



# **Defense Human Resources Activity Privacy Program Playbook**

**Version 2.0**

**May 6, 2015**

## Table of Contents

Purpose.....	3
1.0 SCOPE .....	4
2.0 RESPONSIBILITIES .....	4
3.0 PERSONALLY IDENTIFIABLE INFORMATION .....	6
4.0 REQUIREMENTS FOR COLLECTING PII.....	6
4.1 System of Records Notices .....	7
4.1.1 Developing a New SORN.....	8
4.1.2 Biennial Review of a Current SORN.....	8
4.1.3 Altering an Existing SORN .....	9
4.1.4. Deleting a SORN .....	9
4.2 Privacy Impact Assessment (PIA) .....	11
4.2.1 Developing a Privacy Impact Assessment.....	12
4.3 Privacy Act Statements and Privacy Advisories.....	13
4.4 Social Security Number Use .....	14
4.5 Records Management.....	17
4.6 Forms Management .....	18
4.7 Public Information Collections.....	19
5.0 SAFEGUARDING PII .....	22
5.1 Safeguarding Paper Documents.....	23
5.2 Safeguarding Electronic Files .....	23
5.2.1 Websites.....	24
5.2.2 Email.....	25
5.2.3 Portable Electronic Devices / Mobile Devices .....	25
5.3 Telework Procedures for Safeguarding PII.....	26
5.4 Proper Disposal of PII.....	26
6.0 PII BREACH REPORTING AND INCIDENT RESPONSE .....	27
6.1 Reporting Procedures.....	27
6.2 Penalties .....	28
7.0 TRAINING .....	28
8.0 GLOSSARY .....	29

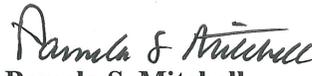
9.0 ACRONYMS .....	33
10.0 TABLE OF FIGURES .....	34
11.0 APPENDICES .....	35
Appendix A: New, Altered, and Deleted SORN Templates.....	35
Appendix B: System of Records Blanket Routine Uses.....	45
Appendix C: Privacy Act Exemptions.....	47
Appendix D: PIA Checklist .....	57
Appendix E: Acceptable SSN Use Cases .....	61
Appendix F: SSN Justification Memorandum and Elimination Plan Templates .....	63
Appendix H: Public Information Collection 60-Day Notice Template .....	65
Appendix G: Privacy Incident Reporting Procedures.....	65
12.0 REFERENCES .....	71

## 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, safeguarding, maintaining, storing, and sharing personally identifiable information (PII) in accordance with the references in section 12.0, including but not limited to:

- The Privacy Act of 1974, as amended, section 552a of title 10, United States Code (Reference (a))
- Section 208 of Public Law 107-347, "E-Government Act of 2002" (Reference (b))
- Department of Defense Directive 5400.11, "DoD Privacy Program" (Reference (c))
- DoD 5400.11-R, "DoD Privacy Program" (Reference (d))
- Administrative Instruction 81, "OSD/Joint Staff (JS) Privacy Program" (Reference (e))

Revisions to this document will be issued periodically by the DHRA Headquarters (HQ)-Chief Management Officer (CMO) to reflect changes to policy, procedures, or responsibilities.

  
**Pamela S. Mitchell**  
**Director**

## 1.0 SCOPE

This reference provides guidance to ensure field activity compliance and management of all privacy-related items, specifically as they relate to:

- Systems of Records Notices (SORNs),
- Privacy Impact Assessments (PIAs),
- Privacy Act Statements (PASs) and Privacy Advisories,
- Social Security Number (SSN) Use,
- Records Management,
- Forms Management,
- Public Collection Compliance,
- Safeguarding PII,
- PII Breach Reporting, and
- Training.



## 2.0 RESPONSIBILITIES

### **DHRA Chief Management Officer (CMO)/Chief Information Officer (CIO)**

- Serve as the DHRA CIO approval authority for DHRA privacy compliance requirements.
- Establish guidance and procedures for collecting, safeguarding, maintaining, storing, and sharing PII.
- Disseminate guidance to the field activity and oversee the implementation of the statutory laws, federal regulations and standards, and DoD policies listed in Section 12.0, in coordination with the DHRA Office of General Council.
- Review all Component-level SORNs, PIAs, PASs and privacy advisories, SSN justification memorandums, records disposition schedules, official, public information collection packages, and PII breach reports.
- Manage the overall compliance of all DHRA systems and ensure that privacy requirements are evaluated throughout the certification and accreditation, and portfolio management processes.
- Establish training requirements and consolidate training numbers, as necessary.
- Provide DoD and federal reporting requirements to the Office of the Secretary of Defense (OSD)/Joint Staff (JS) Privacy Office and the Defense Privacy and Civil Liberties Division (DPCLD), as necessary.
- As part of the monthly DHRA HQ-CMO meetings, hold meetings with Component Privacy Officials to provide monthly updates and additional guidance and ensure compliance with all facets of this policy.
- Work in conjunction with the OSD Records and Information Management Program to ensure documents containing PII are kept in accordance with established records retention schedules.

- Work in conjunction with the DoD Forms Management Program to ensure DHRA information systems are compliant with DoD 7750.07-M (Reference (f)) and DoDI 8910.01 (Reference (g)).
- Work in conjunction with the DoD Information Collections Branch to ensure systems collecting PII from members of the public are in compliance with the requirements of the Paperwork Reduction Act of 1995 (Reference (h)).
- Coordinate privacy-related process changes with the Director, DHRA as necessary.

#### **DHRA Component Directors<sup>1</sup>**

- Ensure all systems and electronic collections containing PII have completed SORNs, PIAs, PASs or privacy advisories, records disposition schedules, and public information collection packages, as applicable.
- Review all SORNs biennially and provide the results of the review to the DHRA HQ-CMO.
- Reduce the use of SSNs to the greatest extent practicable, and ensure the completion of SSN justification memorandums, as applicable.
- Ensure all personnel are compliant with annual privacy training requirements.
- Designate a Component Privacy Official who is responsible for attending monthly DHRA HQ-CMO meetings, as well as complying with and executing the responsibilities of this guidance.
- Report all potential PII incidents and make notifications to affected person(s), as directed by the DHRA CMO/CIO in the event of a breach.

#### **Component Privacy Officials**

- Attend DHRA HQ-CMO meetings monthly, or as required.
- Ensure all government and contractor personnel have completed required training and report completion semiannually to the DHRA HQ-CMO in accordance with FISMA Section 803 reporting requirements.
- Coordinate with the DHRA HQ-CMO when responding to reports of PII incidents.
- Coordinate with Component Program Managers, Information Assurance Managers (IAMs), and Records Managers to produce and review SORNs, PIAs, and PASs or privacy advisories to ensure information system compliance.
- Ensure all Component systems are compliant with DoD records disposition requirements and records containing PII are not kept longer than required.
- Ensure all Component systems are compliant with the forms management requirements contained within DoD 7750.07-M (Reference (f)) and DoDI 8910.01 (Reference (g)).
- Ensure all Component systems collecting PII from members of the public are in accordance with the Paperwork Reduction Act (Reference (h)).
- Ensure all Component systems which collect SSNs have a current SSN justification memorandum.

<sup>1</sup> As long as the DMDC Component Director maintains an active Privacy Act program, and keeps the DHRA CMO/CIO informed of the status of all actions, DMDC need not go through DHRA HQ when working with the other offices in DoD (e.g., OSD/JS/DPCLD), but can continue to work directly with these offices.

## Component Program Managers

- Be responsible for working with the Component Privacy Official in maintaining the overall compliance of the information system.
- Provide subject matter expertise through the Component Privacy Official as required.

### 3.0 PERSONALLY IDENTIFIABLE INFORMATION

Personally identifiable information (PII) is defined as 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 only has a moderate 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 individual. Non-PII can become PII when combined with other publically available elements to positively identify an individual. So too, moderate-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 be high-risk PII, while a list of people receiving treatment for substance abuse would be.



**High-Risk PII:** PII which, if lost or compromised, is likely to cause significant harm to an individual

#### **Names and Identification:**

- Name and other names used
- Social security number, whole or partial
- Mother's maiden name
- Driver's license and other ID numbers (e.g., passport)

#### **Personal Contact Information:**

- Personal phone or email
- Home/ mailing address

#### **Birth Information and Demographics:**

- Date and/or place of birth
- Gender, race/ethnicity
- Legal status/citizenship

#### **Employment and Education:**

- Information on other employment
- Education records

#### **Medical and Financial Information:**

- Personal health information
- Genetic information
- Disability status
- Debt and assets

#### **Family Information:**

- Marital status
- Dependents' information
- Emergency contact information

#### **Biometrics:**

- Biometric records (fingerprint)
- Biometric statistics (eye color)

#### **Law Enforcement and Security:**

- Law enforcement information
- Security clearance level/date

**Moderate-Risk PII:** PII which, if lost or compromised, may cause harm to an individual

- Office location
- Business telephone number
- Business email address
- DoD ID number (EDI-PI)
- Job title
- Rank
- Pay grade

Could you find the information on a business card?



When PII is considered to be compromised, the responsible Component is required to follow the PII breach reporting procedures as outlined in section 6.0.

#### 4.0 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 in subsections 4.1- 4.7, as applicable.

In general, compliance documents should be submitted for review/completed in the following order:

1. System of records notice
2. Privacy impact assessment
3. Privacy Act statement/privacy advisory

Before SORNS are submitted:

- SSN justification memos should be drafted, where required.
- Records disposition schedules should be established with OSD Records and Information Management.
- Draft DD forms should be created, where required.

Following review of a SORN and PIA by the OSD/JS Privacy Office:

- Public information collection packages should be submitted to the DoD Information Collections Branch, where required.

Following approval of a PAS by the OSD/JS Privacy Office:

- Any draft DD forms should be submitted for coordination and processing with the DoD Forms Management Program.

Before a SORN can be submitted to the DPCLD for final approval:

- Public information collection packages must be approved by OMB.
- PIAs must be finalized and signed by the OSD/JS Privacy Office.

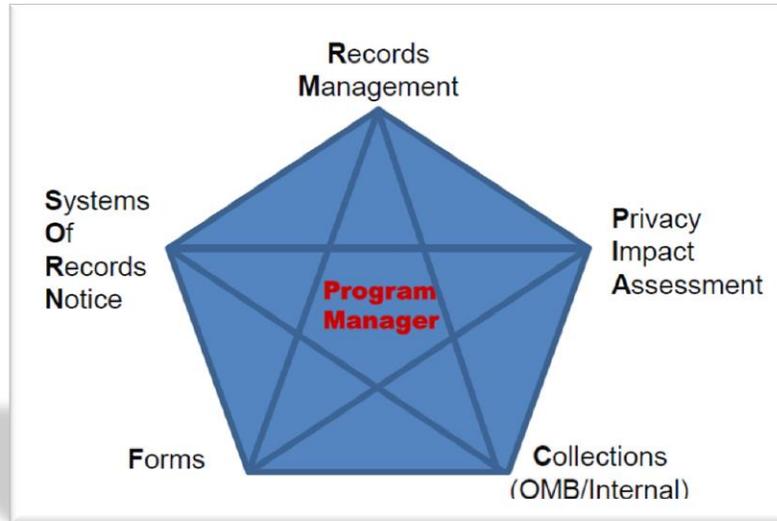
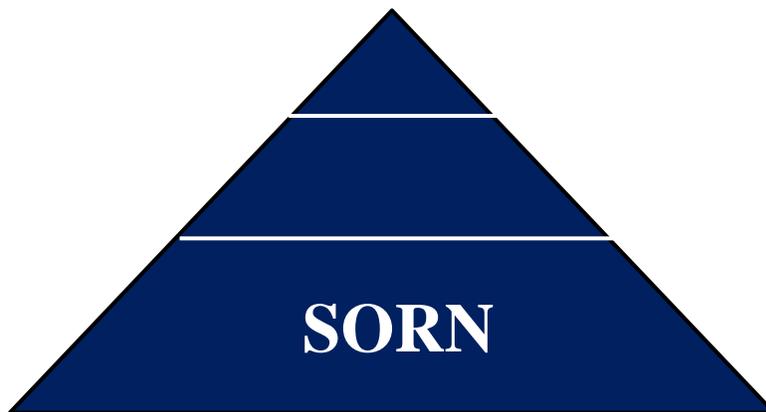


Figure 1. Privacy Compliance Matrix

#### 4.1 System of Records Notices

The Privacy Act requires all executive branch agencies to have a completed SORN for any electronic system or application that retrieves information about an individual using the individual’s name, or by an identifying number, symbol, or other identifying element assigned to the individual, before a system can begin to operate. The SORN is the foundation of the federal privacy program and defines the rules for collecting, using, storing, sharing, and safeguarding 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. All current SORNs must be reviewed biennially for relevance and accuracy and updated accordingly. A list of current SORNs is available on the DPCLD website at: <http://dpclد.defense.gov/Privacy/SORNs.aspx>.

#### 4.1.1 Developing a New SORN

The Component Privacy Official should take the following steps, in coordination with the Program Manager, when developing a new SORN:

1. The Component Privacy Official, in coordination with the Program Manager, develops and submits a draft SORN to DHRA HQ-CMO (See Appendices A-C for templates and additional information).
2. The DHRA HQ-CMO works with the Component Privacy Official to review and edit the SORN, as necessary. Once all edits have been adjudicated, the DHRA HQ-CMO submits the SORN to the OSD/JS Privacy Office.
3. The Component Privacy Official, in coordination with the DHRA HQ-CMO, responds to any questions from OSD/JS Privacy Office and updates the SORN as necessary.
4. The OSD/JS Privacy Office forwards the SORN to DPCLD for review. Upon DPCLD approval, the SORN will be submitted to the Federal Register by DPCLD for the required 30-day comment period. DPCLD will review and adjudicate public comments.
5. Once the SORN is finalized, the OSD/JS Privacy Office notifies the DHRA HQ-CMO and the SORN is published on the DPCLD webpage.
6. DHRA HQ-CMO notifies the Component that SORN has been finalized.



Figure 2. SORN Development Process

#### 4.1.2 Biennial Review of a Current SORN

Each Component is required to review its SORNs biennially. Component Privacy Officials are responsible for initiating and completing their biennial reviews on time. If review is not initiated

by the Component, the DHRA HQ-CMO will notify each Component Privacy Official regarding the required biennial reviews based on the established Federal Register publication date or the recertification date. Where no updates are needed, a memorandum for the record should be submitted to the DHRA-HQ CMO indicating that a review was conducted and the SORN was found to be current.

### 4.1.3 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 alter significantly the character and purpose of the record system are considered alterations.



#### Criteria for the Alteration of a SORN

- A significant increase or change in the number, type, or scope of individuals about whom records are maintained. Increases in numbers of individuals due to normal growth are not considered alterations unless they truly alter the character or purpose of the system.
- An expansion in the types or categories of information maintained.
- An alteration in how the records are organized or the manner in which the records are indexed and retrieved. If the records are no longer retrieved by name or personally identified then the SORN should be canceled.
- A change in the purpose for which the information in the system is used.
- Changes that alter the computer environment (such as changes to equipment, configuration, software, or procedures) so as to create the potential for greater or easier access—for example, increasing the number of offices with direct access, or the addition of online capability to a previously batch-oriented system.
- The connection of two or more formerly independent automated systems or networks, creating a potential for greater access.
- The addition of an exemption.
- The addition or deletion of a routine use pursuant to 5 U.S.C. 552a(b)(3).
- A change in applicable safeguards as a result of risk analysis.

The Component Privacy Official, in coordination with the Program Manager, should follow the same steps for altering a SORN as those required for developing a new SORN (Section 4.1.1.).

The notice of alteration should include:

1. Draft “Narrative Statement on an Altered System of Record”.
2. Summary of proposed changes.
3. Draft SORN with proposed changes incorporated (See Appendices A-C for templates and additional information).

### 4.1.4. 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 Privacy Official must verify why the SORN is no longer required and whether records must continue to exist or may be destroyed in accordance with the established National Archives Records Administration (NARA) records disposition schedule.

To discontinue a system, the Component Privacy Official should prepare a notice of deletion. Until the notice of deletion is completed, the SORN will be maintained and all records must remain intact until the NARA retention and disposal schedule is approved. The Component Privacy Official may essentially follow the steps in Section 4.1.1 when completing the notice of deletion. The notice of deletion must include:

1. The system identifier, system name, and current Federal Register citation.
2. The reason for deletion.
3. List of successor systems in the deletion notice, if eliminated through combination or merger (See Appendix A for template).

The Component Privacy Official should take the following steps, in coordination with the Program Manager, when deleting a system:

1. The Component Privacy Official, in coordination with the Program Manager, submits notice of deletion to DHRA HQ-CMO.
2. The DHRA HQ-CMO will work with the Component Privacy Official to review and edit the notice, as necessary. Once all edits have been adjudicated, the DHRA HQ-CMO submits the notice to the OSD/JS Privacy Office.
3. The Component Privacy Official, in coordination with the DHRA HQ-CMO, responds to any questions from OSD/JS Privacy Office and updates the notice as necessary.
4. The OSD/JS Privacy Office forwards the notice to DPCLD for review. Upon DPCLD approval, the notice will be submitted to the Federal Register by DPCLD for the required 30-day comment period. DPCLD will review and adjudicate public comments.
5. Once the notice is finalized, the OSD/JS Privacy Office notifies the DHRA HQ-CMO and the SORN is removed from the DPCLD webpage.
6. DHRA HQ-CMO notifies the Component that the notice has been deleted, and removes the coordinating system PIA from the DHRA webpage.

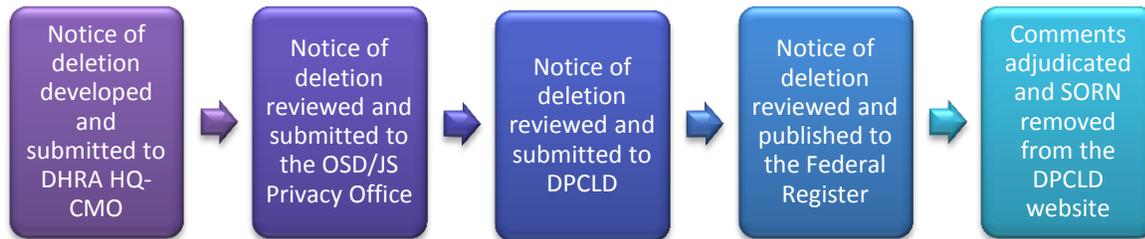


Figure 3. SORN Deletion Process

## 4.2 Privacy Impact Assessment (PIA)

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

- Developing or procuring 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 for ten or more members of the public.

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

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

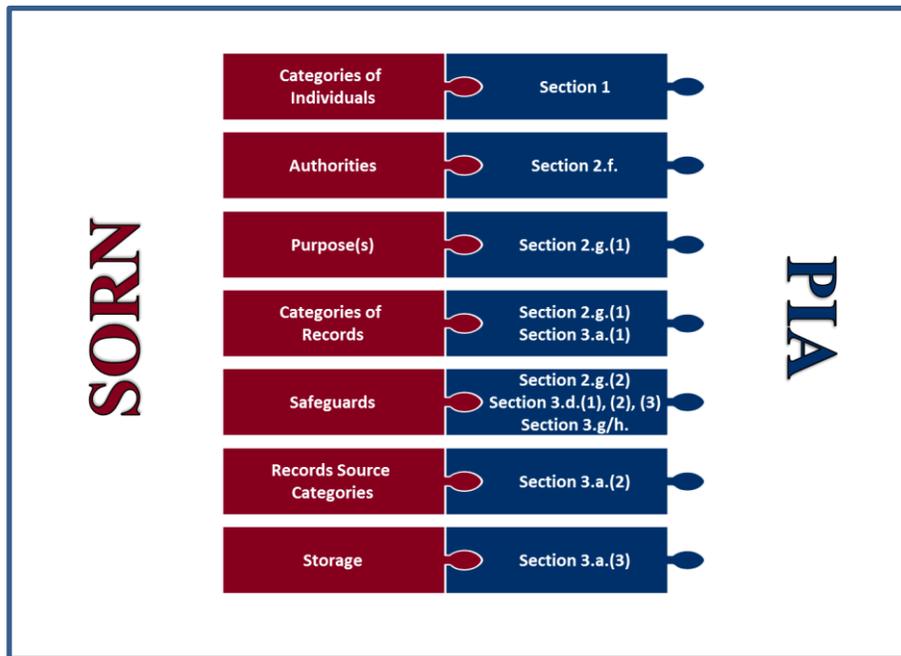
PIAs are conducted in order to:

- 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 (Reference (b)) and DoDI 5400.16 “DoD Privacy Impact Assessment Guidance” (Reference (i)), systems owners and privacy officials must complete a PIA for every Information Technology (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 by the Component Privacy Official; however, it is recommended that PIAs be updated as part of the biennial SORN review process if significant changes are made.

### 4.2.1 Developing a Privacy Impact Assessment

Every IT initiative will, at a minimum, have completed Section 1 of DD Form 2930, “Privacy Impact Assessment (PIA),” which is used to determine if the system processes PII. (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j)).) If it is determined that a system does not process PII during completion of Section 1 of DD Form 2930, no further sections need to be completed. The Component Privacy Official, Program Manager, or other designee must only locally maintain a copy of the DD Form 2930 with Section 1 completed.



**SORN and PIA Similarities**

If the information system does process PII, the Component Privacy Official should take the following steps, while working with the IAM and Component Program Manager as necessary:

1. Submit a draft PIA to the DHRA HQ-CMO (See Appendix D for additional guidance).
2. DHRA HQ-CMO will work with the Component Privacy Official to review and edit the PIA, as necessary. Once all edits have been adjudicated, the DHRA HQ-CMO submits the PIA to the OSD/JS Privacy Office for review.
3. The Component Privacy Official responds to any questions from the OSD/JS Privacy Office, in coordination with the DHRA HQ- CMO, and updates the PIA as necessary.
4. Once the PIA is finalized, it will be routed for signature by the Component Program Manager or designee. The PIA will be signed by the Component Privacy Official,

Component Program Manager, DHRA Privacy Officer, DHRA CMO/CIO, and the OSD/JS Privacy Official.

5. The DHRA HQ-CMO will post Sections 1 and 2 of all Component PIAs at <http://www.dhra.mil/website/headquarters/info/pia.shtml>. If it is determined by the Component Privacy Official/DHRA HQ-CMO that publishing the PIA may raise security concerns due to the sensitive nature of the system, a non-sensitive summary of the document may be prepared and submitted for publication along with the original PIA. If a summary will not eliminate the security concerns, the PIA will not be posted and will be maintained by the Component.
6. Once posted online, the DHRA HQ-CMO provides the final PIA and the website address of where it is located to DoD CIO at [osd.mc-alex.dod-cio.mbx.pia@mail.mil](mailto:osd.mc-alex.dod-cio.mbx.pia@mail.mil) and to the Component Privacy Official.

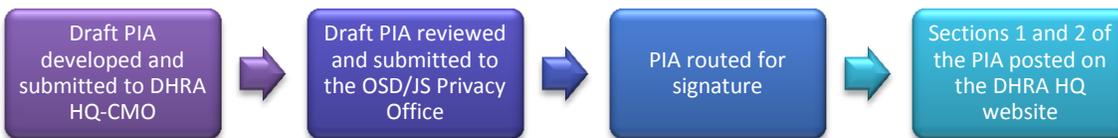


Figure 4. PIA Development Process

### 4.3 Privacy Act Statements and Privacy Advisories

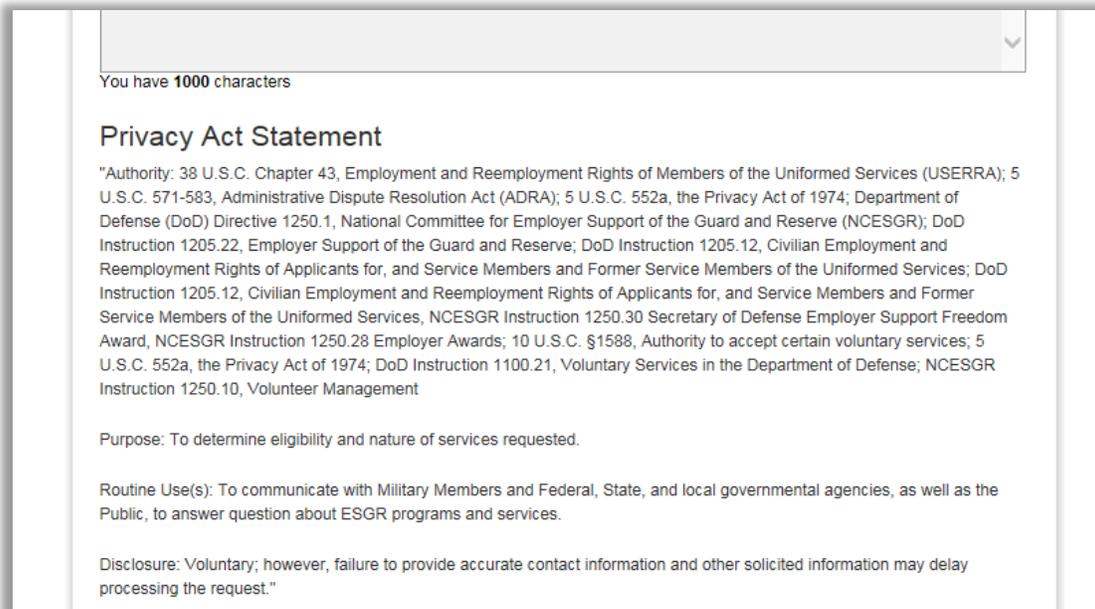
When an individual is requested to provide PII (e.g., name, date of birth, SSN) for inclusion into a system of record or to confirm that their information is current and correct, a PAS must be provided to the individual at the point of collection, regardless of the method used to collect the information (e.g., paper or electronic forms, personal interviews, telephonic interviews). When SSNs are being collected, a PAS is always required.

A PAS enables an individual to make an informed decision on whether to provide the information being requested by identifying:

- The authority for collecting the information,
- The purpose for collecting the data,
- The routine uses of the data, 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 shall 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” (Reference (d)). The PAS should be completed following review and approval of a system’s SORN and PIA.

Alternatively, 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, 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 shall be posted on the web page or other source where the information is being solicited, or via a click through pop up window or well-marked hyperlink (See Appendix I for process map).



#### 4.4 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” (Reference (d)).

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



#### Most Commonly Used SSN Acceptable Use Cases

Law Enforcement, National Security, and Credentialing. Almost every law enforcement application available to federal, state, and local law enforcement and other criminal justice agencies reports and tracks individuals, and makes application information available to other agencies, through the use of SSNs. This includes, but is not limited to, checks of the National Crime Information Center, state criminal histories, and Federal Bureau of Investigation records checks (Use Case 2).

Security Clearance Investigation or Verification. The initiation, conduct, adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of SSNs. The SSN is the single identifier that links all of the aspects of these investigations together. This use case is also linked to other federal agencies that continue to use SSNs as a primary identifier (Use case 3).

Computer Matching. Systems, processes, or forms that interact with other Government agencies may require the continued use of SSNs as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions (Use case 8).

Legacy System Interface. Many systems, processes, or forms that do not meet the criteria of numbers 1-10 for the continued use of SSNs may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using SSNs, or due to the excessive cost associated with the change. In these cases, the continued use of SSNs may be acceptable for a specified period of time, provided that formalized, written plans are in place for the migration away from SSNs in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from SSNs not cause unacceptably long interruptions to continued operations (Use case 11).

Operational Necessity. In austere or tactical environments where continuity of operations requires the use of SSNs even on hard copy lists and spreadsheets, approval can be granted that supersedes normal requirements. An example of this may include a system in a tactical environment where hard copies are used in the event of a loss of power to the system. To ensure that this is only used in cases of absolute necessity, justification of this use case must be approved by the Combatant Commander (Use case 12).

\*See Appendix E for complete list of SSN Acceptable Use Cases.

When requesting, collecting, transmitting, or maintaining an individual's SSN in any form (including truncated, masked, and encrypted SSNs), the responsible official shall:

1. Conduct a review to determine if the collection is compliant with Reference (k), and falls under the purview of one of the acceptable uses for SSN collection above.
2. Based on the determination above, complete 2a and/or 2b as follows:
  - a) Complete a SSN justification memorandum for all forms and IT systems that currently collect SSNs in accordance with Reference (k). The memorandum (see Appendix F for template) should include:
    - Name of the DoD information system or name and number of the form that will collect, use, maintain, and/or disclose a SSN.
    - Specific use case that grants authority for use of SSNs.
    - Citation of statutory requirement for the use of SSNs, if applicable.

- Appropriate system or form supporting documentation (e.g. SORN).
  - Physical, technical, and administrative safeguards to be put in place to reduce exposure of SSNs.
  - If a legacy system interface, an explanation of why any alternatives to the SSN that were considered are unacceptable.
  - If continued use of the SSN is not justified by one of the 13 acceptable use cases, an elimination plan should be developed and submitted to the DHRA-CMO with the SSN justification memorandum.
- b) Complete a SSN elimination plan, in addition to a SSN justification plan, for any use of SSNs that cannot be justified through appropriate authorities in accordance with Reference (k), going forward. The plan (see Appendix F for template) should outline what key actions are to be taken to eliminate the use of SSNs, along with POCs and timelines. The plan should also include the following, where relevant:
- What is replacing the SSN in the function for which it was used.
  - Associated forms and systems that will be affected by elimination of the SSN.
  - A mitigation strategy to reduce or eliminate the effects of removal of SSNs in conjunction with associated forms or systems.
  - Where elimination is not to occur immediately, include interim measures to provide additional protection of the SSNs.
  - Where elimination is dependent on changes to other systems and/or forms, include efforts made to work with the owners of those systems and/or forms to collaborate and eliminate the use of SSNs.
3. Submit the SSN justification memorandum and/or elimination plan for review to the DHRA HQ-CMO in coordination with review of the system SORN. DHRA HQ-CMO will then coordinate with the OSD/JS Privacy Office prior to the memorandum being submitted to DPCLD. Note: SSN elimination plans are not submitted to the OSD/JS Privacy Office or DPCLD.
4. Review the SSN justification memorandum biennially in coordination with SORN reviews. Component Privacy Officials are responsible for initiating and completing their biennial reviews on time. Where no updates are needed, a memorandum for the record should be submitted to the DHRA-HQ CMO indicating that a review was conducted and the SSN justification memorandum was found to be current.



Figure 5. SSN Use Process



## SSN Use Reminders

- 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.
- Remember that while DoD ID numbers have been used widely across the Department to replace the use of SSNs, these numbers are still considered PII and must be protected accordingly.

### 4.5 Records Management

It is DoD policy to create, maintain, and preserve information as records, in any medium, that document the transaction of business and mission in wartime and peacetime to provide evidence of DoD Component organization, functions, policies, procedures, decisions, and activities, in accordance with DoD Directive 5015.2, “DoD Records Management Program” (Reference (l)).

Section 1236 of title 36 of the Code of Federal Regulations (Reference (m)) requires both paper and electronic systems or applications to have a NARA-approved records disposition schedule to ensure that records created, maintained or stored in an electronic format are not kept longer than required. The Component Privacy Official will work with the DHRA HQ-CMO and the OSD Records and Information Management Program to request the retention and disposition schedule from NARA in accordance with Administrative Instruction 15, “OSD Records and Information Management Program” (Reference (n)).

If a General Records Schedule (GRS) or OSD records schedule applies to your collection:

1. Submit proposed retention schedule to DHRA HQ-CMO for review.
2. Submit reviewed retention schedule to the OSD Records Management Program, along with applicable SORNs and PIAs, for review and approval.
3. The OSD Records Management Program will complete a Memorandum for the Record (MFR) outlining the records retention schedule.
4. Submit final MFR to DHRA HQ-CMO.

If a GRS or OSD records schedule does not apply to your collection:

1. Complete a standard form (SF) 115 and submit it to the DHRA HQ-CMO for review. (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j))).
2. Submit the reviewed SF 115 to the OSD Records Management Program, along with applicable SORNs and PIAs, for review and approval.
3. The OSD Records Management Program will submit all new or revised retentions schedules to NARA for final approval.



## Records Retention Reminders

- Any SF-115 with a retention period less than three years must go to the General Accountability Office for further approval.
- Until a collection’s records schedule is approved, records may not be destroyed. Applicable SORNs and PIAs should note: “Disposition pending (until the National Archives and Records Administration approves a retention and disposal schedule, records will be treated as permanent).”

## 4.6 Forms Management

In accordance with DoD 7750.07-M (Reference (f)), any form used to collect information from other DoD Components, federal agencies, or the public must display an official DD form number. Further, per DoDI 8910.01 (Reference (g)), information collection forms that have not been properly approved and numbered will not be honored.

DoD forms must:

- Satisfy a valid need.
- Have a prescribing document or issuance.
- Have clear instructions and be standardized.
- Utilize information technology, to the maximum extent possible.
- When collecting PII, contain a PAS.

Before a SORN can be reviewed and approved by OSD/JS Privacy Office, any required DD form should be drafted in coordination with the DHRA-HQ CMO and the DoD Forms Management Program. Once a system’s PAS is reviewed and approved, DD Form 67, “Form Processing Action Request” should be completed, coordinated, and submitted to the DoD Forms Management Program in order to complete form creation and information collection approval. (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j)). All DHRA forms must be coordinated with the OSD/JS Privacy Office and the OSD Records and Information Management Program. Where a DD form will collect information from the public, a system must also have a valid public information collection package and be coordinated with the DoD Information Collections Branch before a form can be approved.

The image shows a screenshot of the DD Form 67, Form Processing Action Request. The form is divided into several sections:
 

- 1. DATE OF REQUEST (Y/M/D)**: A field for the date.
- 2. FORM AND COMPLETION (M, Department and Agency)**, **3. TITLE and (Approved) (M) Department and Agency**, **4. TO (Department and complete mailing address)**.
- 5. FORM DESIGNATION AND NUMBER**, **6. DDITION DATE and (M) Department**, **7. FORM TITLE**.
- 8. ACTION TYPE (Classification)**, **9. FORM TYPE (Classification)**, **10. SUBJECT GROUP (Classification)**, **11. PRIORITY/CLASSIFICATION (Classification)**.
- 12. FORM DISPOSITION (Classification)**, **13. UNCLASSIFIED FORM DESIGN CONSIDERATIONS**, **14. PURPOSE AND DESCRIPTION OF USE (Other information) (M) (Priority)**.
- 15. INTERNAL COORDINATION AND CONCURRENCE**: A table with columns for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D' and rows for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D'.
- 16. EXTERNAL COORDINATION AND CONCURRENCE (M) (Priority)**: A table with columns for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D' and rows for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D'.
- 17. APPROVALS (M) (Priority)**: A table with columns for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D' and rows for 'M', 'S', 'C', 'R', 'I', 'O', 'A', 'D', 'E', 'I', 'T', 'Y', 'C', 'O', 'M', 'P', 'L', 'E', 'T', 'E', 'D'.

 The form also includes a 'CERTIFICATION OF COMPLETION' section and a footer with 'DD FORM 67, FEB 2008' and 'PREVIOUS EDITION IS OBSOLETE'.

Note that electronic forms, including Excel and web-based forms, are still considered forms for the purposes of DoD policy and requirements, and require DD form development.

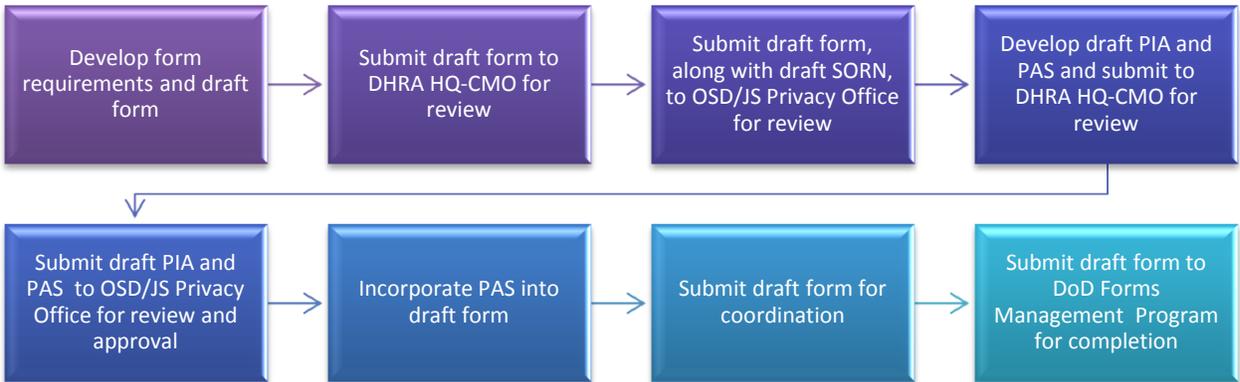


Figure 6. Forms Management Process

## 4.7 Public Information Collections

A public information collection is defined as a collection of standardized data from ten or more members of the public within a 12 month period. In accordance with the Paperwork Reduction Act (PRA) (Reference (h)) and updated guidance released in the Office of Management and Budget (OMB) memorandum “Information Collection under the Paperwork Reduction Act” (Reference (o)), before conducting a public information collection, federal agencies are required to seek public comment on proposed collections and to submit proposed collections for review and OMB approval. (Public information collection packages are also commonly referred to as OMB license or PRA packages.)



### Determining Whether the Paperwork Reduction Act Applies

Evaluate each of the questions below. If you answer yes to all four questions, follow the steps for creating and submitting a public information collection package outlined at the end of this section.

- **Are you collecting information on members of the public?**
  - Members of the public are defined as anyone who is not a federal employee or member of the military, including:
    - Individuals, partnerships, associations, corporations, business trusts or legal representatives, organized groups of individuals, and State, territorial, tribal, or local governments, or Components thereof;
    - Federal employees or Service members answering questions in their capacity as a private citizen;
    - Federal contractors; and
    - Foreign nationals.

- **Are you collecting standardized information?**
  - In other words, are respondents being asked to provide the same level of information on the same subject?
    - Questions need not be phrased exactly the same way each time they are asked.
  
- **Are you collecting non-minimal information?**
  - In other words, is the information being collected more than just name, address, phone, and/or email?
  
- **Does the information being collected fall within the OMB definition of information?**
  - OMB regulations define “information” as “any statement or estimate of fact or opinion, regardless of form or format, whether in numerical, graphic, or narrative form, and whether oral or maintained on paper, electronic or other media.” This may include:
    - Requests for information to be sent to the government, such as forms (e.g., the IRS 1040), written reports (e.g., grantee performance reports), and surveys (e.g., the Census).
    - Recordkeeping requirements (e.g., OSHA requirements that employers maintain records of workplace accidents).
    - Third-party or public disclosures (e.g., nutrition labeling requirements for food).
  - OMB regulation also specifies a number of items that are generally not “information” under the PRA. Important examples include:
    - Affidavits, receipts, changes of address, or consents;
    - Tests of the aptitude, abilities, or knowledge of persons; and
    - Facts or opinions that are:
      - Submitted in response to general solicitations of public comments.
      - Addressed to a single person.
      - Obtained or solicited at or in connection with public hearings or meetings.
      - Obtained through direct observation by the agency (e.g., through visual inspection to determine how long it takes for people to complete a specific transaction).
      - Obtained from participants in clinical trials (which typically do not involve answers to “identical questions”).

When OMB approves an information collection, it assigns an OMB control number which must be displayed on the information collection. PIAs and SORNs that cover collections from the public must include a valid (unexpired) OMB control number. The Component Privacy Official should work with the Office of the Undersecretary for Personnel and Readiness (OUSDP&R)) Information Management Control Officer (IMCO), in coordination with the DHRA HQ-CMO, to submit the information collection request to OMB. The Component Privacy Official should follow the following steps when processing a collection:

1. Contact the OUSD (P&R) IMCO, in coordination with the DHRA HQ-CMO, to verify that your collection requires compliance with the PRA and ensure that your information collection is not duplicative.
2. Estimate the burden of the collection and draft a 60-day Federal Register notice to inform the public of your intent to collect the information and solicit comments. (See Appendix G for template). The OUSD (P&R) IMCO must submit the draft 60-day notice to the DoD Clearance Officer for posting to the Federal Register.
3. Draft the OMB 83-I and Supporting Statement Part A for the collection. (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j))). If your collection involves statistical methods (surveys, focus groups, etc.), Supporting Statement Part B must also be completed. Once completed, conduct the following coordination on the 83-I coordination form, in collaboration with DHRA HQ-CMO, as appropriate (see [http://www.dtic.mil/whs/directives/collections/public\\_process.html](http://www.dtic.mil/whs/directives/collections/public_process.html) for more information on mandatory coordination):
  - a. OUSD(P&R) Forms Management Officer
  - b. Office of the Director, Defense Manpower and Data Center (DMDC) [Only required for surveys and focus group protocols.]
  - c. OSD/JS Privacy Office
  - d. OSD Records Manager
4. Adjudicate all public comments, in coordination with OUSD(P&R) IMCO. All comments from the public must be addressed in the supporting statement or submitted in a separate document to accompany the public information collection package to OMB.
5. Submit the public information collection package to the OSUD(P&R) IMCO. The package should include:
  - a. Signed OMB 83-I and completed 83-I coordination form.
  - b. Supporting Statement Part A.
  - c. Supporting Statement Part B if your collection involves statistical methods.
  - d. Copy of current SORN .
  - e. Copy of current PIA.
  - f. Applicable screenshots of system and collection or copies of currently approved or draft official form(s), as well as any instructions for completing information collection.

The OUSD(P&R) IMCO will submit the action package to the DoD Clearance Officer for:

1. Final review,
2. Posting to the Federal Register for a 30-day notice, and
3. Final submission to OMB.

OMB has 60 days to review the request. The second 30-day Federal Register notice is accomplished during this review period. During the 30-day Federal Register notice period, comments from the public are submitted directly to OMB.

At the conclusion of the 60-day OMB review period, OMB issues a notice of action. Components may begin collecting information as soon as they receive the approval notice of action. OMB may provide “terms of clearance” with their approval notice of action; these terms of clearance must be adjudicated before requests for changes or extensions are submitted. If OMB does not approve the collection, they will provide procedures to take in coordination with the OUSD(P&R) IMCO and the DoD Clearance Officer to appeal the decision. If OMB disapproves the request (typically due to package incompleteness), the approval process must begin again from the 60-day Federal Register notice [step 2].

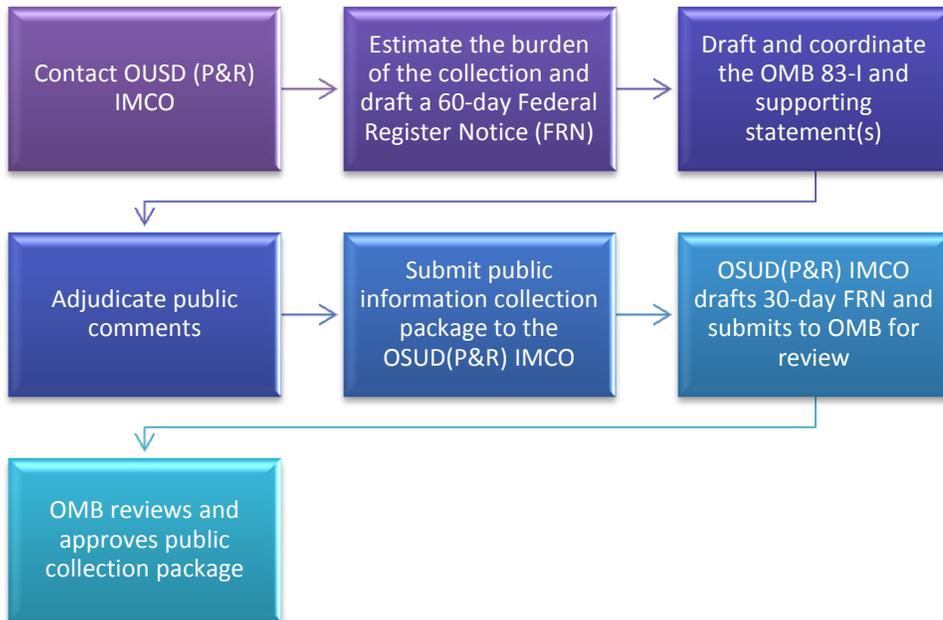


Figure 7. Public Collection Approval Process

## 5.0 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.

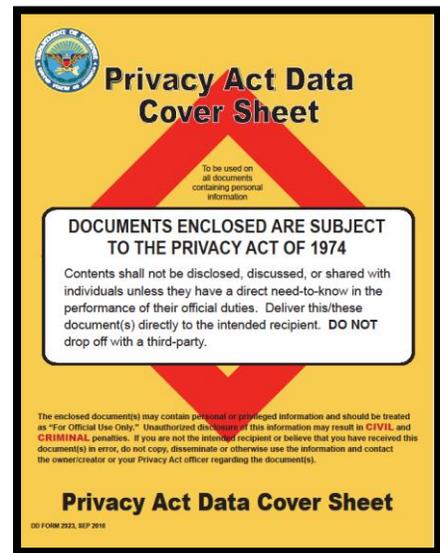
Safeguards should be tailored to the size and sensitivity of each system, as well as system-specific vulnerabilities. All records should be protected via physical and administrative safeguards, and ultimately disposed of via proper procedures. Electronic records must also possess technical safeguards to ensure damaging breaches do not occur.

PII must only be viewed by individuals who have an official need to know 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 breach has occurred and should be reported based on the procedures outlined in section 6.0.

## 5.1 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.” (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j)). This includes when faxing or mailing the document.
- Ensure control of the document and limit access to the document during the course of the day.
  - Never 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.
- Ensure all PII is placed securely out of sight at the end of each day in a locked cabinet or drawer.



## 5.2 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 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. This includes documents stored on shared drives or SharePoint platforms.
- 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.

### 5.2.1 Websites

OSD Memorandum 13798-10, “Social Security Numbers Exposed on Public Facing and Open Government Websites” (Reference (p)) 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.

All DHRA and Component intranet sites providing access to or maintaining PII, at a minimum, will be:

- Secured in a manner consistent with current encryption and authentication mechanisms, (e.g., Secure Socket Layer and Public Key Infrastructure (PKI)).
- Only accessible to individuals with an official need to know.

### 5.2.2 Email

The most common breach of PII occurs via email, when PII is transmitted or retransmitted unencrypted 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 DoD-approved PKI certificates.
- When encryption is unavailable, at a minimum, password-protect any related files being transmitted and send the password in a separate communication.
- 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.
- Do not send PII, encrypted or not, via non-DoD email addresses.

### 5.2.3 Portable Electronic Devices / Mobile Devices

Any portable electronic device (e.g., laptop, cell phone, etc.) or mobile storage device which processes or stores electronic records containing PII shall be data-at-rest encrypted and have the capability for data-in-transit encryption. Such security measures should be in accordance with the Cryptographic Module Validation Program as specified in Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules” (Reference (q)). 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).

### **5.3 Telework Procedures for Safeguarding PII**

When you take government records 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:

- All documents must be kept in an enclosed container, such as a briefcase, other bag, or envelope, when transporting them to and from alternate worksites. Open-hand carrying of documents is not permitted.
- Documents and laptop computers may not be left unattended in a private vehicle or other conveyance at any time.
- Never openly 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.
- Once at the telework site, the information must be maintained in a controlled environment where no others have access, including family members. All records and electronic files should remain under the continuous, direct control of the teleworker.
- When the work has been completed, the documents must be placed in a locked cabinet until they are returned to the worksite.
- Personal computers cannot be used to work on files containing PII.

### **5.4 Proper Disposal of PII**

Records containing PII must be properly disposed of so as to prevent inadvertent compromise. All records should be disposed of in accordance with their applicable records disposition schedule. Destruction should be tailored to the type of media involved.

For paper media, disposal methods may include: tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation.

For electronic media, disposal methods may include: overwriting, degaussing, disintegration, pulverizing, burning, melting, incineration, shredding, or sanding.

## 6.0 PII BREACH REPORTING AND INCIDENT RESPONSE

A breach is the actual or possible 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 for an other-than-authorized purpose. Examples of PII breaches include sending an email with PII to a non-.mil recipient or the wrong DoD recipient, or giving access to PII to individuals without an official need to know.

Federal reporting requirements established by the Federal Information System Management Act of 2002 (Reference (r)) and updated procedures established in OMB Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” (Reference (s)) require incidents involving PII to be reported to the federal incident response center, the United States Computer Emergency Readiness Team (US-CERT), within one hour. If an individual suspects a PII breach has occurred, they should follow the reporting procedures in subsection 6.1.

### 6.1 Reporting Procedures

When it is suspected that PII has been breached, an official breach report must be submitted, using the DD Form 2959, “Breach of Personally Identifiable Information (PII) Report.” (All forms can be retrieved from the DoD Forms Management Program Site (Reference (j))). The DD Form 2959 will be used by the DHRA HQ-CMO to report and analyze the breach or suspected breach and document notification to US-CERT or the individual, as well as the facts identified and decisions made by DHRA in accordance with Director of Administration and Management Memorandum, “Use of Best Judgment for Individual Personally Identifiable Information Breach Notification Determinations” (Reference (t)). All Component Privacy Officials or responsible designees should comply with the procedures outlined in Appendix H upon identifying a potential breach.

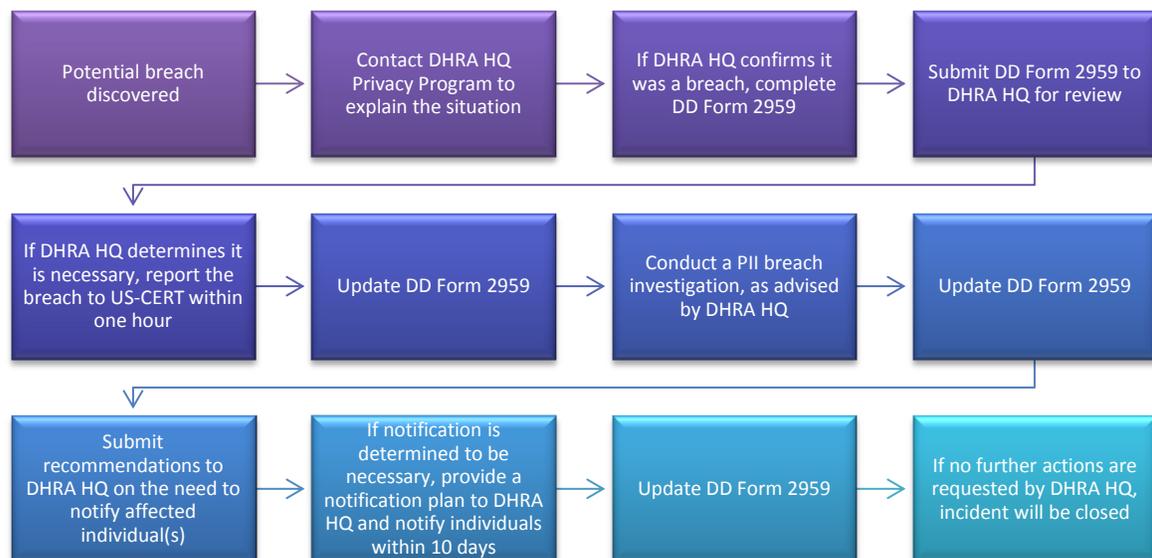


Figure 8. PII Incident Reporting Process

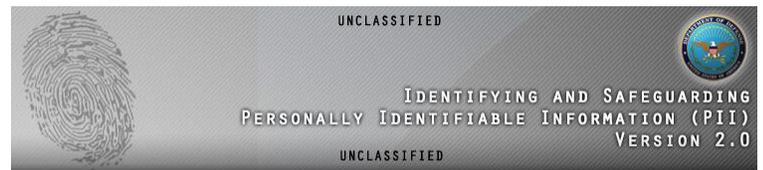
## 6.2 Penalties

A breach of PII may have major implications for the individual(s) responsible for the loss or compromise of the information and may lead to civil or criminal actions against the employee or agency, as well as fines in accordance with the Privacy Act (Reference (a)). 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 misdemeanor conviction and a 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 DHRA HQ-OGC.

## 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 and are available at the sites listed below:



- Cyber Awareness Challenge,  
<http://iatraining.disa.mil/eta/cyberchallenge/launchpage.htm>
- Identifying and Safeguarding Personally Identifiable Information (PII),  
<http://iatraining.disa.mil/eta/piiv2/launchPage.htm>

All DHRA Components are responsible for reaching 100% compliance with these training requirements by the end of February of each year for Cyber Awareness training and the end of July for PII training. Component Privacy Officials will be responsible for reporting training compliance to the DHRA HQ-CMO bi-annually, or as requested. The DHRA HQ-CMO will be responsible for consolidating all training compliance information and providing it to the OSD/JS Privacy Office. Designated Component Privacy Officials may also be required to take additional privacy training, as determined by the DHRA HQ-CMO with consensus of the other Component Privacy Officials at the beginning of each fiscal year.

## 8.0 GLOSSARY

**Breach.** A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where access or potential access to PII, whether physical or electronic, is given to persons other than authorized users and/or 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.

**DD Form.** A form approved by the DoD Forms Management Office, WHS, for use by two or more DoD Components. There are two types of DD forms:

**Prescribed DD Form.** A DD Form, the use of which by all DoD Components to whom the subject matter applies is mandatory.

**Adopted DD Form.** A DD Form, the use of which by DoD Components is optional. Normally, forms in this category are initiated by a DoD Component in conjunction with one or more other DoD Component(s).

**Disposition.** Those actions taken regarding federal records after they are no longer needed in office space to conduct current agency business. Records disposition is any activity that includes disposal of temporary records by destruction or donation; transfer of records to federal agency storage facilities or FRCs; transfer to the Archives of the United States, for records determined to have sufficient historical or other value to warrant continued preservation; or transfer of records from one federal agency to any other federal agency.

**Form.** A fixed arrangement of captioned spaces designed for entering and extracting prescribed information. Forms may be preprinted paper forms or electronic forms.

**General Records Schedule (GRS).** A schedule issued by the Archivist of the United States governing the disposition of specified recurring series common to several or all agencies of the federal government. These series include civilian personnel and payroll records, procurement, budget, travel, electronic, audiovisual, and administrative management records. When records described in the GRS are used by any federal agency, their disposition is governed thereby. Exceptions may be granted only by the Archivist of the United States. The GRS does not apply to an agency's program records.

**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” (Reference (d)). 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.

**Member of the Public.** Any individual or party acting in a private capacity, to include federal employees or military personnel.

**OSD Records Schedule.** A schedule issued by the OSD Records Administrator and approved by the Archivist of the United States governing the disposition of specified reoccurring series common to agencies throughout OSD.

**Permanent Records.** Records appraised by the Archivist of the United States as having enduring value because they document the organization and functions of the agency that created or received them or they contain significant information on persons, things, problems, and conditions with which the agency deals.

**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).** The analysis of how information is handled to: ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining, and disseminating information in

identifiable form in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Public Information Collection.** Information collections where an OSD or DoD Component collects information from the public. These collections require approval by OMB, via the DoD Public Information Collection Officer, pursuant to the requirements of the PRA.

**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.

**Records (Records Management).** Also referred to as federal records or official records. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them.

**Records Management.** The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and disposition in order to achieve adequate and proper documentation of the policies and transactions of the federal government and effective and economical management of agency operations.

**Records Disposition Schedule.** Sometimes called a Records Control Schedule, Records Retention Schedule or a Records Schedule. The administrative document used by OSD to obtain legal disposal authority for categories of its records. When authorized by the Archivist of the United States, these schedules grant continuing authority to dispose of identifiable categories of OSD records that already have accumulated and that will accumulate in the future.

**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.

**System of Records.** A group of records under the control of a DoD Component from which PII is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular uniquely assigned to an individual.

**System of Records Notice (SORN).** A notice published in the Federal Register that constitutes official notification to the public of the existence of a system of records.

**Temporary Records.** Records designated for retention for a specified period of time and then authorized to be destroyed in the current file area. Temporary records are most commonly found among housekeeping records and administrative files.

**Unscheduled Records.** Records whose final disposition has not been approved by the Archivist of the United States. Unscheduled records will be maintained in the current files area and treated like permanent records until disposition instructions have been approved by the National Archives and Records Administration.

## 9.0 ACRONYMS

CIO	Chief Information Officer
CMO	Chief Management Officer
DHRA	Defense Human Resources Activity
DPCLD	Defense Privacy and Civil Liberties Division
DoD	Department of Defense
DoDI	Department of Defense Instruction
FOUO	For Official Use Only
HQ	Headquarters
IAM	Information Assurance Manager
IT	Information Technology
IMCO	Information Management Control Officer
JS	Joint Staff
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
OGC	Office of General Counsel
OSD	Office of the Secretary of Defense
OUSD	Office of the Under Secretary of Defense
P&R	Personnel and Readiness
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
SORN	System of Records Notice
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team
WHS	Washington Headquarters Services

## 10.0 TABLE OF FIGURES

Figure 1. Privacy Compliance Matrix.....	7
Figure 2. SORN Development Process.....	8
Figure 3. SORN Deletion Process .....	11
Figure 4. PIA Development Process.....	13
Figure 5. SSN Use Process .....	16
Figure 6. Forms Management Process.....	19
Figure 7. Public Collection Approval Process.....	22
Figure 8. PII Incident Reporting Process.....	27

## 11.0 APPENDICES

### Appendix A: New, Altered, and Deleted SORN Templates<sup>2</sup>

#### NARRATIVE STATEMENT TEMPLATE

DEPARTMENT OF DEFENSE

[DoD Component]

Narrative Statement on a [New/Altered] System of Records  
Under the Privacy Act of 1974

1. System identifier and name: [System identifier], entitled "[SORN Title]."
2. Responsible official: *List the name, title, address, and telephone number of the official responsible for the report and to whom inquiries and comments about the report may be directed by Congress, the Office of Management and Budget, or the Defense Privacy Office.*
3. Purpose of establishing the system (New): The Office of the Secretary of Defense proposes to establish a new system of records to [purpose language].  
  
*This section should be the same as the purpose in the new SORN.*  
  
Nature of proposed changes for the system (Altered): The Office of the Secretary of Defense proposes to alter this system of records by changing the following sections: [list each section being changed].
4. Authority for the maintenance of the system: *This section should be the same as the authorities in the new SORN*
5. Probable or potential effect on the privacy of individuals: In [updating or establishing] this SORN, the [name of Component] reviewed the safeguards established for the system of records to ensure they are compliant with DoD requirements and are appropriate to the sensitivity of the information stored within

<sup>2</sup> Sources: DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007; Defense Privacy and Civil Liberties Office, "System of Records Notices (SORN) Handout," PACMan Training, September 2013; and OSD/JS Privacy Office, "OSD/JS Privacy Office SORN Quick Reference Guide," March 2014.

the system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information shared has been established.

6. Is the system, in whole or in part, being maintained, by a contractor? [Yes or No] If "Yes", please ensure that the contract has the necessary FAR clauses (subpart 24.1).

7. Steps taken to minimize risk of unauthorized access: Briefly describe the steps taken to minimize the risk of unauthorized access. Should match the safeguards section of the SORN.

8. Routine use compatibility: Provide assurances that any records contained in the system that are disclosed outside the DoD shall be for the use that is compatible with the purpose for which the record was collected. Advise whether or not the blanket routine uses apply to this system. This section should match the routine uses section of the SORN.

9. OMB public information collection requirements:

OMB collection required: [Yes/No]

OMB Control Number (if approved):

Title of collection if different than #10:

Date Approved or Submitted to OMB:

Expiration Date (if approved) or

*Provide titles of any information collection requests (e.g., forms and number, surveys, interview scripts, etc.) contained in the system of records.*

If collecting on members of the public and no OMB approval is required, state the applicable exception(s):

See DoDM 8910.1-V2, Enclosure  
3, paragraph 8.

10. Name of IT system: State "none" if paper records only. Name should be the same as that listed in DITPR.

## PROPOSED CHANGES TEMPLATE

System name:

[System Name] ([Date], [Current Federal Register citation]).

Changes:

\* \* \* \* \*

Start with this wording and list below it each SORN category which is being changed.

System Name:

Delete entry and replace with "[new language]."

\* \* \* \* \*

Use this language to describe each change.

If there are no changes to a category, use 5 asterisks with spaces between them as a place holder.

## SORN TEMPLATE

[System identifier]

System name:

System location:

Categories of individuals covered by the system:

Categories of records in the system:

Authority for maintenance of the system:

Purpose(s):

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted in accordance with 5 U.S.C. 552a(b), the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

[Routine Uses]

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at:  
<http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Retrievability:

Safeguards:

Retention and disposal:

System manager(s) and address:

See "Explanation of SORN Categories" below for a description of each section and more information on how to fill out this template.

Font should be Courier New, size 12.  
  
Spell out all acronyms, except DoD, on first use.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the [title and mailing address of official whom the request must be directed].

Signed, written requests should contain an individual's [data elements required to complete the request].

Record access procedures:

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act, Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155.

Signed, written requests should contain an individual's [data elements required to complete the request].

Contesting record procedures:

The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories:

Exemptions claimed for the system:

## SORN DELETION TEMPLATE

Deletion:

[System identifier]

[System Name] ([Date], [Current Federal Register citation]).

Reason: *This section should explain why the SORN is being deleted and what is happening to the system and/or records.*

## EXPLANATION OF SORN CATEGORIES

### **1. System name:**

The system name must indicate the general nature of the system of records and if possible, the general category of individuals to whom it pertains. The system name should not be more than 55 characters whenever possible.

### **2. System location:**

Provide the complete mailing address of each location/site maintaining the system of records. Be sure to include the 9-digit zip code. Do not use acronyms in addresses unless they are officially part of the U.S. Postal mailing address. P.O. Boxes cannot be used.

### **3. Categories of individuals covered by the system:**

Identify in clear, non-technical terms the specific individuals on whom records in the system are being maintained.

### **4. Categories of records in the system:**

Describe in clear, non-technical terms the records maintained in the system. If your system of records notice covers a database, it is a good idea to get a print out of the data to see all the records being maintained. If official forms are used to collect data for system records, ensure all fields from the forms are included here. Ensure the data elements listed in the notification and access sections are included here, unless used only for verification.

### **5. Authority for maintenance of the system:**

A federal law or executive Order (E.O.) of the President must authorize the collection and maintenance of a system of records. Whenever possible, cite the specific provisions of the statute or E.O. When Components use their general statutory grants of authority statute (“internal housekeeping”) as the primary authority, the regulation/directive/instruction implementing the statute within the DoD Component should also be identified.

When collecting the Social Security Number (SSN), always place “E.O. 9397 (SSN), as amended” in your authority. This E.O. will never stand alone as an authority to collect and maintain information under the Privacy Act. Authorities should be listed in the following order: U.S.C., DoDD, DoDI, DoD manual or regulation, AI, CFR, E.O. Ensure titles of authorities are listed and correct, and only include those authorities which directly authorize the collection or maintenance of the system of records.

### **6. Purpose(s):**

List the specific purpose(s) for establishing the system and the uses made of the information within the DoD Component and the DoD. Explain (1) why you collect this information in the first place and (2) how the information is used in the course of DoD business. Include all purposes and uses within DHRA and DOD. Once the notice is published, you may only use the data for the purposes you described.

**7. Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

List all non-DoD Agencies and entities (including private sector entities) that will routinely be provided access to the data or will be given the data upon request. List the specific activity or element within the agency/entity to which the record may be disclosed. Here you will also include the purpose of providing access. Routine uses should be written as: To [user] to [uses – what they do with the information] for the purposes of [objective]. Keep in mind, if your routine use clause shows “None”, and you get a request from another non-DoD entity for access to the records, you must refuse the request, no matter how valid the request or how important it is that you comply.

All DHRA SORNS should list routine uses 01, 04, 09, 12, and 15, and their full descriptions. All DHRA SORNs which deal with military personnel records should list routine uses 02 and 03, and their full descriptions. All DHRA SORNs which deal with civilian personnel records should list routine uses 02, 03, 08, and 13, and their full descriptions.

**8. Storage:**

State the medium(s) used to store the information in the system. Use one of the following:

- Paper file folders and electronic storage media.
- Records may be stored on paper and/or electronic storage media.
- Maintained in file folders and on electronic storage media.
- Paper and/or electronic media.

**9. Retrieval:**

Indicate how records are retrieved from the system (e.g., “by name,” “by SSN,” or “by name and SSN”). To be subject to the Privacy Act, records within a system of records must be retrieved by a personal identifier.

**10. Safeguards:**

Identify the methods used to protect the records, such as safes, vaults, locked cabinets or rooms, guards, visitor registers, personnel screening, or computer “fail-safe” systems software. Do not describe safeguards in such detail as to comprise system security. Start with describing the facility/building safeguards, then the room, then the computer/file cabinet. Then indicate the personnel getting access to the information.

**11. Retention and disposal:**

State the length of time records are maintained by the Component in an active status, when they are transferred to a federal records center, how long they are kept at the federal records center, and when they are transferred to the National Archives or destroyed. If the disposition for system records in with NARA for approval the SORN should say: “Disposition pending (treat records as permanent until the National Archives and Records Administration has approved the retention and disposition schedule).”

**12. System manager(s) and address:**

Provide the title and complete mailing address of the official(s) responsible for managing the system of records.

**13. Notification procedure:**

Describe how an individual can determine if a record in the system of records pertains to them. Provide the title and complete mailing address of the official to whom the request must be directed, the information the individual must provide in order for the Component to respond to the request, and a description of any proof of identity required.

**14. Record access procedures:**

Describe how an individual can review the record and/or obtain a copy of it. Provide the title and complete mailing of the official to whom the request for access must be directed, the information the individual must provide in order for the Component to respond to the request, and a description of any proof of identity required. If personal visits can be made to access the record, indicate where, when, how, and if any identification is required.

**15. Contesting record procedures:**

This entry should read the same for all Component notices

**16. Record source categories:**

Describe where the Component obtained the information (source documents and other agencies) maintained in the system. Describe the record source in general terms.

**17. Exemptions claimed for the system:**

If no exemption has been established for the system, indicate "None". If any exemption rule has been established, state under which provision(s) of the Privacy Act it was established. Also state that an exemption rule has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e). Use the following text for stating which exemptions apply:

- When establishing a (j)(2) exemption:
  - *Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) if the information is compiled and maintained by a Component of the agency which performs as its principle function any activity pertaining to the enforcement of criminal laws.*
- When establishing a (k)(1) exemption:
  - *Information specifically authorized to be classified under E.O. 12958, as implemented by DoD 5200.1-R, may be exempt pursuant to 5 U.S.C. 552a(k)(1).*
  - NOTE: Each DoD Component should have established a 'blanket' (k)(1) exemption within their respective procedural/exemption rule (See DoD 5400.11-R, Chapter 5, paragraphs C5.1.3 1. and 2).
- When establishing a (k)(2) exemption:
  - *Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C. 552a(j)(2), may be exempt pursuant to 5 U.S.C. 552a(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of the information, the individual will be provided access to the information exempt to the extent that disclosure would reveal the identity of a confidential source.*

- NOTE: When claimed, this exemption allows limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.
- When establishing a (k)(3) exemption:
  - *Records maintained in connection with providing protective services to the President and other individuals under 18 U.S.C. 3506 may be exempt pursuant to 5 U.S.C. 552a(k)(3).*
- When establishing a (k)(4) exemption:
  - *Records maintained solely for statistical research or program evaluation purposes and which are not used to make decisions on the rights, benefits, or entitlement of an individual, except for census records which may be disclosed under 13 U.S.C. 8, may be exempt pursuant to 5 U.S.C. 552a(k)(4).*
- When establishing a (k)(5) exemption:
  - *Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.*
- When establishing a (k)(6) exemption:
  - *Testing or examination material used solely to determine individual qualifications for appointment or promotion in the federal service may be exempt pursuant to 5 U.S.C. 552a(k)(6), if the disclosure would compromise the objectivity or fairness of the test or examination process.*
- When establishing a (k)(7) exemption:
  - *Evaluation material used to determine potential for promotion in the Military Services may be exempt pursuant to 5 U.S.C. 552a(k)(7), but only to the extent that the disclosure of such material would reveal the identity of a confidential source.*

## Appendix B: System of Records Blanket Routine Uses<sup>3</sup>

### **1. Law Enforcement Routine Use:**

If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

### **2. Disclosure When Requesting Information Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

### **3. Disclosure of Requested Information Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

### **4. Congressional Inquiries Disclosure Routine Use:**

Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

### **5. Private Relief Legislation Routine Use:**

Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular A-19, at any stage of the legislative coordination and clearance process as set forth in that Circular.

### **6. Disclosures Required by International Agreements Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and

<sup>3</sup> Source: Defense Privacy and Civil Liberties Office, "System of Record Notices (SORNS): Blanket Routine Uses."

arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

**7. Disclosure to State and Local Taxing Authorities Routine Use:**

Any information normally contained in Internal Revenue Service (IRS) Form W-2 which is maintained in a record from a system of records maintained by a DoD Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 U.S.C., sections 5516, 5517, and 5520 and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76-07.

**8. Disclosure to the Office of Personnel Management Routine Use:**

A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

**9. Disclosure to the Department of Justice for Litigation Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any Component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

**10. Disclosure to Military Banking Facilities Overseas Routine Use:**

Information as to current military addresses and assignments may be provided to military banking facilities who provide banking services overseas and who are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

**11. Disclosure of Information to the General Services Administration Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the General Services Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

**12. Disclosure of Information to the National Archives and Records Administration Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

**13. Disclosure to the Merit Systems Protection Board Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices; including administrative proceedings involving any individual subject of a DoD investigation, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

**14. Counterintelligence Purpose Routine Use:**

A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

**15. Data Breach Remediation Purposes Routine Use:**

A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

**16. Information Sharing Environment Routine Use:**

A record from a system of records maintained by a Component consisting of, or relating to, terrorism information (6 U.S.C. 485(a)(4)), homeland security information (6 U.S.C. 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment, November 22, 2006) may be disclosed to a federal, state, local, tribal, territorial, foreign governmental and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) and Executive Order 13388 (October 25, 2005).

## Appendix C: Privacy Act Exemptions<sup>4</sup>

The head of an agency may promulgate regulations to exempt applicable records from particular provisions of the Privacy Act. Most notably those involving release of information to individuals that by its very nature would interfere with critical processes and/or expose

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i)

In order for the Department to exercise the provisions of these exemptions, notice of proposed rulemaking published in the Federal Register. No system of records within the Department of Defense shall be considered exempt from any provision of this Regulation until the exemption and the exemption rule for the system has been published as a final rule in the Federal Register.

Those exemptions routinely claimed DoD Components include:

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
(c)(3)	<p><b>ACCESS EXEMPTION</b></p> <p>Except for disclosures made under subsection (b)(7), an individual is entitled, upon request, to get access to this accounting of disclosures of his record.</p>	<p>An individual is not entitled to access information that is compiled in reasonable anticipation of a civil action or proceeding.</p> <p>The term “civil action or proceeding” is intended to include court proceedings, preliminary judicial steps, and quasi-judicial administrative hearings or proceedings (i.e., adversarial proceedings that are subject to rules of evidence).</p> <p>Any information prepared in anticipation of such actions or proceedings, to include information prepared to advise the DoD Component officials of the possible legal or other consequences of a given course</p>	<p>(b)(7) (law enforcement request) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.</p> <p>The exemption does not apply to information compiled in anticipation of criminal actions or proceedings.</p>	

<sup>4</sup> Source: Defense Privacy and Civil Liberties Division

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
		of action, is protected.  The exemption is similar to the attorney work-product privilege, except that it applies even when the information is prepared by non-attorneys.		
<b>(d)(5)</b>	Nothing in this [Act] shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.  The subsection (d)(5) provision is sometimes mistakenly overlooked because it is not located with the other exemptions in sections (j) and (k). It is an exemption from only the access provision of the Privacy Act.	This provision shields information that is compiled in anticipation of court proceedings or quasi-judicial administrative hearings.	This Privacy Act provision has been held to be similar to the attorney work-product privilege, and to extend even to information prepared by non-attorneys.  Unlike all of the other Privacy Act exemptions, subsection (d)(5) is entirely "self-executing," in-as-much as it does not require an implementing regulation in order to be effective.	
<b>(j)(1)</b>	The system of records is maintained by the Central Intelligence Agency.			
<b>(j)(2)</b>	Records maintained by an agency or Component thereof which performs as its principal function any activity pertaining to the	(j)(2)'s threshold requirement is that the system of records be maintained by an agency or Component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime	It has been held that the threshold requirement is not met where only one of the principal functions of the Component maintaining the system is criminal law enforcement  Once the threshold requirement is satisfied, it must be shown that	(c)(3); (c)(4); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(2);

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
	enforcement of criminal laws and which consists of identifying data compiled for the purpose of a criminal investigation, associated with an identifiable individual; or reports identifiable to an individual compiled at any stage of the process of enforcement of criminal laws.	<p>or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of:</p> <p>1.) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;</p> <p>2.) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or</p> <p>3.) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.</p>	<p>the system of records at issue consists of information compiled for one of the criminal law enforcement purposes listed in subsection (j)(2)(A)-(C).</p> <p>Several courts have held that an Inspector General's Office qualifies as a "principal function" criminal law enforcement Component.</p>	(e)(3); (e)(4)(G); (e)(4)(H); (e)(4)(I); (e)(5); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5); (g)(1); (g)(2); (g)(3); (g)(4); (g)(5); (h); (l)(1); (l)(2); (l)(3); (m); (n)
<b>(k)(1)</b>	Relate to the national defense or foreign policy and are properly classified.	The exemption has been construed to permit the withholding of classified records from an agency employee with a security clearance who seeks only private access to records about him.	<p>Blanket Exemption for Classified Material</p> <p>Component rules shall include a blanket exemption under section 552a(k)(1) from the access provisions (section 552a(d) and the notification of access procedures (section 552a(e)(4)(H) for all classified material in any systems of records maintained.</p> <p>DoD Components do not need to specifically claim an exemption under section 552a(k)(1) for any system of</p>	(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5);

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
			records. The blanket exemption affords protection to all classified material in all system of records maintained.	
(k)(2)	Investigatory records compiled for law enforcement purposes other than those spelled out in the general exemption.	Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section:  Provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence."	This exemption covers: (1) material compiled for criminal investigative law enforcement purposes, by non-principal function criminal law enforcement entities; and (2) material compiled for other investigative law enforcement purposes, by any agency.  The material must be compiled for some investigative "law enforcement" purpose, such as a civil investigation or a criminal investigation by a non-principal function criminal law enforcement agency.	(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5);
(k)(3)	Maintained in connection with providing protective services to the President of the United States or other individuals.	Maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18.	This exemption is applicable to certain Secret Service record systems.	(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3);

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
				(f)(4); (f)(5);
<b>(k)(4)</b>	<p>Exemption for Statistical Records. Subsection (k) (4) “Required by statute to be maintained and used solely as statistical records;”</p> <p>A “statistical record” is defined in subsection (a) (6) as “a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual by section 6 of title 13 (Census).”</p> <p>It is the intent of this provision to permit exemptions for those systems of records which by operation cannot be used to make a determination about an individual. This provision permits an agency head to exempt a</p>	<p>It is the intent of this provision to permit exemptions for those systems of records which by operation cannot be used to make a determination about an individual.</p> <p>This provision permits an agency head to exempt a system of records which is used only for statistical, research, or program evaluation purposes, and which is not used to make decisions on the rights, benefits, or entitlements of individuals except as permitted by section 8 of Title 13.</p> <p>The use of the language “required by statute to be maintained * * * only” suggests that systems of records which qualify to be exempted under this provision are those composed exclusively of records that by statute are prohibited from being used for any purpose involving the making of a determination about the individual to whom they pertain; not merely that the agency does not engage in such uses.</p> <p>Disclosure of statistical records [to the individual] in most instances would not provide any benefit to anyone, for these records do not have a direct effect on any given individual; it would however, interfere with a legitimate, Congressionally-sanctioned activity.</p>		(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5);

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
	<p>system of records which is used only for statistical, research, or program evaluation purposes, and which is not used to make decisions on the rights, benefits, or entitlements of individuals except as permitted by section 8 of Title 13. The use of the language “required by statute to be maintained * * * only” suggests that systems of records which qualify to be exempted under this provision are those composed exclusively of records that by statute are prohibited from being used for any purpose involving the making of a determination about the individual to whom they pertain; not merely that the agency does not engage in such uses.</p> <p>Disclosure of statistical records [to the individual]</p>			

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
	in most instances would not provide any benefit to anyone, for these records do not have a direct effect on any given individual; it would however, interfere with a legitimate, Congressionally-sanctioned activity. (House Report 93-1416 p 19).			
<b>(k)(5)</b>	Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified material, but only to the extent that the disclosure of material would reveal a source who furnished information to the government under an express promise of confidentiality.	Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence.  This exemption is generally applicable to source-identifying material in background employment and personnel-type investigative files.	Promises of Confidentiality: Only the identity of sources that have been given an express promise of confidentiality may be protected from disclosure under (k)(2) , (k)(5) and (k)(7). However, the identity of sources who were given implied promises of confidentiality in inquiries conducted before September 27, 1975, also may be protected from disclosure.  Ensure that promises of confidentiality are not automatically given but are used sparingly. Establish appropriate procedures and identify fully, categories of individuals who may make such promises. Promises of confidentiality shall be made only when they are essential to obtain the information sought.	(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5);
<b>(k)(6)</b>	Testing or examination	Testing or examination material used solely to determine		(c)(3); (d)(1);

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
	material used solely to determine individual qualifications for appointment or promotion in the federal or military service, if the disclosure would compromise the objectivity or fairness of the test or examination process.	individual qualifications for appointment or promotion in the federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process.		(d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5);
(k)(7)	Evaluation material used to determine potential for promotion in the Military Services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source.	Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [9-25-75], under an implied promise that the identity of the source would be held in confidence.		(c)(3); (d)(1); (d)(2); (d)(3); (d)(4); (d)(5); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); (f)(1); (f)(2); (f)(3); (f)(4); (f)(5); above
	Contents of Exemption Rules: Each exemption rule submitted for publication must contain:	The record system identifier and system name of the system for which the exemption is claimed;  The specific sections of Reference (b) under which the exemption for the system is claimed (for example, sections 552a(j)(2), 552a(k)(3), or 552a(k)(7) of Reference (b)); The specific sections of Reference (b) from which the system is to be exempted (for example, sections 552a(c)(3) or 552a(d)(1)-(5));	Do not claim an exemption for classified material for individual systems of records. The blanket exemption applies.  In order for DoD Components utilize this exemption, each must establish a “rule” in the Federal Register.	

	Use of Exemptions	Use exemptions only for the specific purposes set forth in the exemption rules, and only when they are in the best interest of the Government, and limit them to the specific portions of the records requiring protection.	Do not use an exemption to deny an individual access to any record to which he or she would have access.	Provision for which an exemption may be claimed
		The specific reasons why an exemption is being claimed from each section of the Act identified.		

- (c)(3) – Making disclosure accounting available to the individual
- (c)(4) – Informing prior recipients of corrections
- (d)(1) – Individual access to records
- (d)(2) – Amending records
- (d)(3) – Review of the Component’s refusal to amend a record
- (d)(4) – Disclosure of disputed information
- (d)(5) – Access to information compiled in anticipation of civil action
- (e)(1) – Restrictions on collecting information
- (e)(2) – Collecting directly from the individual
- (e)(3) – Informing individuals from whom information is requested
- (e)(4)(G) – Procedures for determining if a system contains a record on an individual
- (e)(4)(H) – Procedures for gaining access
- (e)(4)(I) – Describing categories of information sources
- (e)(5) – Standards of accuracy
- (f)(1) – Rules for determining if an individual is subject of a record
- (f)(2) – Rules for handling access requests
- (f)(3) – Rules for granting access
- (f)(4) – Rules for amending records
- (f)(5) – Rules regarding fees
- (g)(1) – Basis for civil action
- (g)(2) – Basis for judicial review and remedies for refusal to amend
- (g)(3) – Basis for judicial review and remedies for denial of access
- (g)(4) – Basis for judicial review and remedies for other failure to comply
- (g)(5) – Jurisdiction and time limits
- (h) – Rights of legal guardians
- (l)(1) – Records stored in GSA records center
- (l)(2) – Records archived before September 27, 1975
- (l)(3) – Records archived on or after September 27, 1975
- (m) – Applicability to Government contractors
- (n) – Mailing lists

## Appendix D: PIA Checklist<sup>5</sup>

### **General**

- Ensure all acronyms are spelled out on first use.
  - Exceptions: “DoD,” “OSD,” and “U.S.”
- Only capitalize proper nouns or terms such as: Service member, Federal Government, and Military Service (for more information see: [DoD 5100.40-M-V1](#), pp.30-32).
- Do not answer questions by referencing previous sections (e.g., “See answer to section 2f”).

### **Section 1: Is PIA Required?**

- Select all categories of individuals about whom PII is collected, maintained, used, and/or disseminated.
  - If data is collected on federal contractors or the public:
    - Contact DHRA HQ Privacy Program to discuss OMB/Paperwork Reduction Act licensure requirements.

### **Section 2: PIA Summary Information**

#### **2f. Authority to collect information**

- Ensure the authorities listed match those in the *published or draft* SORN.
  - If SSNs are contained in the system:
    - “E.O. 9397 (SSN), as amended” should be listed as the last authority.
  - If authorities have changed since the SORN was published:
    - Provide an explanation to DHRA HQ Privacy Program, and
    - Contact DHRA HQ Privacy program to discuss revisions to the SORN to reflect new authorities.
- List all authorities in the following order:
  - U.S.C.; DoDD; DoDI; DoD manual or regulation; AI; CFR; E.O.

#### **2g(1). Purpose**

- Describe the purpose clearly and succinctly, in non-technical language.
  - Purpose description should be *identical to or closely match* the purpose section of the published or draft SORN.
    - If the system purpose has changed since the SORN was published:
      - Provide explanation to DHRA HQ Privacy Program, and

<sup>5</sup> Source: DHRA-CMO Privacy Program

- Contact DHRA HQ Privacy Program to discuss revisions to reflect the changes.
- List all categories of PII collected.
  - Ensure all categories of PII listed in section 3a(1) are also listed in this section.

## **2g(2). Privacy risks and mitigation**

- Briefly describe potential privacy risks associated with system.
- Detail the security measures in place designed to mitigate these risks.
  - Summarize *all* security measures listed in section 3d.
    - Remember that only sections 1 and 2 of the PIA are published for the public to access. Make sure security measures are well highlighted in Section 2 to show the public how their privacy is being protected.

## **2h. PII data exchange recipients**

- List all entities with whom *system data* will be shared.
  - This section is *not about who has access to the system* itself, but, rather, with whom data from the system may be shared.

## **2k. Privacy statements and advisories**

- Copy and paste the text of any Privacy Act statements or privacy advisories that are provided to individuals when they are asked to provide PII.
  - Privacy Act Statement: When an individual is requested to furnish personal information about himself or herself for *inclusion in a system of records*, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.
  - Privacy Advisory: A notification informing an individual as to why information is being solicited and how such information will be used. If PII is *solicited by a DoD 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*, the solicitation of such information triggers the requirement for a privacy advisory.

## **Section 3: PIA Questionnaire and Risk Review**

### **3a(2). Source of PII collection**

- Clearly explain *all* sources of PII.

### **3a(3). Manner of collection**

- Select all manners in which information is collected in the system or collection.
  - If “Information Sharing-System to System” is selected:
    - Ensure all related databases are listed in section 3a(2).

- If paper or website forms are used:
  - List official draft or published DD forms used for the collection.
  - If no forms exist, contact DHRA HQ Privacy Program to determine if official form creation is needed.

**3a(4) and (5). Reason for collection and intended use**

- Answer questions clearly and succinctly, utilizing suggested language (e.g. “verification , identification, authentication, data matching” and “mission related use, administrative use”).

**3b. New PII creation via data aggregation**

- Answer this question if new PII is created or derived via *data aggregation*.
  - This question is not asking if the system involves *a data transfer*, but rather if *new PII is created through data aggregation*.
    - Data Aggregation: Any process in which information *is gathered and expressed in summary form* for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

**3d. Security controls**

- Ensure all security controls mentioned in sections 2g(2) and 3g are selected here.

**3f. Information handling practices and privacy**

- List and detail measures put in place to protect individual privacy at *each* of the following information life cycle stages:
  - Collection,
  - Use,
  - Retention,
  - Processing,
  - Disclosure, and
  - Destruction.
  - State the approved records disposition schedule.
    - If no records disposition has been established:
      - Contact DHRA HQ Privacy Program to discuss next steps.
    - If records disposition has been submitted to WHS and is pending:
      - State “Disposition pending (until the National Archives and Records Administration approves a retention and disposal schedule, records will be treated as permanent).”

**3g and h.**

- If this is an *existing* DoD information system or electronic collection (see section 2a):
  - Answer the question in section 3g.
    - Ensure *all* security measures detailed in sections 2g(2) and 3d(1), (2), and (3) are also detailed here.
- If this is a *new* DoD information system or electronic collection (see section 2a):
  - Answer the question in section 3h.
    - Ensure *all* security measures detailed in sections 2g(2) and 3d(1), (2), and (3) are also detailed here.

## Appendix E: Acceptable SSN Use Cases, as specified in DoDI 1000.30, Enclosure 2<sup>6</sup>

- 1. Geneva Conventions Serial Number.** As of the late 1960s, the SSN has served as the Geneva Conventions serial number for the Military Services. Many of the systems, processes, and forms used by the DoD categorize individuals by their SSNs. The Military Departments should begin to transition away from the SSN as the Geneva Conventions identifier.
- 2. Law Enforcement, National Security, and Credentialing.** Almost every law enforcement application available to federal, state, and local law enforcement and other criminal justice agencies reports and tracks individuals, and makes application information available to other agencies, through the use of SSNs. This includes, but is not limited to, checks of the National Crime Information Center, state criminal histories, and Federal Bureau of Investigation records checks.
- 3. Security Clearance Investigation or Verification.** The initiation, conduct, adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of SSNs. The SSN is the single identifier that links all of the aspects of these investigations together. This use case is also linked to other federal agencies that continue to use SSNs as a primary identifier.
- 4. Interactions with Financial Institutions.** Financial institutions may require that individuals provide SSNs as part of the process to open accounts. It may therefore be required to provide SSNs for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions.
- 5. Confirmation of Employment Eligibility.** Federal statute requires that all persons employed within the United States provide a SSN or comparable identifier to prove that they are eligible to work for or with the U.S. Government. Any system that deals with employment eligibility may contain SSNs.
- 6. Administration of Federal Workers' Compensation.** The Federal Workers' Compensation Program continues to track individuals through the use of SSNs. As such, systems, processes, or forms that interact with or provide information for the administration of this system or associated systems may be required to retain SSNs.
- 7. Federal Taxpayer Identification Number.** The application of federal and state income tax programs rely on the use of SSNs. As such, systems that have any function that pertains to the collection, payment, or record keeping of this use case may contain SSNs. Additionally, individuals who operate corporate entities under their own names may use their SSNs as the tax numbers for that business function.

<sup>6</sup> Source: DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012.

- 8. Computer Matching.** Systems, processes, or forms that interact with other Government agencies may require the continued use of SSNs as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions.
- 9. Foreign Travel.** DoD personnel are often required to travel beyond the borders of the United States and many members often require official clearance prior to travel. Currently, the SSN is used as the identifier for these purposes.
- 10. Noncombatant Evacuation Operations (NEOs).** The Department of State requires that all persons repatriated to the United States as part of a NEO present their SSN as part of this process. Any systems, forms, or processes supporting NEOs may be required to process individuals using the SSN as the primary identifier.
- 11. Legacy System Interface.** Many systems, processes, or forms that do not meet the criteria of numbers 1-10 for the continued use of SSNs may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using SSNs, or due to the excessive cost associated with the change. In these cases, the continued use of SSNs may be acceptable for a specified period of time, provided that formalized, written plans are in place for the migration away from SSNs in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from SSNs not cause unacceptably long interruptions to continued operations.
- 12. Operational Necessity.** In austere or tactical environments where continuity of operations requires the use of SSNs even on hard copy lists and spreadsheets, approval can be granted that supersedes normal requirements. An example of this may include a system in a tactical environment where hard copies are used in the event of a loss of power to the system. To ensure that this is only used in cases of absolute necessity, justification of this use case must be approved by the Combatant Commander.
- 13. Other Cases.** The previous categories may not include all uses of SSNs authorized by law. Should an application owner be able to show sufficient grounds that a use case not specified in numbers 1-12 is required by law, that use case may continue to use SSNs. Any application that seeks to use this clause as justification must provide specific documentation in order to continue use in accordance with this provision.

## Appendix F: SSN Justification Memorandum and Elimination Plan Templates<sup>7</sup>

### SSN JUSTIFICATION MEMORANDUM TEMPLATE

MEMORANDUM FOR DEFENSE PRIVACY AND CIVIL LIBERTIES DIVISION

SUBJECT: Justification for the Use of the Social Security Number (SSN) – [Form or System Name/Number]

*The memorandum should begin by naming and describing the system or form that is the subject of the justification. The description should be sufficiently detailed that someone unfamiliar with the system should be able to grasp a general understanding of its intent.*

*The justification for the use of the SSN should include a reference to the SSN instruction use case that is being used to justify the use of the SSN. If the justification does not fall under either the operational necessity use case or the legacy system interface use case, then the justification shall also include the specific legal authority that requires the use of the SSN and why it is applicable to the use being justified.*

*Reference should be made to the system or form supporting documentation, including, but not limited to, SORN, PIA, public information collection clearance, or any other documentation that may be appropriate. If the substance of the documentation is not attached, reference should be made to how the reader may gain access to this documentation.*

*Justification for the use of the SSN does not constitute blanket permission to use the SSN. Specific reference shall be made to indicate actions being taken to reduce the vulnerability of SSNs, which may include indicating where SSNs are being removed from transactions or any other protections that have been included. It should be obvious to the reader that a thorough effort has been made to evaluate the risk associated with the system or form and that every reasonable step has been or is being taken to reduce the use of the SSN and protect it where the use is still required.*

*If continued use of the SSN is not justified by one of the 13 acceptable use cases, reference shall be made to the plan and timeline for the elimination of the use of the SSN.*

[Director's Name]

[Title]

<sup>7</sup> Source: DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

## SSN ELIMINATION PLAN TEMPLATE

Social Security Number Elimination Plan				
<b>Component:</b>		<b>Date Last Updated:</b>		
<b>System Name:</b>		<b>POC Name:</b>		
<b>SORN Number:</b>		<b>POC Phone Number:</b>		
<b>Date Submitted:</b>		<b>POC Email:</b>		
<b>Key Action</b>	<b>Action POC</b>	<b>Initiation Date</b>	<b>Target Completion Date</b>	<b>Comments</b>
			<b>Final Completion Date</b>	

## Appendix G: Privacy Incident Reporting Procedures<sup>8</sup>

1. DHRA-HQ/DHRA Component discovers confirmed or potential PII breach.
  - 1.1. DHRA-HQ/DHRA Component contacts DHRA HQ-CMO to confirm the validity of, and alert DHRA-HQ CMO to, a potential breach.
2. DHRA-HQ/DHRA Component completes and submits the DD Form 2959 to the DHRA HQ-CMO within one hour of confirming the validity of a PII breach by emailing: [dhra.mc-alex.dhra-hq.mbx.privacy@mail.mil](mailto:dhra.mc-alex.dhra-hq.mbx.privacy@mail.mil).
3. DHRA HQ-CMO reviews the DD Form 2959 and coordinates with DHRA HQ-Office of General Council (OGC) and the OSD/JS Privacy Office as necessary.
  - 3.1. DHRA HQ-OGC provides input and guidance to DHRA HQ-CMO as needed regarding the PII breach.
4. DHRA HQ-CMO determines whether notification of the PII breach to the US-CERT is required. Generally if an incident is determined to be a cyber related (electronic) breach of PII, notification to the US-CERT is required.
  - 4.1. If DHRA HQ-CMO determines that notification of the PII breach to the US-CERT is not required, then the DHRA-HQ/DHRA Component updates section 2.b of the DD Form 2959 to include all actions take and lessons learned, then resubmits the form to the DHRA HQ-CMO.
    - 4.1.1. DHRA HQ-CMO notifies and submits the DD Form 2959 to the OSD/JS Privacy Office within 24 hours, in order to provide notification to the Defense Privacy and Civil Liberties Division (DPCLD) within 48 hours. If no further actions are requested, then the incident is closed.
  - 4.2. If DHRA HQ-CMO determines that notification of the PII breach to the US-CERT is required, then the DHRA-HQ/DHRA Component reports the breach, within one hour of notification, to the US-CERT by filling out the form at: <https://forms.us-cert.gov/report/>.
    - 4.2.1. US-CERT provides the DHRA-HQ/DHRA Component involved with the US-CERT number that tracks the breach.
    - 4.2.2. DHRA-HQ/DHRA Component adds the US- CERT number to the DD Form 2959.

---

<sup>8</sup> DHRA HQ Standard Operating Procedure 8.0, Privacy Incident Reporting, January 27, 2015.

5. DHRA-HQ/DHRA Component conducts a PII breach investigation to determine the medium (e.g. paper, email, etc.), category (e.g. lost, stolen, compromised, etc.), timeline and circumstances, number of individuals affected, type of PII compromised (e.g. SSN, personal email address, etc.) and risk level of the breach, as advised by the DHRA HQ-CMO.
  - 5.1. DHRA-HQ/DHRA Component updates DD Form 2959 with any new information discovered and provides it to the DHRA HQ-CMO.
  - 5.2. DHRA HQ-CMO notifies and submits the DD Form 2959 to the OSD/JS Privacy Office within 24 hours, in order to provide notification to the DPCLD within 48 hours.
6. DHRA-HQ/DHRA Component makes a recommendation to the DHRA HQ-CMO regarding notification of the PII breach to affected individual(s), based upon the number of data elements breached, number of individuals affected, likelihood the information is accessible and usable, likelihood the breach may lead to harm, and ability of the Department to mitigate the risk of harm.
7. DHRA HQ-CMO determines whether notification to the affected individual(s) is required and informs the DHRA-HQ/DHRA Component.
  - 7.1. If DHRA HQ-CMO determines that notification is not required, then the DHRA-HQ/DHRA Component updates section 2.b of the DD Form 2959 to include all actions taken and lessons learned, and submits the form to the DHRA HQ-CMO.
    - 7.1.1. If no further actions are requested by the DHRA HQ-CMO, then the DHRA HQ-CMO notifies the OSD/JS Privacy Office that the action is complete and the incident is closed.
  - 7.2. If DHRA HQ-CMO (with coordination from DHRA HQ-OGC) determines that notification to the affected individual(s) is required, then the DHRA-HQ/DHRA Component will provide the DHRA HQ-CMO with a notification plan, to include a template of the notification, anticipated notification date, and method of notification.
    - 7.2.1. DHRA HQ-CMO reviews and approves notification plan.
  - 7.3. DHRA-HQ/DHRA Component notifies all of the affected parties within ten days of the breach. In some instances, there may be circumstances where notification could be made at a higher level than DHRA. In certain cases credit monitoring may also be offered at the determination and cost of the DHRA-HQ/DHRA Component, or a determination made by the Director, DHRA.
    - 7.3.1. DHRA-HQ/DHRA Component updates section 2.b of the DD Form 2959 to include all actions taken and lessons learned, and submits it to DHRA HQ-CMO.

7.3.2. If no further actions are requested by the DHRA HQ-CMO, then the DHRA HQ-CMO notifies the OSD/JS Privacy Office that the action is complete and the incident is closed.

## Appendix H: Public Information Collection 60-Day Notice Template<sup>9</sup>

**Billing Code: 5001-06**

**DEPARTMENT OF DEFENSE**

Office of the Secretary

[Docket ID: DoD-[YEAR]-XX-XXXX]

Proposed collection; comment request

**AGENCY:** Office of the Under Secretary of Defense for Personnel and Readiness, DoD.

**ACTION:** Notice

**SUMMARY:** In compliance with the *Paperwork Reduction Act of 1995*, the Office of the Under Secretary of Defense for Personnel and Readiness announces a proposed public information collection and seeks public comment on the provisions thereof. Comments are invited on: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

**DATES:** Consideration will be given to all comments received by [insert 60 days from publication in the Federal Register].

---

<sup>9</sup> Source: DoD Information Collections Branch, "Public Collections," [http://www.dtic.mil/whs/directives/collections/public\\_process.html](http://www.dtic.mil/whs/directives/collections/public_process.html).

**ADDRESSES:** You may submit comments, identified by docket number and title, by any of the following methods:

- Federal eRulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100.

*Instructions:* All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

Any associated form(s) for this collection may be located within this same electronic docket and downloaded for review/testing. Follow the instructions at <http://www.regulations.gov> for submitting comments. Please submit comments on any given form identified by docket number, form number, and title.

**FOR FURTHER INFORMATION CONTACT:** To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to the [Component/Office Name], ATTN: [Name of Project Officer], [Address], or call [Component/Office Name], at [Telephone Number].

**SUPPLEMENTARY INFORMATION:**

**TITLE; ASSOCIATED FORM; AND OMB NUMBER:** [System/Collection Title]; [DD Form #####]; [OMB Control Number #####-#####].

**NEEDS AND USES:** The information collection requirement is necessary to [purpose].

**AFFECTED PUBLIC:** [Brief summary of category of individuals]

**ANNUAL BURDEN HOURS:** #

**NUMBER OF RESPONDENTS:** #

**RESPONSES PER RESPONDENT:** #

**AVERAGE BURDEN PER RESPONSE:** # [minutes/hours]

**FREQUENCY:** [On occasion, quarterly, etc]

[Brief description of categories of individuals, how the information is collected and stored, and need]

## 12.0 REFERENCES

- (a) Section 552a of title 5, United States Code (also known as “the Privacy Act” as amended)
- (b) Section 3501, et seq. of title 44, United States Code, Note (Public Law 107-347, Section 208 “Privacy Provisions,” E-Government Act of 2002)
- (c) Department of Defense Directive 5400.11, “DoD Privacy Program,” October 29, 2014
- (d) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (e) Administrative Instruction 81, “OSD/Joint Staff (JS) Privacy Program,” November 20, 2009
- (f) DoD 7750.07-M, “DoD Forms Management Procedures Manual,” August 14, 2012
- (g) DoD Instruction 8910.01, “Information Collection and Reporting,” May 19, 2014
- (h) Chapter 35 title 44 United States Code (also known as the “Paperwork Reduction Act of 1995”)
- (i) DoD Instruction 5400.16, “DoD Privacy Impact Assessment Guidance,” February 12, 2009
- (j) “DoD Forms Management Program,” <http://www.dtic.mil/whs/directives/forms/index.htm>.
- (k) DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use within DoD,” August 1, 2012
- (l) DoD Directive 5015.2, “DoD Records Management Program,” March 6, 2000
- (m) Section 1236 of title 36, Code of Federal Regulations
- (n) Administrative Instruction 15, “OSD Records and Information Management Program,” May 3, 2013
- (o) Office of Management and Budget Memorandum, “Information Collection under the Paperwork Reduction Act,” April 7, 2010
- (p) Office of Secretary of Defense Memorandum 13798-10, “Social Security Numbers Exposed on Public Facing and Open Government Websites,” November 23, 2010
- (q) Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules,” May 25, 2001
- (r) Section 3541, et seq. of title 44, United States Code (also known as the “Federal Information Security Management Act of 2002”)
- (s) Office of Management and Budget Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 22, 2007
- (t) Director, Administration and Management Memorandum, “Use of Best Judgment for Individual Personally Identifiable Information Breach Notification Determinations,” August 2, 2012