



Defense Manpower Data Center (DMDC)

DHRA Privacy Playbook

Version 3.0

Defense Manpower Data Center (DMDC)
Defense Human Resources Activity (DHRA)
4800 Mark Center Drive
Alexandria, VA 22350

January 16, 2023



Revision History

Date	Version	Description	Author
May 21, 2020	1.0	Final Version	
May XX, 2021	2.0	Added Security Control Footnotes and Reference Table; Expanded Section 4.0 Safeguarding PII; Replaced FOUO references with CUI; Updated Telework Guidance	
January 16, 2024	3.0	Transition from DEOC to DMDC; clarifies playbook as policy; clarifies that SOPs will be reviewed routinely and updated at Privacy Officers discretion; additional security controls; addition on policy for use of PII in research and test regions; addition on policy as it relates to PII in cloud service offerings	

Security Controls Table

The following table lists the NIST SP 800-53 Rev 4 Security Control Identifiers and Family names that are satisfied through this artifact.

Security Control Identifier	Security Control Name
AP-1.1, AP-1.2, AP-1.3, AP-1.4	Authority to Collect
AP-2.1, AP-2.2, AP-2.3, AP 2.4	Purpose Specification
AR-1.2, AR-1.7, AR-1.8, AR-1.9, AR-1.10, AR-1.11, AR-1.12, AR-1.13, AR-1.14, AR-1.15, AR-1.16, AR-1.17	Governance and Privacy Program
AR-2.1, AR-2.2, AR-2.3, AR-2.4, AR-2.5, AR-2.6, AR-2.7, AR-2.8, AR-2.9	Privacy Impact and Risk Assessment
AR-4.4	Privacy Monitoring and Auditing
AR-5.1, AR-5.2, AR-5.3, AR-5.4, AR-5.5, AR-5.6, AR-5.7	Privacy Awareness and Training
DI-1.1, DI-1.2, DI-1.3, DI-1.4, DI-1.5, DI-1.7, DI-1.8, DI-1.9, DI-1.10, DI-1.11, DI-1.12, DI-1.13, DI-1.14, DI-1.15, DI-1(2).1, DI-1(2).2	Data Quality
DM-1.1, DM-1.2, DM-1.3, DM-1.4, DM-1.5, DM-1.6, DM-1.7, DM-1.8, DM-1.9	Minimization of Personally Identifiable Information
DM-2.1	Data Retention and Disposal
DM-3.1, DM-3.2, DM-3.3, DM-3.4, DM-3.5, DM-3.6, DM-3.7, DM-3.8, DM-3.9	Minimization of PII Used in Testing, Training, and Research
IP-1.1, IP-1.2, IP-1.3, IP-1.4, IP-1.5, IP-1.6, IP-1.7, IP-1.8, IP-1.9, IP-1.10, IP-1.11	Consent



IP-2.1, IP-2.2, IP-2.3, IP-2.4, IP-2.5, IP-2.6	Individual Access
SE-1.2, SE-1.3, SE-1.4, SE-1.5	Inventory of PII
TR-3.2, TR-3.3	Dissemination of Privacy Program Information
UL-1.1	Internal Use
UL-2.1, UL-2.8, UL-2.9	Information Sharing with Third Parties

Approvals

The undersigned has/have reviewed this document and approve its contents.

Approver Name	Department/Role	Signature	Date
	DHRA Privacy Officer		January 16, 2024



1.0 Purpose

This document provides policy and guidance to all Defense Human Resources Activity (DHRA) Offices and Centers on how to maintain compliance with federal law and Department of Defense (DoD) policy when collecting, maintaining, safeguarding, and sharing personally identifiable information (PII) in accordance with the below references and as directed by the Assistance to the Secretary of Defense for Privacy, Civil Liberties and Transparency (ATSD)(PCLT)), to which DHRA Privacy Office routinely monitors for any changes that may impact the DHRA Privacy program¹:

- The Privacy Act of 1974, as amended, section 552a of title 10, United States Code
- Section 208 of Public Law 107-347, “E-Government Act of 2002”
- Department of Defense Directive (DoDD) 5400.11, “DoD Privacy and Civil Liberties Program,” January 29, 2019
- DoD 5400.11-R, “DoD Privacy Program,” May 4, 2007
- Administrative Instruction 81, “OSD/Joint Staff (JS) Privacy Program,” April 20, 2017
- Office of Management and Budget Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information,” January 3, 2017
- Department of Defense Instruction (DoDI) 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” August 1, 2012
- NIST 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”

Revisions to this document will be issued no less than biennially by the Defense Manpower Data Center to reflect changes to policy, procedures, or responsibilities, and ensure this document reflects all latest privacy standards and best practices. Standard Operating Procedures (SOPs) outlining related privacy procedures are published concurrently to this document and will be reviewed annually, with necessary updates being published at the discretion of the DHRA Privacy Officer. All documents will be published to the DHRA Privacy and Civil Liberties Webpage (DHRA Privacy and Civil Liberties - Home).²

¹ AR-1.2

² NIST 800-53 Revision 4: AR-1.7; NIST 800-53 Revision 4: AR-1.8; NIST 800-53 Revision 4: AR-1.9; NIST 800-53 Revision 4: AR-1.10; NIST 800-53 Revision 4: AR-1.11; NIST 800-53 Revision 4: AR-1.12; NIST 800-53 Revision 4: AR-1.13; NIST 800-53 Revision 4: AR-1.14; NIST 800-53 Revision 4: AR-1.15; NIST 800-53 Revision 4: AR-1.16; NIST 800-53 Revision 4: AR-1.17; NIST 800-53 Revision 4: AR-4.4; NIST 800-53 Revision 4: TR-3.3; NIST 800-53 Revision 4: UL-3.2; NIST 800-53 Revision 4: UL-3.3



1.0 Purpose	3
3.0 Personally Identifiable Information	5
4.0 Safeguarding PII	5
4.1 Safeguarding Paper Documents.....	7
4.2 Safeguarding Electronic Files	7
4.2.1 Websites.....	8
4.2.2 Email.....	9
4.2.3 Shared Drive.....	9
4.2.4 Task Management Tool.....	10
4.2.5 Portable Electronic Devices / Mobile Devices	11
4.3 Use of PII in Research and Test Regions	11
4.4 Telework Procedures for Safeguarding PII.....	12
5.0 Requirements for Collecting PII	12
5.1 System of Records Notices (SORN)	12
5.1.1 Developing a New SORN	14
5.1.2 Biennial Review of a Current SORN	14
5.1.3 Altering an Existing SORN	15
5.1.4. Deleting a SORN	15
5.2 Privacy Impact Assessment (PIA)	15
5.2.1 Confidentiality Impact Level for Cloud-Hosted Systems and Applications.....	18
5.3 Privacy Act Statements and Privacy Advisories	20
5.4 Social Security Number Use	22
5.5 Contractor Run Systems.....	22
6.0 PII Breach Reporting Response	23
6.1 Penalties.....	23
7.0 Training	24
8.0 Integrity and Compliance	25
8.2 Required Reporting.....	26
9.0 Glossary	27



3.0 Personally Identifiable Information

Personally identifiable information (PII), as defined by DoD 5400.11- R, DoD Privacy Program, is any information used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, biometric records, home phone numbers, and other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, either alone, or when combined with other personal or identifying information. The definition of PII is not anchored to any single category of information or technology.

While some PII is low-risk, such as that found on a business card, other PII is high-risk, such that if it were lost, compromised, or disclosed without authorization it could result in substantial harm, embarrassment, inconvenience, or unfairness to an organization or individual. Non-PII can become PII when combined with other publically available elements to positively identify an individual. So too, low-risk PII can also become high-risk PII when combined with other information or identifiers. For example, the name of an individual would become high-risk when grouped with place and date of birth and/or mother's maiden name. Each of these elements alone, however, would not constitute high-risk PII. Additionally, one must remember that context is important. For example, a list of people subscribing to a newsletter would likely not constitute as high-risk PII, while a list of people receiving treatment for substance abuse would.

Note, DoD ID Numbers should only be used for DoD business purposes. This may include transactions involving entities outside DoD, so long as individuals are acting on behalf of or in support of DoD. Per DoDI 1000.30, the knowledge of an individual's DoD Identification Number alone should be considered no more significant than the presence or knowledge of that individual's name. Internal unencrypted transmittal of the DoD ID, to those with a need-to-know in the performance of their duties, does not constitute a breach or policy violation.

When PII is considered to be potentially compromised, the responsible DHRA Office or Center is required to follow the PII breach reporting procedures as outlined in the Privacy Breach Reporting Standard Operating Procedure (SOP).

4.0 Safeguarding PII

Properly safeguarding PII is critical to reducing the possibility of a loss or compromise of sensitive information. Safeguards are used to protect agencies from "reasonably anticipated



threats” which could cause harm, embarrassment, inconvenience, or unfairness to the organization or individual. These include:

- Unauthorized access
- Unauthorized alteration
- Unauthorized disclosure

Safeguards should be tailored to the size and sensitivity of each system, as well as system-specific vulnerabilities. All records should be protected via physical and administrative safeguards. All records must be retained and disposed of via proper records management procedures³, as dictated by the National Archives and Records Administration and set forth through policies outlined in the DHRA Records Management Playbook. Electronic records must also possess technical safeguards to ensure damaging breaches do not occur.

Safeguards should include ensuring the system or collection does not create, collect, use, process, store, maintain, disseminate, or disclose PII unless it is directly relevant and necessary to accomplish a legally authorized purpose, and only maintain PII for as long as is necessary to accomplish the purpose.⁴ This holds true for all PII, including PII that has been authorized for training, testing, and/or research purposes.⁵

PII must only be viewed by individuals who have an official need to know for the information as a specific aspect of their job function. If information is viewed or accessed by individuals without an official need to know, a PII policy failure has occurred and should be reported based on the procedures outlined in the Privacy Breach Reporting SOP.

³ Records Management Policies & Procedures - All Documents

⁴ NIST 800-53 Revision 4: DM-1.1

⁵ NIST 800-53 Revision 4: DM-3.1; NIST 800-53 Revision 4: DM-3.2; NIST 800-53 Revision 4: DM-3.3; NIST 800-53 Revision 4: DM-3.4; NIST 800-53 Revision 4: DM-3.5; NIST 800-53 Revision 4: DM-3.6

4.1 Safeguarding Paper Documents

Paper documents containing PII include, but are not limited to: human resources information, sensitive health information, security clearance information, and recall rosters. When handling paper documents containing PII, the following protections are to be taken:

- Mark and or cover all documents in accordance with DODI 5200.14, “Controlled Unclassified Information”.
- Ensure control and limit access to the document during the course of the day.
 - Ensure all PII is placed securely out of sight when away from your desk, in a locked office, cabinet, or drawer.
 - Do not leave PII sitting out on printers or your desk.
 - If files need to be transported to an approved alternate location, do not leave files unattended or in vehicles.
 - Do not print, transport or store files containing PII outside of secured, approved work locations, to include personal residences.
- Ensure PII is directly provided to individuals with an official need to know, in order to maintain control of the information.
 - Do not discuss PII around individuals without a need to know.
 - Do not release PII to individuals unless it is specifically required to perform their official duties.
 - Rank, position or title alone does not authorize access to personal information about others.
- Only use a burn bags or approved shred bins to destroy paper PII.
 - Do not dispose of documents containing PII in trashcans or recycling bins.



4.2 Safeguarding Electronic Files

PII stored on shared drives, portals, and other network devices can lead to catastrophic PII breaches when not properly protected due to the accessibility, portability, and the sheer volume of records that can be stored. When handling PII in electronic files, the following precautions are to be taken:

- Ensure PII is only accessible to individuals with an official need to know in the performance of their duties. This includes documents stored on shared drives, on electronic devices, or in electronic systems.
 - Do not post PII to SharePoint.
- Ensure appropriate access provisioning is implemented and managed for shared drives that contain PII.

- Ensure laptops and mobile devices where PII is stored are encrypted in accordance with DHRA Cybersecurity Policy⁶.
- Ensure that facilities handling PII are access-controlled and hardware is locked up via safeguards, including:
 - Security guards
 - Cipher locks
 - Identification badges
 - Combination locks
 - Key cards
 - Closed circuit TV (CCTV)
 - User identification
 - Biometrics
 - Password protection
 - Encryption
 - DoD Public Key Infrastructure certificates
 - External Certificate Authority (CA) certificate
 - Common Access Card (CAC)
- Only maintain PII on U.S. Government furnished or approved equipment.
- At a minimum, all files containing PII should be password-protected (e.g., if compiled on a compact disc, or in a ZIP file that cannot be encrypted). However, encryption should be used whenever possible.
- Lock your computer and secure your CAC when stepping away.
- Additional technical safeguards may include:
 - Firewalls
 - Intrusion Detection Systems (IDS)
 - Virtual Private Networks (VPN)
- Additional administrative safeguards may include:
 - Periodic security audits
 - Regular monitoring of users' security practices
 - Backups secured off-site
- All electronic safeguards should be tested regularly to ensure they perform as intended.



4.2.1 Websites

OSD Memorandum 13798-10, “Social Security Numbers Exposed on Public Facing and Open Government Websites” mandates full and partial SSNs not be posted on any public-facing or

⁶ Cyber Security - Guidance



open government website in any form. These same practices should be followed for all manners of PII, unless authorized for release.

In general, public disclosure of PII should be limited to pictures, names, biographies, and contact information of DoD personnel who, by the nature of their position and duties, frequently interact with the public, such as general or flag officers, public affairs officers, or personnel designated as official spokespersons. Public disclosure of family information shall be generic and not include specific information such as names or ages. This includes PII in photographs, videos, captions, and other media.

4.2.2 Email

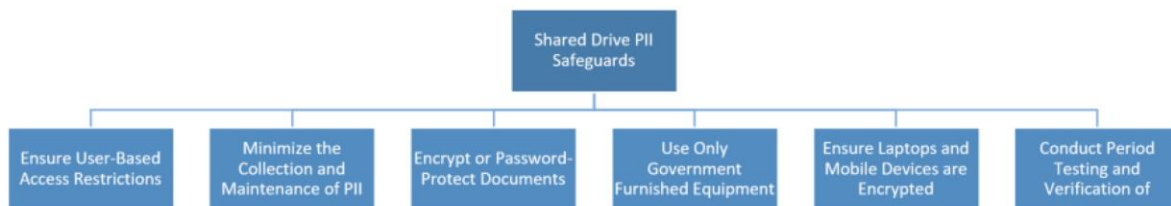
The most common breach of PII occurs via email, when PII is transmitted or retransmitted unencrypted outside the Department, or to individuals who do not have an official need to know. When transmitting PII via email, the following protections are to be taken:

- Digitally sign and encrypt all emails using a DoD email address and DoD-approved PKI certificates.
 - Do not send PII to group mailboxes, as these mailboxes cannot receive encrypted emails.
 - Do not email PII outside the .mil domain, as these emails cannot be encrypted.
- Include “Controlled Unclassified Information” or (CUI) in the subject line, to the greatest extent practicable.
- Place the following statement in the body of the email: “CONTROLLED UNCLASSIFIED INFORMATION (CUI) - PRIVACY SENSITIVE. ANY MISUSE OR UNAUTHORIZED ACCESS MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES” to the greatest extent practicable.
- PII should only be transmitted electronically via encrypted emails or authorized file transfer services such as [DoD SAFE](#).
 - Do not transmit, display, or share PII using Defense Collaboration Services (DCS), or Microsoft Skype.
 - DoD SAFE should always be used to transmit PII outside the .mil domain.
 - Microsoft Teams may be used to transmit PII for collaborative purposes, but should be done sparingly and with non-group audiences.

4.2.3 Shared Drive

PII stored on shared drives can lead to catastrophic PII breaches when not properly protected due to the accessibility, portability, and the sheer volume of records that can be stored. When handling PII in DHRA shared drive locations, the following precautions are to be taken:

- Ensure PII is only accessible to individuals with an official need to know in the performance of their duties.
 - Place user-based restrictions on all folders containing PII, in coordination with your organization's network administrator. Accessibility should be regularly monitored and updated accordingly.
 - Encrypt or password-protect all documents, at a minimum, where user-based restrictions are not in place.
- Limit the amount of PII collected and maintained on shared drives to only that which is required to meet mission needs, whenever possible.
- Ensure all laptops and mobile devices used to access PII within shared drive locations are encrypted.
- Use only U.S. Government furnished or approved equipment, where local maintenance of records containing PII is temporarily required.
- Conduct tests to ensure individuals without a need-to-know are unable to access restricted folders, upon initial establishment of access controls and on a regular basis thereafter. Periodic network maintenance can sometimes result in the removal of access controls.



4.2.4 Enterprise Task Management Software

PII uploaded and shared within the DHRA Enterprise Task Management Software (ETMS) must be properly safeguarded and protected the same as all PII collected and maintained within the DHRA Enterprise. When handling PII in ETMS, the following precautions are to be taken:

- Review all taskers at the initiator stage to determine whether PII is contained within the task instructions or attachments.
 - Take additional care when creating taskers containing data calls, as well. While the instructions or initial attachments for such tasks may not contain PII, the responses to the taskers may ultimately include PII and must be appropriately protected.
 - Contact the DHRA Privacy for guidance and clarification, as needed.
- Take the following actions when creating a ETMS tasker containing PII:
 1. Select "Unclassified PII/HIPAA" as the tasker "Classification" in the initial subject area.
 2. Ensure the check box next to "Is Private" is selected.

1.

Classification *	UNCLASSIFIED
Is Private	UNCLASSIFIED EOU
Priority +	UNCLASSIFIED PII/HIPAA
Category *	Routine
Coord Level *	--
Action *	--

2.

Is Private	<input checked="" type="checkbox"/>
Priority +	Routine
Category *	--
Coord Level *	--
Action *	--

4.2.5 Portable Electronic Devices / Mobile Devices

Any portable electronic device (e.g., laptop, cell phone, etc.) or mobile storage device which process or store electronic records containing PII shall be data-at-rest encrypted and have the capability for data-in-transit encryption. Reasonable physical safeguards should also be taken to protect against theft or unauthorized access (e.g., laptops should not be left in the open or unattended; screen should lock after no more than 30 minutes of inactivity).



4.3 Use of PII in Research and Test Regions

Use of complete records, to include PII, for research or analysis are not always required. To the greatest extent possible, records should be de-identified through obfuscation or removal of data in a manner that results in the inability to reasonably identify an individual.

The development of new or modification to existing IT systems require certain levels of testing prior to introduction into a production environment. This often necessitates the simulation of real conditions to ensure the system operates as expected. Use of PII in test regions introduces additional risks to the records entrusted with DHRA, such as improper disclosure to those without a need-to-know or the storage of information on systems with insufficient protections and controls. The use of production data in test regions is prohibited, unless otherwise authorized by the DHRA Cybersecurity and Privacy Officers. Any use of production data in test regions should go through a rigorous anonymization process to ensure the inability to reasonably identify an individual.



4.4 Telework Procedures for Safeguarding PII

When you take work documents to a telework site, such as your home, you have in your possession official government records which require preservation and safeguarding under federal law. In order to properly safeguard PII while teleworking:

- Only handle PII when teleworking on an approved DoD-device.
 - Do not take paper PII documents home, nor copy PII to a CD or removable drive.
 - Do not print PII at home.
 - Do not download attachments and emails containing PII from Outlook Web Access or any other remotely accessible sites to non-DoD devices.
 - Do not forward PII to a personal email account.
- Ensure all DoD-devices containing PII maintain in your control.
 - Do not leave laptops, or other devices, unattended in a private vehicle or other conveyance at any time.
- Only review PII in secure locations.
 - Do not review sensitive information while in a public place, such as public transportation, a car, or a coffee shop, where unauthorized persons might be able to view the records.

5.0 Requirements for Collecting PII

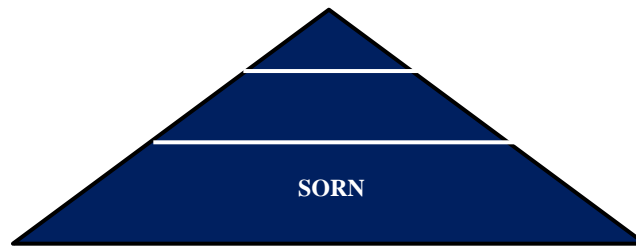
The collection and storage of PII is regulated by statutory law, federal regulations and standards, and DoD policy. When an individual is requested to provide PII for collection, all DHRA Components must ensure that these collections are compliant with the procedures described below, as applicable.

5.1 System of Records Notices (SORN)

The Privacy Act requires all executive branch agencies to have a completed SORN for any collection of PII, electronic or paper, that retrieves information about an individual using the individual's name, an identifying number, symbol, or other identifying element assigned to the individual, before a system can begin to operate. Mere maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act. To trigger the SORN requirements, information must actually be retrieved by a personal identifier. These collections are known as Privacy Act Systems of Records.

The SORN is the foundation of the federal privacy program and defines the rules for collecting, maintaining, safeguarding, and sharing of personal data when records are retrieved by a personal identifier. It provides notice to the public of the authority to collect and maintain the PII, purpose/use for which it is being collected, categories of individuals covered by the system, categories of records collected, record source categories, the routine uses under which the PII

may be shared with external entities, legal records retention schedule, system safeguards, and procedures for records access, contesting records, and notification.^{7 8}



All SORNs must be published in the Federal Register for a 30-day period to notify the public of the categories of individuals on whom data is being collected, data elements to be collected, purpose of the collection, authority for the information collection, and routine uses, and to afford an opportunity for public comment. PII collected and maintained in a system of records cannot be collected, used/utilized, maintained, or shared for any other purpose other than that which is clearly stated in the SORN, and supported by the applicable, listed legal authorities.⁹ Additionally, only the minimum personally identifiable information, as outlined in the SORN categories of records, which is relevant and necessary to accomplish the legally authorized purpose may be collected or retained.¹⁰ This is confirmed by the DHRA Privacy Office upon review of new or revised SORNs.

All sharing of PII with non-DOD entities from a system of records must also align with the routine uses outlined in the SORN.¹¹ While DHRA entities may begin collecting PII in a system of records as soon as the SORN is published in the federal register, PII may not be shared with non-DoD entities until the 30-day public comment period closes. All new proposed uses and instances of sharing of PII must be reviewed against the SORN prior to implementation to ensure

⁷ All requests by individuals to access their own PII are processed in accordance with the DHRA Freedom of Information Act and Privacy Release Accountability System Standard Operating Procedures.

⁸ NIST 800-53 Revision 4: DM-2.1; NIST 800-53 Revision 4: IP-2.1; NIST 800-53 Revision 4: IP-2.2; NIST 800-53 Revision 4: IP-2.3; NIST 800-53 Revision 4: IP-2.4; NIST 800-53 Revision 4: IP-2.5; NIST 800-53 Revision 4: IP-2.6;

⁹ NIST 800-53 Revision 4: AP-1.1; NIST 800-53 Revision 4: AP-1.2; NIST 800-53 Revision 4: AP-1.3; NIST 800-53 Revision 4: AP-1.4; NIST 800-53 Revision 4: AP-2.1; NIST 800-53 Revision 4: AP-2.2; NIST 800-53 Revision 4: AP-2.3; NIST 800-53 Revision 4: AP-2.4; NIST 800-53 Revision 4: DI-1.9; NIST 800-53 Revision 4: DM-1.1; NIST 800-53 Revision 4: DM-1.2; NIST 800-53 Revision 4: DM-1.3

¹⁰ NIST 800-53 Revision 4: DM-1.1; NIST 800-53 Revision 4: DM-1.2; NIST 800-53 Revision 4: DM-1.3

¹¹ NIST 800-53 Revision 4: UL-2.1



the proposed sharing is authorized and updates to the SORN are not required. Any changes to the Routine Use section requires an additional 30-day comment period prior to external sharing.¹²

A list of current SORNs is available on the ATSD (PCLT) website at:

<http://dpcl.d.defense.gov/Privacy/SORNs.aspx>.

Members of the public may also learn more about DHRA collections of PII by visiting the link below and contacting the appropriate OSD Privacy Officials:

<https://dpcl.d.defense.gov/Privacy/Privacy-Contacts/>¹³

5.1.1 Developing a New SORN

A new system of records is one for which no public notice has been published in the Federal Register. A new SORN must be published when any one of the following criteria are met:

- A new collection of PII, which is retrieved by unique identifier, is created.
- A previous collection of PII begins retrieving records by a unique identifier.
- A previous collection of PII, which is retrieved by unique identifier, is discovered which is not covered by an existing SORN.

The SORN must publish in the Federal Register before the agency begins to operate the system to collect and use PII. The 30-day Federal Register comment period must close before any disclosure of information from the system of record may be made outside the Department, in accordance with the system of record's routine uses.

When developing or identifying a new system or collection, consult with the DHRA CPO to check whether a SORN has previously been published that covers the collection and verify the data elements are covered. If your system is already covered by a SORN, it would negate the need to publish a duplicate system of records notice. For instructions on developing a SORN, see the System of Records Notice SOP found in the Privacy Document Library.

5.1.2 Biennial Review of a Current SORN

Each Component is required to review its SORNs biennially. The DHRA Privacy Office will initiate all biennial reviews. Component Privacy Liaison (PL), system owner and DHRA Privacy office will coordinate collaboratively to assess the needs of applicable SORNs. The DHRA Privacy Office will track the outcome of each review and maintain those records accordingly.

¹² NIST 800-53 Revision 4: UL-2.8; NIST 800-53 Revision 4: UL-2.9; NIST 800-53 Revision 4: IP-1.10; NIST 800-53 Revision 4: IP-1.11

¹³ NIST 800-53 Revision 4: TR-3.2



5.1.3 Altering an Existing SORN

Minor administrative changes to a system do not necessitate an alternation of a SORN. For example, a change in the designation of the system manager due to a reorganization would not require an alteration, so long as an individual's ability to gain access to his or her records is not affected.

Only changes that significantly alter the character and purpose of the system are considered alterations. Such changes may include:

- A significant increase or change in the number, type, or scope of individuals about whom records are maintained.
- An expansion in the types or categories of information maintained.
- A change in the purpose for which the information in the system is used.
- The connection of two or more formerly independent automated systems or networks, creating a potential for greater access.
- A change in system location due to infrastructure modernization.
- The addition or deletion of a routine use.
- A change in applicable safeguards as a result of risk analysis

For instructions on updating an existing SORN, see the System of Records Notice SOP found in the Privacy Document Library.

5.1.4. Deleting a SORN

If it is determined that a system should be discontinued and the SORN is no longer relevant, a deletion notice in the Federal Register for that system is required. (When a SORN is combined into another system, a new SORN for the merged system must also be submitted.) When discontinuing a system, the Component PL, in collaboration with the system owner, must verify why the SORN is no longer required.

To discontinue a system, contact the DHRA or DMDC CPO.

5.2 Privacy Impact Assessment (PIA)

Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct a PIA when:

- Developing or procuring Information Technology (IT) systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
- Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form from ten or more members of the public.



This includes all systems or collections of PII used for training, testing, and/or research.¹⁴

DoD Instruction (DoDI) 5400.16 “DoD Privacy Impact Assessment Guidance” further expands this requirement such that PIAs are required when:

- PII is collected, maintained, used, or disseminated in electronic form on members of the public, as well as federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally.

PIAs are conducted in order to:

- Ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form; and
- Examine and evaluate protections and alternative processes to mitigate potential privacy risks.¹⁵

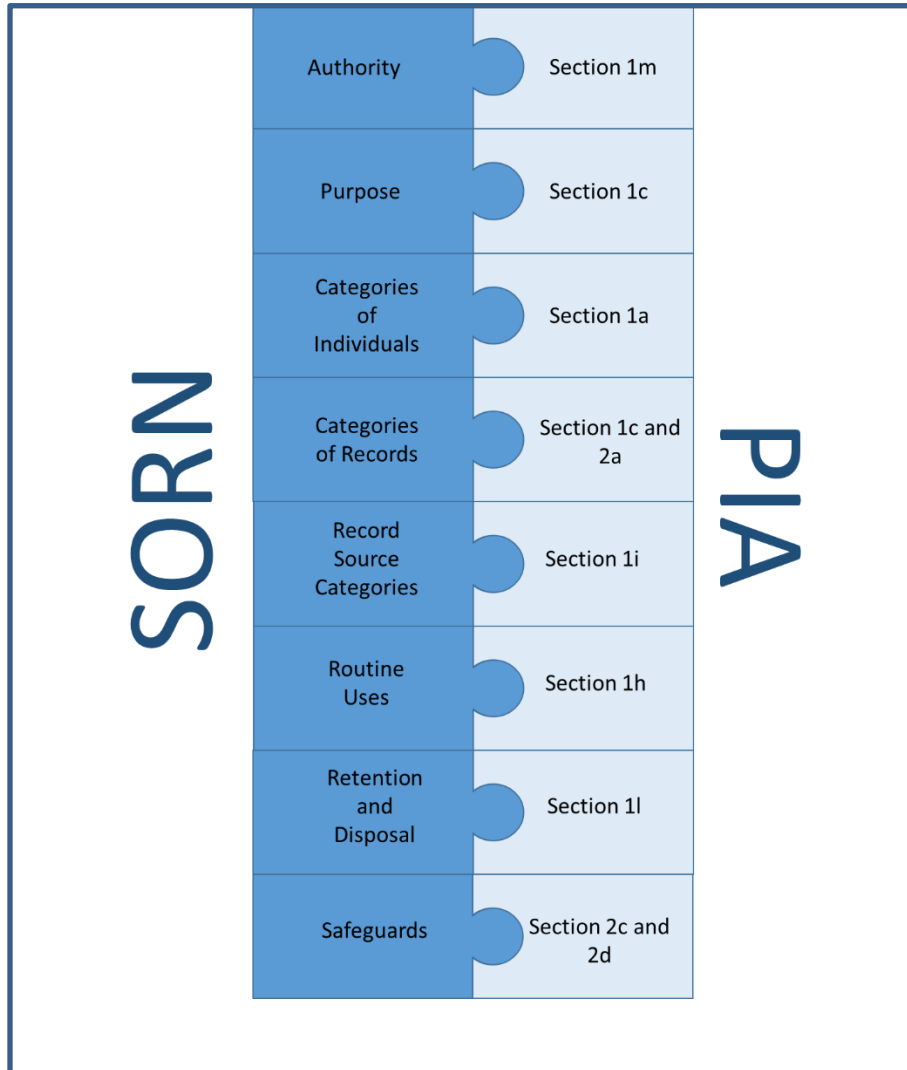
In accordance with the E-Government Act of 2002 and DoDI 5400.16 “DoD Privacy Impact Assessment Guidance,” systems owners and privacy officials must complete a PIA for every IT system containing PII under their responsibility, including any localized data collection (e.g., local websites, limited-use applications). All completed PIAs are to be recertified no less than triennially; however, it is recommended that PIAs be updated as part of the biennial SORN review process if significant changes are made. In fact, draft SORNs should be leveraged to help complete the PIA, per the figure below.

The PIA serves to ensure PII handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, determine the need, privacy risks, and effects of collecting, maintaining, using, and disseminating PII in electronic form, and examine and evaluate protections and alternative processes to mitigate potential privacy risks. It provides information to the DoD CIO and public of the purpose of the system or collection, types of PII collected in the system, the purpose/intended use of the PII, opportunity to object to the collection of PII, opportunity to consent to the specific uses of PII, with whom the PII will be shared, sources of the PII, how the information will be collected, other coordinating privacy and information collections compliance documentation, records retention authority and disposition, authority for the collection of information, PII confidentiality impact level, and system/collection safeguards.¹⁶

¹⁴ NIST 800-53 Revision 4: DM-3.7; NIST 800-53 Revision 4: DM-3.8; NIST 800-53 Revision 4: DM-3.9

¹⁵ NIST 800-53 Revision 4: AR-2.9

¹⁶ NIST 800-53 Revision 4: IP-1.9



SORN and PIA Similarities

As part of every PIA, the DHRA Privacy Office, in coordination with DHRA Cyber Security Division, makes a determination on the PII confidentiality impact level. This determination of the privacy risk to either the individuals or Department resulting from the collection, sharing, storing, transmitting, use, and disposal of PII is based upon the factors outlined in, NIST 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)”:

- Identifiability - how easily PII can be used to identify specific individuals;
- Quantity of PII - how many individuals are identified in the information;
- Data Field Sensitivity - sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together;
- Context of Use - the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated;



- Obligation to Protect Confidentiality - laws, regulations, or other mandates governing the obligation to protect personal information; and
- Access to and Location of PII- nature of authorized access to PII.¹⁷

Additionally, Privacy Risk is also incorporated into the information system's Federal Information Processing Standards Publication 199 Categorization process, a crucial step of the Risk Management Framework yet distinct from the one above.¹⁸ Systems that contain PII will automatically be assigned a Moderate impact level for Confidentiality, Integrity, and Availability in determining the applicable Risk Management Framework privacy controls under this process. An approved PIA is often used to support this system categorization. The below table defines the potential impact resulting from the loss of confidentiality or integrity of a system or information within the system:

		Potential Impact		
Security Objective	Low	Moderate	High	
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	

19

For instructions on developing or updating a PIA, see the Privacy Impact Assessment SOP found in the Privacy Document Library.

5.2.1 Confidentiality Impact Level for Cloud-Hosted Systems and Applications

Cloud computing technologies and services are becoming more prevalent within the Department, enabling components to consolidate their infrastructure footprint while leveraging information

¹⁷ NIST 800-53 Revision 4: AR-2.1; NIST 800-53 Revision 4: AR-2.2; NIST 800-53 Revision 4: AR-2.3; NIST 800-53 Revision 4: AR-2.4; NIST 800-53 Revision 4: AR-2.5; NIST 800-53 Revision 4: AR-2.6; NIST 800-53 Revision 4: AR-2.7; NIST 800-53 Revision 4: AR-2.8

¹⁸ NIST 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

¹⁹ FIPS Publication-199



technology functions that increases mission continuity and effectiveness. Although many cloud-based services being utilized have baseline cyber security controls already implemented, all services are not created equally and thus not authorized to collect, maintain, use or disseminate the same categorizations of information.

The DoD has defined information Impact Levels (IL) for cloud services that take into consideration the potential impact in the event the confidentiality or integrity of a system or information has been compromised. When developing a new or reviewing an existing system that leverages cloud services, we must determine if that service has the appropriate IL that aligns with the categorization of information being collected, maintained, used or disseminated. The below chart defines six ILs that cloud services may fall within, each requiring an increasingly more stringent level of security.

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	CSP PERSONNEL REQUIREMENTS & INVESTIGATION EQUIVALENCY
2	PUBLIC	FedRAMP Moderate Baseline (MBL)	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	Tier 1 (T1)
4	CUI (FOUO, PII, PHI) or Non-CUI	Level 2 + CUI-Specific Tailored Set OR FedRAMP HBL	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 (IT-1) Tier 5 (T5)
5	CUI (FOUO, PII, PHI), U-NSI/NSS	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 (IT-2) Tier 3 (T3) Non-Disclosure Agreement (NDA)
6	Classified SECRET NSS	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Endave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated T5 & SECRET Clearance NDA

20

The majority of systems that process PII in the cloud must minimally be protected in an IL4 cloud service offering. It is understood that there will be a need for some business functions that collect, maintain, use or disseminate low-confidentiality PII on cloud services with an IL2 authorization. Although there is no definitive list of data elements that qualify as low-level confidentiality, it is generally understood that this information equates to what was previously

²⁰ DoD Cloud Computing SRG V1.4



defined as rolodex information: Name, DoD ID, office contact information or similarly minimally invasive information.

In order for low-confidentiality PII to be collected, stored or processed in a commercial cloud service offering, it must meet the following requirements²¹:

- Mission owners will only publish, collect, store and process low confidentiality impact (sensitivity) PII in a CSO minimally possessing a FedRAMP Moderate P-ATO listed on the FedRAMP Marketplace and a DoD Level 2 PA, with privacy officer approval.
- Mission owner PII impact level determination will consider all relevant factors together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor.
- Prior to authorizing the system, the AO is accountable to review the PIA and ensure that appropriate cyber assessments are performed per DoDI 8510.01 and the CC SRG, and that required CSSP cybersecurity support services are provided per DoDI 8530.01.
- Low impact/sensitivity PII, when published or collected in a CSO with a Level 2 PA, must be minimally protected in accordance with NIST SP 800-122 and privacy laws as supported by a FedRAMP Moderate P-ATO, and the low PII overlay of the privacy overlay (see Section 5.1.5.2, CNSSI 1253 Privacy Overlay).

5.3 Privacy Act Statements and Privacy Advisories

When an individual is requested to provide PII (e.g., name, date of birth, SSN) for inclusion into a system of record or to confirm that their information contained in the system of record is current and correct, a PAS must be provided to the individual at the point of collection. This is true regardless of the method used to collect the information (e.g., paper or electronic forms, personal interviews, telephonic interviews). When SSNs are being collected, a PAS is always required, regardless of whether the information will be stored in a system of record or not.

A PAS enables an individual to make an informed decision on whether to provide the information being requested, and the consequences for not providing the information, by identifying:

- The authority for collecting the information,
- The purpose for collecting the information,
- The routine uses of the information, under which information may be disseminated external to the Department, and
- Explaining whether disclosure of the information is voluntary or mandatory.

The PAS also provides a link the SORN, which provides further information on the use, purpose, dissemination, safeguards, and retention of the requested PII.

²¹ DoD Cloud Computing SRG V1.4



Generally, disclosure is mandatory when a penalty may be imposed on the individual for failing to provide the requested information. Personal information obtained without a PAS must not be incorporated into any system of records. System PASs must be updated, with the coordinating SORN, whenever new information is to be collected, as well as when the purpose, use, disclosure, safeguards, or authorities change. All current or proposed purposes, uses, disclosure, safeguards, or authorities must be described in the PAS, and coordinating SORN, prior to collection. The PAS should be prepared in accordance with Chapter 2 of DoD 5400.11-R, “Department of Defense Privacy Program.” The PAS should be completed following the initial review and approval of a system’s SORN and PIA.²²

PRIVACY ACT STATEMENT
AUTHORITY: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 131, Office of the Secretary of Defense; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); and 50 U.S.C. 1913, National Language Service Corps. PRINCIPAL PURPOSE(S): To allow U.S. citizens with language skills to self-identify their skills for the purpose of temporary employment on an intermittent work schedule or service opportunities in support of DoD or another department or agency of the United States. The information will be used to determine applicants' eligibility for NLSC membership and to identify and contact NLSC members. ROUTINE USE(S): To another department or agency of the United States in need of temporary short-term foreign language services, where government employees are required or desired. For a complete list of routine uses, visit the applicable system of records notice at: http://dpclid.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/ < Caution- http://dpclid.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/ > DISCLOSURE: Voluntary; however, failure to provide information may result in non-enrollment in the NLSC and refusal to grant access to member areas of the NLSC portal.

For information on the latest PAS template, visit the DHRA Privacy Program Document Library.

Alternatively, when PII is solicited from an individual and the information will not be maintained in a Privacy Act system of records, a Privacy Advisory is required. A Privacy Advisory informs the individual as to why the information is being solicited and how the information will be used. The privacy advisory must be posted on the web page or document where the information is being solicited or displayed.

PRIVACY ADVISORY
When completed, this form contains personally identifiable information and is protected by the Privacy Act of 1974, as amended.

For information on the latest Privacy Advisory template, visit the DHRA Privacy Program Document Library.

²² NIST 800-53 Revision 4: IP-1.1; NIST 800-53 Revision 4: IP-1.2; NIST 800-53 Revision 4: IP-1.3; NIST 800-53 Revision 4: IP-1.4; NIST 800-53 Revision 4: IP-1.5; NIST 800-53 Revision 4: IP-1.6; NIST 800-53 Revision 4: IP-1.7; NIST 800-53 Revision 4: IP-1.8; NIST 800-53 Revision 4: IP-1.9; NIST 800-53 Revision 4: IP-1.10; NIST 800-53 Revision 4: IP-1.11



5.4 Social Security Number Use

The process for collecting, handling, and maintaining SSNs is regulated by federal law and DoD 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, policy or other legal authority requires that the SSN be furnished, as further discussed in DoD 5400.11-R “Department of Defense Privacy Program.”

In accordance with DoDI 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” use of SSNs should be eliminated or reduced whenever possible and the SSN should be replaced with another identifier (e.g., DoD ID number).

When requesting, collecting, transmitting, or maintaining an individual’s SSN in any form (including truncated, masked, and encrypted SSNs), the collection must be documented and justified, in accordance with an acceptable use case, via a SSN Justification Memorandum.

Additionally, all automated systems containing SSNs must be included in the DoD Information Technology Portfolio Repository (DITPR). All DITPR fields relating to SSN use are mandatory.

For a complete list of SSN Use Cases, see the Acceptable Social Security Number Use Cases document found in the Privacy Document Library.

For instructions on developing a Social Security Justification Memorandum, see the Social Security Number Justification Memorandum SOP found in the Privacy Document Library.

5.5 Contractor Run Systems

When an agency contracts for the operation of a Privacy Act system of record, certain Federal Acquisition Regulations (FAR) provisions must be adhered to by the agency. Additionally, specific FAR clauses and the name of the system of record must be included in the contract and Request for Proposals (RFPs), as appropriate.

All DHRA components, contracts, and RFPs involving contractor operation of a Privacy Act system of records must adhere to the following FAR Privacy Act provisions.

Agency Requirements:

- Subpart 24.1- Protection of Individual Privacy
- Subpart 24.3 – Privacy Training



Contractor Requirements:

- Clause 52.224-1, Privacy Act Notification
- Clause 52.224-2, Privacy Act
- Cause 52.224-3, Privacy Training

Any additional protections which are determined to be necessary by the program and system managers who are responsible for the system, must also be included in the contract or RFP.

For more details on these clauses, see Privacy Federal Acquisition Regulation Clauses document found in the Privacy Document Library.

6.0 PII Breach Reporting Response

A PII breach is defined as loss of control, unauthorized disclosure, unauthorized access, or theft of PII, where individuals other than authorized users gain access or potential access to such information or an authorized user accesses or potentially accesses such information for an unauthorized purpose. Examples of PII breaches include sending an email with PII to a non-.mil recipient or publication of PII on a public facing website.

If an individual suspects a PII breach has occurred, follow the PII breach reporting procedures as outlined in the Privacy Breach Reporting Standard Operating Procedure (SOP) found in the Privacy Document Library.

Procedure should begin with immediate notification to the DHRA Privacy Office. Note: Do NOT include PII when reporting unless specifically requested by the Privacy Office:

- DMDC Privacy Officer
- DHRA Privacy Mailbox: dodhra.mc-alex.dhra-hq.mbx.privacy@mail.mil

6.1 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 civil or criminal actions against the employee or agency, as well as fines in accordance with the Privacy Act. Criminal penalties may be enacted when an agency official or employee willfully makes a disclosure of a record knowing it to be in violation of the Privacy Act. Such penalties may include a misdemeanor conviction and fine of up to \$5,000. Civil penalties may be imposed when an agency unlawfully refuses to amend or grant access to a record, or fails to comply with any Privacy Act provision or agency rule that results in adverse effect.

Note that criminal penalties may be applied to government employees and contractors alike. Administrative actions may also be taken, at the discretion of the involved office/center, and should be coordinated with the DHRA Office of the General Counsel.

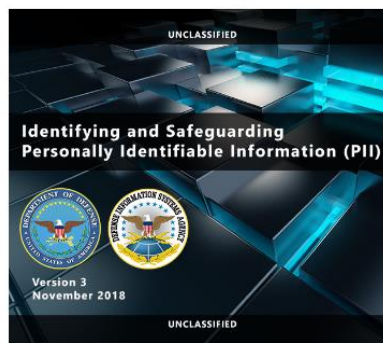
7.0 Training

All new federal employees and contractors are required to take PII and cybersecurity training prior to gaining access to the DoD network. All employees and contractors are required to refresh this training annually. The following trainings should be taken in the DHRA Learning Management System, when required:

- “PERSONALLY IDENTIFIABLE INFORMATION AWARENESS ANNUAL TRAINING”

Designated Component PLs may also be required to take additional or role-based privacy training, as determined by the DHRA SCOP, and in accordance with the DHRA Specialized Privacy Training SOP. Additional training is also provided through quarterly DHRA Privacy webinars, on a range of rotating topics based on current organizational need. For a list of recordings past webinars and how to access them, visit the DHRA Privacy folder at:

Employees and contractors may also be required to take the below PII training when involved in PII breaches or policy violations at the request of the DHRA Privacy Office. Such training must be completed, and the certificate provided to the DHRA Privacy Officer, within 5 business days where requested.²³



- Identifying and Safeguarding Personally Identifiable Information (PII) Version 3.0

²³ NIST 800-53 Revision 4: AR-5.1; NIST 800-53 Revision 4: AR-5.2; NIST 800-53 Revision 4: AR-5.3; NIST 800-53 Revision 4: AR-5.4; NIST 800-53 Revision 4: AR-5.5; NIST 800-53 Revision 4: AR-5.6; NIST 800-53 Revision 4: AR-5.7



8.0 Integrity and Compliance

The DHRA Privacy Office conducts initial and regular reviews of the DHRA inventory of PII and provides coordination on all collection instruments (i.e. forms and other tools used to collect PII) upon creation and revision in order to ensure the enterprise remains in compliance with all applicable laws and policies, and that all systems of record and other collections of PII are:²⁴

- Legally authorized, relevant, and necessary to accomplish an established DoD mission or function.
- Collected, maintained, used, and disseminated only for authorized purposes.²⁵
- Accurate, relevant, timely, consistent (data integrity), complete for its stated purpose, and collected directly from the individual to the greatest extent practicable, particularly when the information may result in adverse determinations or compromise the objectivity or fairness on the determination of an individual's rights, benefits, and privileges.²⁶
 - All systems and collections should have system-specific, defined procedures to validate, and correct as necessary, any inaccurate or outdated PII, and ensure that PII is shared only in accordance with the system of records notice and appropriate policy. To ensure the quality of privacy act information, these system-specific guidelines to ensure and maximize utility will differ based on collection and system, and should include:
 - Annual reviews of collection instruments and data holdings;
 - Annual reviews of system of record notice routine uses; and
 - Use of change audit logs.²⁷
 - Individuals should be requested to confirm the accuracy, relevancy, current (timeliness), and completeness of their data that time of collection and validate their data when changes are requested.²⁸
- Provide information to the individual on:
 - The specific purpose or purposes for which the information is intended to be used;
 - The authority for collection;
 - How the PII may be used;
 - Whether disclosing of such information is mandatory or voluntary; and

²⁴ NIST 800-53 Revision 4: DM-1.5

²⁵ NIST 800-52 Revision 4: UL-1.1

²⁶ NIST 800-53 Revision 4: DI-1.1; NIST 800-53 Revision 4: DI-1.2; NIST 800-53 Revision 4: DI-1.3; NIST 800-53 Revision 4: DI-1.4; NIST 800-53 Revision 4: DI-1.5; NIST 800-53 Revision 4: DI-1.11; NIST 800-53 Revision 4: DI-1.12; NIST 800-53 Revision 4: DI-1.13; NIST 800-53 Revision 4: DI-1.14; NIST 800-53 Revision 4: DI-1.15

²⁷ NIST 800-53 Revision 4: DI-1.7; NIST 800-53 Revision 4: DI-1.8; NIST 800-53 Revision 4: DI-1.10; NIST 800-53 Revision 4: DI-1.11; NIST 800-53 Revision 4: DI-1.12; NIST 800-53 Revision 4: DI-1.13; NIST 800-53 Revision 4: DI-1.14; NIST 800-53 Revision 4: DI-1.15

²⁸ NIST 800-53 Revision 4: DI-1.1; NIST 800-53 Revision 4: DI-1.2; NIST 800-53 Revision 4: DI-1.3; NIST 800-53 Revision 4: DI-1.4; NIST 800-53 Revision 4: DI-1(1).1; NIST 800-53 Revision 4: DI-1(2).1; NIST 800-53 Revision 4: DI-1(2).2



- The consequences to the individual of not providing that information.
- Apply appropriate, system-specific administrative, physical, and technical safeguards and procedures to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected.

8.2 Required Reporting

The DHRA Privacy Office is responsible for compiling inputs for the ATSD (PCLT) in order to report on privacy program effectiveness, progress and compliance as required. These reports include, but are not limited to, the Section 803 Report and the Federal Information Management Security Act (FISMA) Report. Reports are compiled on behalf of the DHRA SCOP, who has ultimate authorization prior to final delivery.



9.0 Glossary

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

Computer Matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

Disclosure. The sharing or transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, government agency, or private entity other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Individual. A living person who is a U.S. citizen 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, except as otherwise provided in DoD 5400.11-R "Department of Defense Privacy Program." Members of the Military Services are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses (whether incorporated or unincorporated), and other commercial entities are not "individuals" when acting in an entrepreneurial capacity with the DoD, but persons employed by such organizations or entities are "individuals" when acting in a personal capacity (e.g., security clearances, entitlement to DoD privileges or benefits).

Information. Any communication or representation of knowledge, such as facts, data, or opinions, in any medium or form, including textual, numeric, graphic, cartographic, narrative, or audiovisual forms.

Personally Identifiable Information (PII). Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, and other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, either alone, or when combined with other personal or identifying information.

Privacy Act Statements (PAS). A statement required when collecting PII from an individual for inclusion in a system of record. A Privacy Act statement must be presented at the point of collection regardless of the means of collection (e.g., paper or electronic forms, personal interviews, telephonic interviews). Informs individuals as to the authority, purpose, routine use,



and disclosure of a collection, and allows the individual to make an informed decision about providing their data.

Privacy Advisory. A statement required when PII is solicited from an individual by a DoD website (e.g., collected as part of an email feedback/comments feature on a website), and information is not maintained in a Privacy Act system of records. Informs an individual as to what purpose the PII is being requested from them, and allows the individual to make an informed decision about providing their data.

Privacy Impact Assessment (PIA). An 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 Liaisons. Appointed Component lead for all privacy compliance matters. Coordinates with the DHRA Privacy Office and Component personnel to ensure compliance with all applicable privacy laws and policies. Attends quarterly DHRA Privacy Working Groups.

Privacy Policy Violation. An occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose, but the information never left the control of the Department.

Record (Privacy). Any item, collection, or grouping of information in any media (e.g., paper, electronic) about an individual that is maintained by a DoD Component or Contractor on behalf of the Component, including but not limited to education, financial transactions, medical history, and criminal or employment history, and that contains the name or identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph.

Routine Use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

Social Security Number (SSN) Justification Memorandum. A SSN justification memorandum is required to validate the use of the SSN on any form or IT system. This includes, but is not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs. SSN



justifications must be submitted when a new requirement exists to collect the SSN, when the use has not previously been justified, and when DoD policy requires a review and update.

System of Records. A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual. The Privacy Act requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a System of Records Notice or SORN.

System of Records Notice (SORN). A public notice detailing the conditions, contents, and procedures for a system of records, including system identifications, system locations, categories of records and individuals contained in the system, access procedures, and legal exemptions.