DHRA Enterprise Operations Center (DEOC)

DHRA Privacy Playbook

DHRA Enterprise Operations Center (DEOC)
Defense Human Resources Activity (DHRA)
4800 Mark Center Drive
Alexandria, VA 22350

May 1, 2020

1.0 Purpose

This document outlines guidance to all Defense Human Resources Activity (DHRA) Components 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:

- 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

Revisions to this document will be issued periodically by the DHRA Enterprise Operations Center (DEOC) to reflect changes to policy, procedures, or responsibilities.

Katrina L. Logan
Director, DHRA Enterprise Operations Center and DHRA Senior Component Official for Privacy

2.0 Index

1.0 Purpose 1
2.0 Index 2
3.0 Personally Identifiable Information 3
4.0 Safeguarding PII 3
4.1 Safeguarding Paper Documents 4
4.2 Safeguarding Electronic Files 5
4.2.1 Websites 6
4.2.2 Email 6
4.2.3 Portable Electronic Devices / Mobile Devices 7
4.3 Telework Procedures for Safeguarding PII 7
5.0 Requirements for Collecting PII 7
5.1 System of Records Notices 7
5.1.1 Developing a New SORN 8
5.1.2 Biennial Review of a Current SORN 9
5.1.3 Altering an Existing SORN 9
5.1.4. Deleting a SORN 9
5.2 Privacy Impact Assessment (PIA) 10
5.3 Privacy Act Statements and Privacy Advisories 11
5.4 Social Security Number Use 13
5.5 Contractor Run Systems 13
6.0 PII Breach Reporting Response 14
6.1 Penalties 14
7.0 Training 15
8.0 Glossary 16

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 not likely be 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.

When PII is considered to be potentially compromised, the responsible Component is required to follow the PII breach reporting procedures as outlined in the Privacy Breach Reporting Standard Operating Procedure (SOP) found in the Privacy Document Library: https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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:

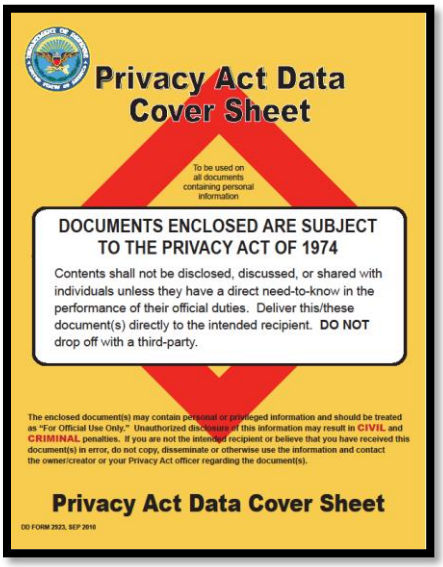
- Unauthorized access
- Unauthorized alteration

- 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, and ultimately disposed of via proper records management procedures. Electronic records must also possess technical safeguards to ensure damaging breaches do not occur.

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 found in the Privacy Document Library:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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:

- Cover all documents with DD Form 2923, "Privacy Act Data Cover Sheet," including when faxing or mailing the document.
- 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.
    - Do not leave files unattended or in vehicles.
- 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.
- 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 laptops and mobile devices where PII is stored are encrypted.
- 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 remove 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 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 by encrypted.
- Include "For Official Use Only" or (FOUO) in the subject line, to the greatest extent practicable.
- Place the following statement in the body of the email: "For Official Use Only (FOUO) - 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.

4.2.3 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 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 download attachments and emails containing PII from Outlook Web Access or any other remotely accessible sites to non-DoD devices.
- 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

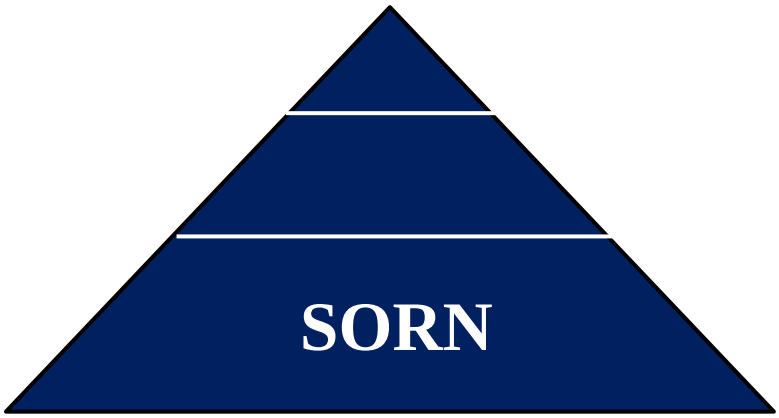
The collection and storage of PII is regulated by statutory law, federal regulations and standards, and DoD policy. When an individual is requested to provide PII for collection, all DHRA Components must ensure that these collections are compliant with the procedures described below, as applicable.

5.1 System of Records Notices

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.

The SORN is the foundation of the federal privacy program and defines the rules for collecting, maintaining, safeguarding, and sharing, and personal data when records are retrieved by a personal identifier.



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. A list of current SORNs is available on the DPCLD website at: http://dpcld.defense.gov/Privacy/SORNs.aspx.

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 or DMDC CPO to check whether a SORN has previously been published which 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: https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

5.1.2 Biennial Review of a Current SORN

Each Component is required to review its SORNs biennially. Component PLs are responsible for initiating and completing Component biennial reviews on time. If a review is not initiated by the Component, the DHRA or DMDC CPO will notify each Component PL regarding the required biennial reviews based on the established Federal Register publication date or the last date of review. Where no updates are needed, a memorandum for the record should be submitted to the DHRA or DMDC CPO indicating that a review was conducted and the SORN was found to be current.

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: https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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 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 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.

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

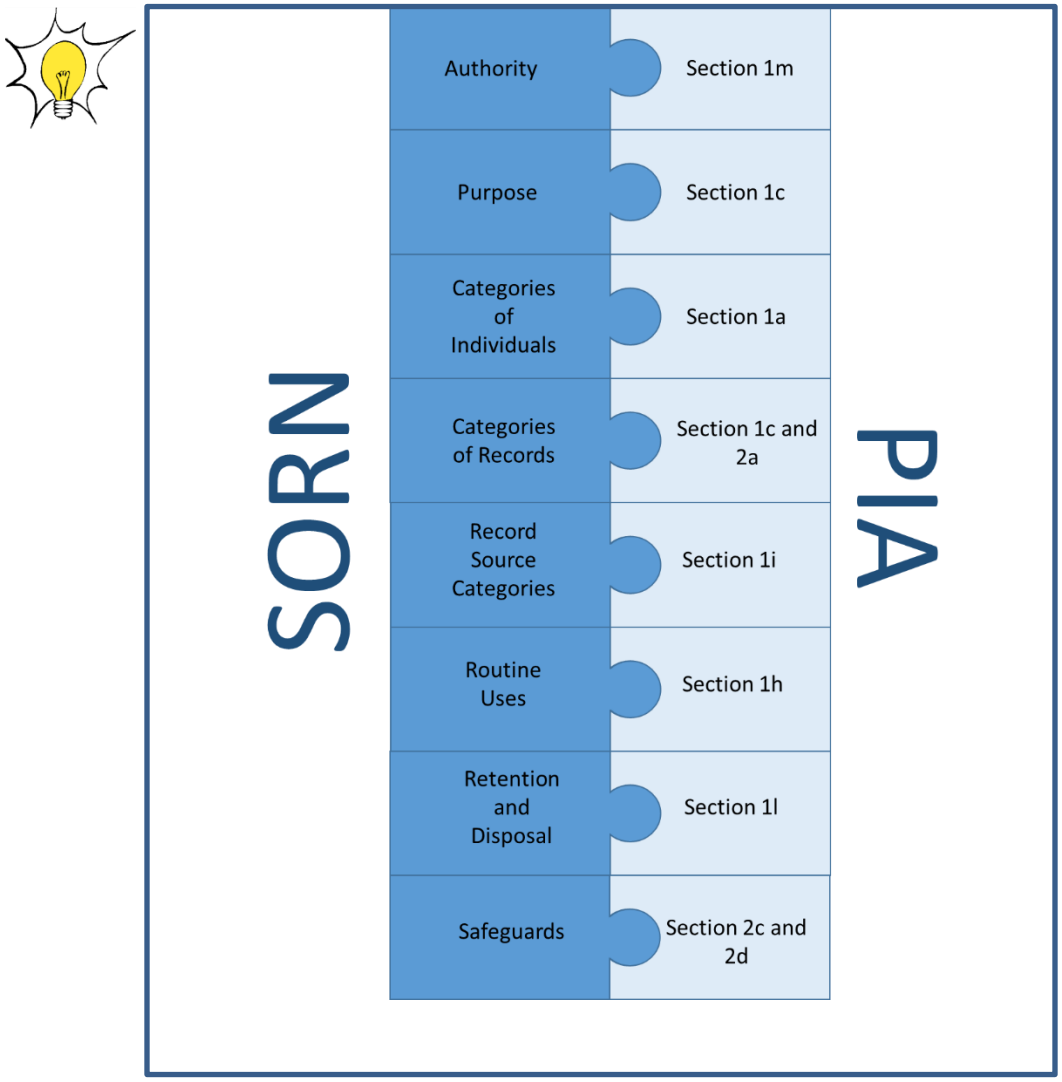
- PII is collected, maintained, used, or disseminated in electronic form on members of the public, as well as federal personnel, contractors, or foreign nationals employed at U.S. military facilities internationally.

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.

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.

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. Systems that contain PII will automatically be assigned a Moderate impact level for Confidentiality, Integrity, and Availability. An approved PIA supports the system categorization and is used to support any required changes from the Moderate impact level.



SORN and PIA Similarities

For instructions on developing or updating a PIA, see the Privacy Impact Assessment SOP found in the Privacy Document Library:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

5.3 Privacy Act Statements and Privacy Advisories

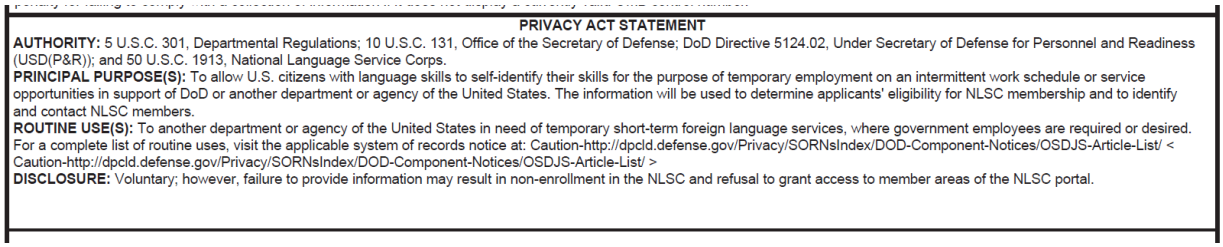
When an individual is requested to provide PII (e.g., name, date of birth, SSN) for inclusion into a system of record or to confirm that their information contained in the system of record is current and correct, a PAS must be provided to the individual at the point of collection. This is true regardless 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 by identifying:

- The authority for collecting the information,
- The purpose for collecting the information,
- The routine uses of the information, and
- Explaining whether disclosure of the information is voluntary or mandatory.

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. 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.

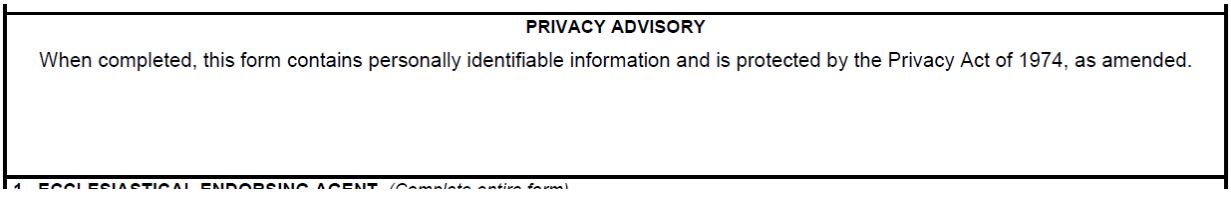


PRIVACY ACT STATEMENT

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: Caution-http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/ < Caution-http://dpcld.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: https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

Alternatively, when PII is solicited from an individual and the information will not 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:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

For instructions on developing a Social Security Justification Memorandum, see the Social Security Number Justification Memorandum SOP found in the Privacy Document Library:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

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:
https://dhra.deps.mil/CO/serv/ITPPM/Internal/Privacy%20Documents/Forms/AllItems.aspx

Procedure should begin with immediate notification to the DHRA or DMDC Privacy Office:

- DHRA Privacy Officer: Jessica Levin (jessica.m.levin.civ@mail.mil571, Desk: 571-372-2240, Cell: 571-289-3442)

- DMDC Privacy Officer: Samuel Peterson (Samuel.m.peterson2.civ@mail.mil, Desk: 831-583-2400 x4457, Cell: 571-438-1951)[1]

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

[1] POCs subject to change. If unable to reach the above POCs, contact the DEOC Service Center at 1-888-920-DEOC.

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 and should be coordinated with the DHRA Office of the General Counsel.

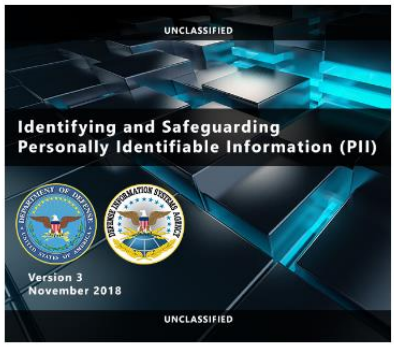
7.0 Training

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 privacy training, as determined by the DHRA SCOP.

Employees and contractors may also be required to take the below PII training when involved in PII breaches or policy violations:



- Identifying and Safeguarding Personally Identifiable Information (PII) Version 3.0
  - https://securityawareness.usalearning.gov/piiv2/index.htm

8.0 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 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.