “*DoD Privacy Program*,” May 14, 2007.

c) Section 552a, of Title 5, United States Code.

d) Section 208 of Public Law 107-347, “*E-Government Act of 2002*,” December 17, 2002

e) DoD Instruction 8500.2, “*Information Assurance (IA) Implementation*,” February 6, 2003.

f) Commandant of the Marine Corps White Letter, NO. 2-11 “*Cyberawareness and Accountability*,” August 23, 2011.

g) DoD Memorandum, “Department of Defense Guidance on Protecting Personally Identifiable Information,” August 18, 2006.

h) DoD Instruction 5400.16, “*Privacy Impact Assessment (PIA) Guidance*,” February 12, 2009.

i) Department of Defense (DD) Form 2930, “*Privacy Impact Assessment*,” November

j) 11, 2008.

k) Directive Type Memorandum 07-015-USD(P&R), “*DoD Social Security Number Reduction Plan*,” March 28, 2008.

l) MARADMIN 646/10, “Department of the Navy Social Security Reduction Plan for Forms Phase One,” November 18, 2010.

m) SECNAV Form 5213/1, “*SSN Reduction Review*,” July 2010 https://navalforms.daps.dla.mil/formsDir/_SECNAV_5213_1_4999.pdf .

n) ALNAV Message 0XX/11, “*DON Social Security Number Reduction Plan Phase 3*,” TBD.

o) USD(P&R) memorandum, “*Updated Plan for the Removal of Social Security Numbers from Department of Defense Identification Cards*,” November 5, 2010.

p) GENADMIN, “*Protecting Personally Identifiable Information on DON Shared Drives and Application Based Portals,*“ DON CIO Msg 201839Z NOV 08.

q) OSD Memorandum 13798-10, “*Social Security Numbers Exposed on Public Facing and Open Government Websites*,” November 23, 2010.

r) MARADMIN 732/07, “*Data at Rest Encryption for Mobile Computing Devices and*

s) *Removable Storage Media*,” December 14, 2007.

t) Federal Information Processing Standards Publication 140-2, “*Security Requirements for Cryptographic Modules*,” December 3, 2002.

u) Enterprise Cyber Security Directive 005: Portable Electronic Devices.

v) OMB Memorandum 06-19, "*Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*," July 12, 2006.
w) OPNAV Form 5211/13, "*DON Loss or Compromise of PII Breach Reporting Form*," October 1, 2009, https://hqdod.hqmc.usmc.mil/PII.asp?page=PIIBreach.
x) OPNAV Form 5211/14, "*DON Loss or Compromise of PII After Action Reporting Form*," May 1, 2009, https://hqdod.hqmc.usmc.mil/PII.asp?page=PIIBreach.
y) SECNAV M 5210.1, "*Department of the Navy Records Management Manual*," November 16, 2007.
z) ALNAV 070/07,"*DON PII Annual Training Policy*," October 4, 2007.
aa) MCO 5400.52, *DON Deputy Chief Information Officer Marine Corps Roles and Responsibilities*, 5 Jan 2010

Other Related References:

- DODD 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction, 28Nov07
- DISA Wireless Security Technical Implementation Guides (STIGs), Current Version
- DODI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 03Nov09
- Marine Corps Enterprise Information Assurance Directives/Information Assurance Operational Standards
  - Incident Reporting 001
  - Firewalls 002
  - Routers 003
  - Remote Access 004
  - Portable Electronic Devices (PEDs) 005
  - Virtual Private Networks (VPNs) 006
  - IT Resource Access Guide 007
  - Secure Data Transfer 008
  - NATO Information Handling on MCEN 009
  - Unauthorized Disclosure and Electronic Spillage Handling 010
  - Personally Identifiable Information 011
  - Distributed Virtual Coalition Network (DVCN) Enclaves on the MCEN 012
  - Wireless Local Area Networks (WLANs) 014
  - INFOCON Implementation in the Marine Corps 017
  - Marine Corps Certification and Accreditation Process 018

10.2 Websites

- http://www.doncio.navy.mil/PolicyView.aspx?ID=424
- https://www.disa.mil
- https://hqDOD.hqmc.usmc.mil/
- https://www.cybercom.mil/

SECTION 11.0: DEFINITIONS

Breach of PII - 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.

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.

Destruction – Causes the paper or electronic collection unreadable and unusable along with the PII written on it; any remnants may be handled and disposed of as unclassified waste material.

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.

High Impact Personally Identifiable Information - Any information that can positively distinguish an individual and have an adverse affect on their personal life if compromised. These elements include, but are not limited to, any of the following when presented with the name: SSN, medical information, and financial information. Also includes the combination of multiple elements, that when presented together, including: name, date of birth, family members' names, home address, personal email address, and personal cell phone number.

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 or 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.

Moderate Impact Personally Identifiable Information – Information that only affects the individual in their work atmosphere including, but not limited to: work address, work phone, email address, pay grade, and rank. Moderate Impact PII that is compromised is not a reportable offense and is generally information that is releasable to the public.

Official Need to Know– 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.

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.

Personally Identifiable Information (PII) – Any information that can be used to distinguish or trace an individual's identity such as their name, social security number, date and place of birth, mother's maiden name, biometric records, and any other information that is linked or linkable to a specified individual.

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.

Portable Electronic Devices - A 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.

PII Impact Category – In accordance with Reference (f) all PII electronic records shall be assigned an Impact Category (High or Moderate) according to the potential of negative impact if PII lost or disclosed without authorization.

Privacy Act Statements – A required statement provided when an individual is requested to furnish personal information for inclusion in a System of Records. The statement is required to enable the individual to make an informed decision whether to provide the information requested.

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

Record – Any item, collection, or grouping of information, whatever the storage media(e.g., paper, electronic), 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 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 (c) 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.

ENCLOSURES

ENCLOSURE A – PRIVACY ACT STATEMENT

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).

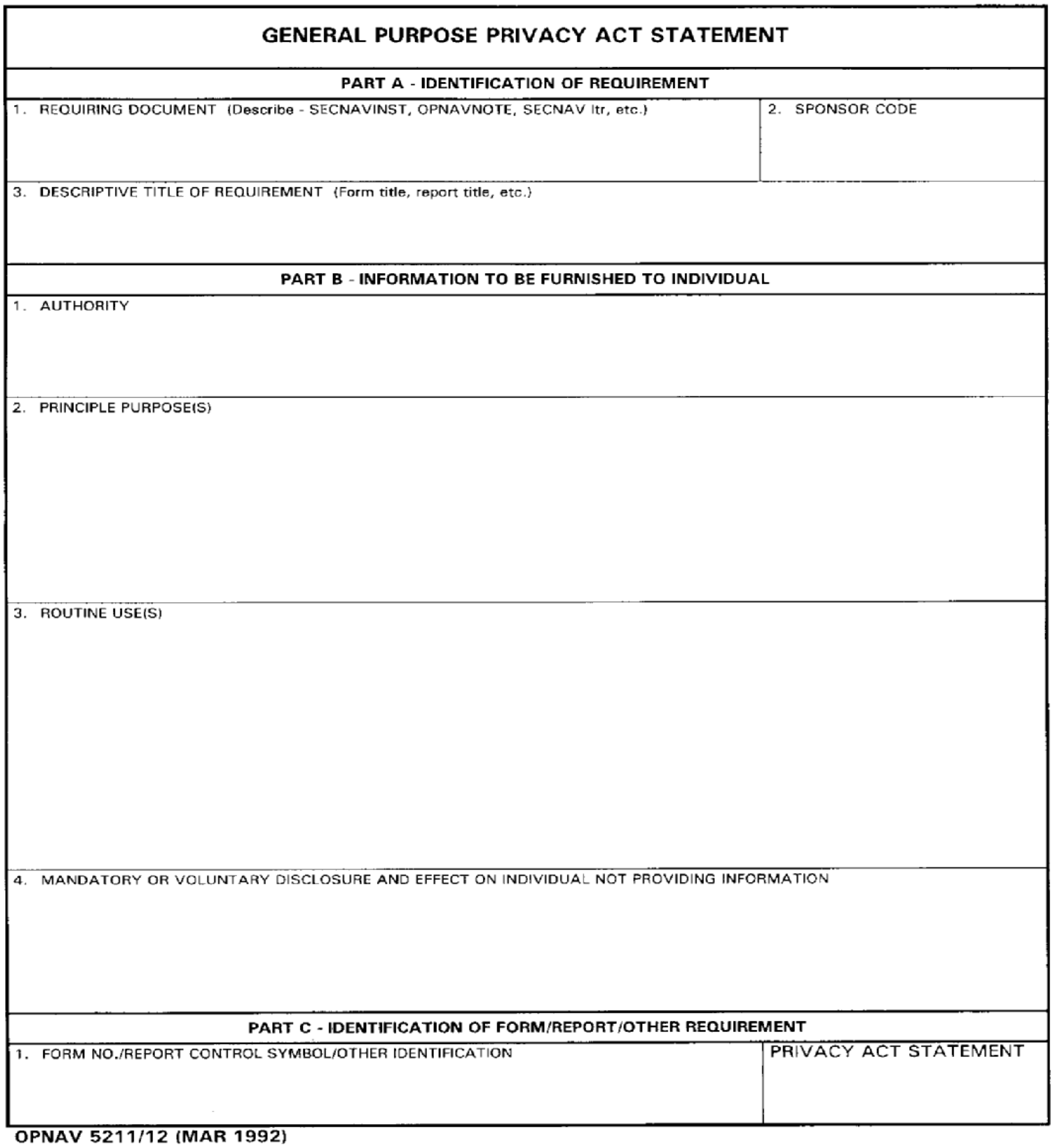
Fill in the following areas: AUTHORITY AND PURPOSE. Under AUTHORITY, please list the Federal law or Executive Order that appears in the systems notice. Under PURPOSE, copy the same information that is contained in the systems notice under Purpose.

Under ROUTINE USES, address who within and outside the organization will have access to the information. Do not cite “BLANKET ROUTINE USES APPLY”.

Under DISCLOSURE, cite whether or not the disclosure of information is “Voluntary” or “Mandatory”. Mandatory is appropriate when a Federal Law or Executive Order (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.



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.

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 jurisdiction. Essentially, the Privacy Act "cannot be used to block the normal course of court proceedings, including court-ordered discovery." 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: MARINE CORPS PII COMPLIANCE CHECKLIST

Marine Corps PII Spot Checklist

This form is an internal document and is to be used by command leadership to assess the level of compliance in the handling of PII as delineated by law and or specific DoD, DON, and Marine Corps policy. Where deficiencies are noted, the command should take immediate corrective action. For additional guidance and information go to the Marine Corps PII website at https://hqdod.hqmc.usmc.mil/pii.asp or contact Marine Corps Privacy Act Officer at smbhqmcprivacyact@usmc.mil or the Marine Corps C4 CY Identity Management Team at USMC_C4CY_idm@usmc.mil.

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

Date:

Section 1 Administrative

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

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

The MSC / MARFORCOM Privacy Act Coordinator has been identified in writing with clear roles and responsibilities identified.

□ Yes □ No

The MSC / MARFORCOM has an implementing Privacy Act instruction per SECNAV 5211.5E.

□ Yes Site document: □ No

The chain of command has a clear understanding of the Marine Corps reporting policy when a breach of personally identifiable information occurs.

□ Yes □ No

How many PII incidents were reported in the past 12 months?

Of the number of reported incidents, how many required notification? Was notification made within10 calendar days from the date of discovery?

incidents that required notification.

□ Yes □ No □ N/A, no incidents reported

Has the command disseminated guidance to its personnel on how to properly mark email, messages, letters, etc., that contains PII prior to transmission?

□ Yes □ No

Has the command taken action to eliminate or reduce the need for the use of SSN in accordance with Phase one and Phase two of the SSN reduction plan?

□ Yes □ No

Section 2 Paper Records

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

Number of containers checked

Number of containers containing unsecured PII

At random spot check 10% of recycle containers within your organization to ensure that no PII has been placed inside.

Number of containers checked Number of containers containing PII

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

□ Yes □ No

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

□ Yes □ No

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

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

Section 3 - Electronic Records and Hardware

Does the Command have a check in /check out log with written procedures for all laptops and portable electronic equipment that are transported outside a secure government space.

□ Yes □ No

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

Number of devices checked

Number of devices not in compliance

□ N/A - command has no PEDs

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

Number of documents containing PII

Number of documents not encrypted or password protected

□ N/A - command has no laptops or thumb drives

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

□ Yes □ No

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

Number of files checked

Number of files containing PII

□ N/A - command does not utilize shared drives

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

Number of systems requiring PIAs

Number of systems with PIAs submitted

For DITPR DON registered systems that contain PII, has there been a PIA submitted for approval and a SSN justification memo completed if collecting SSN?

Number of systems requiring PIAs

Number of systems with PIAs submitted

Number of systems with SSN justification memo submitted

Section 4 - Websites

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

□ Yes □ No

Are command sponsored websites properly registered in the DefenseLINK Locator?

Number of sites Number properly registered

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

Number of sites checked Number of records with PII

Section 5 - Training

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

□ Yes □ No