

# Privacy Program



## Defense Human Resources Activity

April 28, 2014

## Table of Contents

0.0	PREFACE .....	3
1.0	PURPOSE .....	4
2.0	SCOPE .....	4
3.0	RESPONSIBILITIES .....	4
4.0	PERSONALLY IDENTIFIABLE INFORMATION .....	6
5.0	REQUIREMENTS FOR COLLECTING PERSONALLY IDENTIFIABLE INFORMATION.....	6
5.1	System of Records Notice.....	6
5.2	Privacy Act Statement.....	8
5.3	Privacy Impact Assessment .....	8
5.4	Collecting Social Security Numbers.....	10
6.0	SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION .....	11
6.1	Paper Documents .....	11
6.2	Electronic Files .....	11
7.0	RETENTION, MAINTENANCE, AND DISPOSAL OF PERSONALLY IDENTIFIABLE INFORMATION .....	13
8.0	PII BREACH REPORTING AND INCIDENT RESPONSE .....	13
8.1	Reporting Procedures.....	13
8.2	Penalties .....	15
9.0	TRAINING .....	15
10.0	REFERENCES .....	17
11.0	ACRONYMS.....	18

## PREFACE

This document establishes the Defense Human Resources Activity (DHRA) Headquarters (HQ) Privacy Office and delineates guidance to all 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 Privacy Act of 1974, as amended, 552a of Title 10, United States Code (Reference (a))
- Office of Management and Budget Circular No. A-130 Revised, “Management of Federal Information Resources” (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 April 28, 2014 document will be issued periodically by the DHRA HQ Privacy Office to reflect changes to policy, procedures, or responsibilities. A complete list of all revisions will be issued with each new change to ensure all documents are kept current. Changes are entered in the document and recorded in the Table below.

### Record of Changes

Change Number	Date of Change	Section	Description of Change
Version			

  
**Sharon H. Cooper**  
**Director**

## **1.0 PURPOSE**

This policy establishes the Defense Human Resources Activity (DHRA) Headquarters (HQ) Privacy Office and provides guidance to DHRA Components regarding collecting, safeguarding, maintaining, storing, and sharing Personally Identifiable Information (PII). The DHRA HQ Privacy Office will disseminate guidance to the Field Activity and oversee the implementation of statutory law, Federal standards, and Department of Defense (DoD) policy.

## **2.0 SCOPE**

This policy provides guidelines to ensure Field Activity compliance and management of all Privacy related items, specifically as they relate to:

- Collection and use of PII
- Social Security Number (SSN) Use Reduction
- Safeguarding PII
- Maintenance and Disposal of PII
- PII Breach Reporting and Incident Response
- Training and Reporting Requirements

## **3.0 RESPONSIBILITIES**

DHRA HQ Privacy Office. The DHRA HQ Privacy Office, through the Director, DHRA, will:

- Establish policy for collecting, safeguarding, maintenance, storing, and sharing of PII.
- Disseminate guidance to the Field Activity and oversee the implementation of statutory law, Federal standards, and DoD policy in accordance with the noted References.
- Review all Component-level Privacy Impact Assessments (PIA), Systems of Records Notices (SORNs), SSN Justification Memorandums, forms, and PII breaches, unless otherwise designated to the Component.
- 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 Office (DPCLC), as necessary.
- Hold quarterly meetings with Component Privacy Officials to ensure compliance with all facets of this policy and as necessary.
- Work in conjunction with the Personnel and Readiness (P&R) Records Manager to ensure documents containing PII are kept in accordance with the established retention schedule.

DHRA Component Directors. DHRA Component Directors will establish processes that comply with the requirements of this policy and will:

- Ensure all information collections have completed PIAs, SORNs and records disposition schedules.
- Review all SORNs biennially and provide results to the DHRA HQ Privacy Office.
- Reduce the use of the SSN to the greatest extent practicable.
- Ensure all personnel are compliant with annual training requirements.
- Designate a Component Privacy Official(s) who is responsible for attending quarterly meetings and complying with and executing the responsibilities of this policy.
- Report all potential PII incidents and make notifications to affected person(s), as directed by the Director, DHRA in the event of a breach.

DHRA Chief Management Officer (CMO)/Chief Information Officer (CIO). The DHRA CMO/CIO will:

- Manage the overall compliance of all DHRA systems and ensure that privacy requirements are evaluated through the certification and accreditation process and proper portfolio management.
- Serve as the DHRA CIO and Senior Information Security Official and review all Component PIAs and other necessary requirements.
- Coordinate Privacy related process changes with the Director, DHRA as necessary.

Component Privacy Officials. The designated Component Privacy Official will:

- Attend DHRA quarterly privacy meetings, or as required.
- Ensure all government and contractor personnel have completed required training and report quarterly to the DHRA HQ Privacy Office.
- Coordinate with the DHRA HQ Privacy Office when responding to PII breach reports.
- Coordinate with Component program managers, information assurance managers (IAMs), and records managers to produce and review PIAs and SORNs to ensure information system compliance.
- Ensure all new and old systems are compliant with DoD Records Management and records disposition requirements and ensure records containing PII are not kept longer than required.

Component Program Managers. The designated Component Program Manager will:

- 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.

#### **4.0 PERSONALLY IDENTIFIABLE INFORMATION**

PII is information that identifies, links, relates, is unique to, or describes the individual, such as name, SSN, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information, or any other PII which is linked or linkable to a specified individual. This definition of PII is not anchored to any single category of information or technology. Non-PII can become PII when information is publically available and when combined with other elements to positively identify an individual. When PII is considered to be compromised, the responsible Component will be required to follow the PII breach reporting procedures as outlined in section 8.0.

#### **5.0 REQUIREMENTS FOR COLLECTING PERSONALLY IDENTIFIABLE INFORMATION**

The collection and storage of PII is regulated by statutory law, Federal standards, and DoD policy. When an individual is requested to provide PII for collection, all DHRA Components must ensure that their collections are compliant with the procedures described in subsections 5.1- 5.4.

##### **5.1 System of Records Notice**

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. The SORN defines the rules for collecting, using, storing, sharing, and safeguarding personal data when records are retrievable by a personal identifier.

All SORNS must be published in the Federal Register for a 30-day period to notify the public of the data elements being collected, the purpose of the collection, the authority for the information collection, and 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 DPCLC website at: <http://dpclc.defense.gov/Privacy/SORNs.aspx>. If an employee has questions regarding SORNs, the individual may contact the DHRA HQ Privacy Official or their Component Privacy Official.

### **5.1.1 Developing a System of Records Notice**

The Component Privacy Official or program manager should take the following steps when developing a new SORN:

1. Component Privacy Official submits draft SORN to DHRA HQ Privacy Official.
2. The DHRA HQ Privacy Office will work with the Component Privacy Official to review and edit the SORN, as necessary, and assist with submission to the Office of Under Secretary of Defense (OUSD) P&R / DHRA Records Management Officer to be processed for a records disposition and retention schedule. Once all edits have been adjudicated, the DHRA HQ Privacy Office submits the SORN to the OSD/JS Privacy Office.
3. The Component Privacy Official responds to any questions from OSD/JS and updates the SORN with assistance from the DHRA HQ Privacy Office as necessary.
4. The OSD/JS Privacy Office forwards the SORN to DPCLC for review. Upon DPCLC approval the SORN will be submitted to the Federal Register by Washington Headquarters Service (WHS) for the required 30-day comment period.
5. Once the SORN is finalized, the OSD/JS Privacy Office notifies the DHRA HQ Privacy Office.

### **5.1.2 Requesting an Office of Management and Budget Control Number**

In accordance with the Paperwork Reduction Act and updated guidance released in the Office of Management and Budget (OMB) memorandum, "Information Collection under the Paperwork Reduction Act" (Reference (f)), before requesting information from members of the public, Federal agencies are required to seek public comment on proposed collections and to submit proposed collections for review and OMB approval. 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 OUSD(P&R) Information Management Control Officer (IMCO) to submit the information collection request to WHS. The Component Privacy Official should follow the instructions available at: <http://www.dtic.mil/whs/directives/infomgt/collections/index.htm>, when processing a collection. The Component Privacy Official will need to prepare and submit the following documents through the OUSD(P&R) IMCO, who will then submit the documents through WHS to OMB for approval:

1. OMB Form 83-I
2. Supporting Statement
3. 30-day Federal Register Notice
4. Copy of current SORN
5. Copy of current PIA

6. Applicable screenshots of system and collection or copies of currently approved or draft official form(s)

### **5.1.3 Biennial Review of a Current System of Records Notice**

Each Component is required to review their SORNs biennially. Component Privacy Officials are responsible for initiating and completing their biennial reviews on time. The DHRA HQ Privacy Office will notify each Component Privacy Official regarding the required biennial reviews based on the established Federal Register publication date or the recertification date, if not initiated by the Component. The Component Privacy Official will follow the steps in subsection 5.1.1 when completing a biennial review.

### **5.1.4 Discontinuing a System**

If it is determined that a system should be discontinued or combined into another system and the SORN is no longer relevant, a deletion notice for that system is required. A new SORN should be submitted when combining into another system. When deleting, the Component Privacy Official must verify why the SORN is no longer required and whether records continue to exist or if the records may be destroyed in accordance with the established National Archives Records Administration (NARA) records disposition schedule. To discontinue a system, the Component Privacy Official shall 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 fulfilled. The Component Privacy Official may essentially follow the steps in subsection 5.1.1 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.

## **5.2 Privacy Act Statement**

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 Privacy Act Statement (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 an SSN is 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 by 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 Reference (d). The PAS will be

reviewed as part of the SORN and PIA approval process. If a Component Privacy Official has a question regarding completing a PAS, they should contact the DHRA HQ Privacy Official.

### **5.3 Privacy Impact Assessment**

Section 208 of Public Law 107-347, “E-Government Act of 2002” (Reference (g)) requires all Federal government agencies to conduct a PIA for all new or substantially changed information technology (IT) systems that collect, maintain, or disseminate PII from members of the public. A PIA allows for the evaluation and mitigation of possible privacy risks throughout the lifecycle of a program or system.

In accordance with Reference (g) and DoD Instruction (DoDI) 5400.16 “DoD Privacy Impact Assessment Guidance” (Reference (h)), systems owners and privacy officials will ensure the completion of a PIA for every IT system containing PII under their responsibility, including any localized data collection (e.g., local websites, limited use applications). PIAs are required when PII is collected, maintained, used, or disseminated in electronic forms on members of the public, Federal personnel, contractors or foreign national employees. All completed PIAs shall be reviewed 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.

#### **5.3.1 Developing a Privacy Impact Assessment**

Every IT initiative will, at a minimum, have completed section 1 of DD Form 2930, “Privacy Impact Assessment (PIA),” available at: <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3438.html> which is used to determine if the system processes PII. If it is determined that a PIA is not required, the Component Privacy Official, Program Manager, or other designee, must maintain a copy of the DD Form 2930 locally and no further steps will be required. If the information system does process PII, the Component Privacy Official should take the following steps, while working with the IAM as necessary, when developing the PIA:

1. Submit a version of the draft PIA to the DHRA HQ Privacy Official.
2. DHRA HQ Privacy Office will work with the Component Privacy Official to review and edit as necessary. Once all edits have been adjudicated, the DHRA-HQ Privacy Office submits the PIA to the OSD/JS Privacy Office and the DHRA CIO for review.
3. The Component Privacy Official responds to any questions from OSD/JS or the DHRA CIO 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, the DHRA HQ Privacy Official, the OSD/JS Privacy Official, the DHRA Senior Information Assurance Official, and the DHRA CIO.

5. The DHRA HQ Privacy Office will post sections 1 and 2 of all Component PIAs at <http://www.dhra.mil/website/headquarters/info/pia.shtml>. If a Component currently posts PIAs to their website, a link will be provided to that page from the DHRA Privacy website, if a Component link changes they should notify the DHRA HQ Privacy Office. If it is determined by the Component Privacy Official / DHRA HQ Privacy Office 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 concern, the PIA will not be posted and will be maintained by the Component.
6. Once posted online, the DHRA HQ Privacy Official 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.

#### **5.4 Collecting Social Security Numbers**

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 his/her SSN unless a statute, executive order, regulation, policy or other legal authority requires that the SSN be furnished, as further mentioned in Reference (d). In accordance with DoDI 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD" (Reference (i)), use of the SSN should be eliminated or reduced whenever possible and the SSN should be replaced with another identifier (e.g., DoD ID number). When requesting, collecting, transmitting, or maintaining an individual's SSN, the responsible official shall:

- Ensure the collection is compliant with all associated requirements (e.g., SORN, PIA, PAS, records retention schedule, OMB license).
- Ensure the collection is compliant with Reference (i), and falls under the purview of one of the 13 acceptable uses for SSN collection.
- Ensure the SSN is properly protected.
- Complete an SSN Justification Memorandum for all forms and IT systems that collect the SSN in accordance with Reference (i).
- Complete an SSN Elimination Plan for any use of the SSN that cannot be justified through appropriate authorities in accordance with Reference (i). If the justification for the use of the SSN falls under the legacy use case and is not specifically required by law, reference shall be made to a Plan of Actions and Milestones for the elimination of the use of the SSN.

- Submit the SSN Justification Memorandum and Elimination Plan for review, when applicable, to the DHRA HQ Privacy Official, who will then coordinate with the OSD/JS prior to being submitted to DPCLCLO.
- Review the SSN Justification Memorandum biennially. Component Privacy Officials are responsible for initiating and completing their biennial reviews on time.

## **6.0 SAFEGUARDING PII**

Properly safeguarding PII is critical to reducing the possibility of a loss or compromise of sensitive information. PII shall 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 8.0. All PII should be handled using current information assurance (IA) and records management policies and procedures in accordance with DoDI 8500.01, “Cybersecurity,” (Reference (j)).

### **6.1 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 will be taken:

- Use a DD Form 2923, “Privacy Act Data Cover Sheet,” available at: <http://www.dtic.mil/whs/directives/infomgt/forms/efoms/dd2923.pdf>.
- Ensure PII is directly provided to individuals with an official need to know.
- Ensure control of the document and limit access to the document during the course of the day.
- Ensure all PII is placed securely out of sight at the end of each day.
- Ensure proper disposal of PII, in accordance with the guidelines provided in Section 7.0.

### **6.2 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 protections will be taken:

- At a minimum PII will be password protected (e.g., if compiled on a compact-disc, or in a ZIP-file that cannot be encrypted).
- Ensure PII is only accessible to individuals with an official need to know.

- Only maintain PII on U.S. Government furnished or approved equipment.

### **6.2.1 Websites**

OSD Memorandum 13798-10, “Social Security Numbers Exposed on Public Facing and Open Government Websites” (Reference (k)) mandates full and partial SSNs not be posted on any public facing or open government website in any form. 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)).
- Limited to those individuals with an official need to know.

### **6.2.2 Email**

The most common breach of PII occurs via email, when an SSN 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 will be taken:

- Digitally sign and encrypt 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.

### **6.2.3 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, in accordance with the Cryptographic Module Validation Program as specified in Federal Information Processing Standards Publication 140-2, “Security Requirements for Cryptographic Modules” (Reference (l)). 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).

## **7.0 RETENTION, MAINTENANCE, AND DISPOSAL OF PERSONALLY IDENTIFIABLE INFORMATION**

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 (m)).

When developing a system of records, the Component Privacy Official, Program Manager, or designee, will request a records retention schedule from the DHRA Records Management Officer as part of the system creation process. Component Privacy Officials should be familiar with Administrative Instruction 15, “OSD Records and Information Management Program” (Reference (n)). Title 36 Code of Federal Regulations section 1236 (Reference (o)) requires both paper and electronic systems or applications to have a NARA approved records disposition schedule to ensure records created, maintained or stored in an electronic format are not kept longer than required. The Component Privacy Official will work with the DHRA Records Management Officer and the WHS Records Manager to request the retention and disposition schedule from NARA. Further information regarding records management is available at: <http://www.dtic.mil/whs/esd/rdd/recordsmgt.html>.

Proper disposal of PII is any means of destruction that renders documents or records, physical and electronic, unrecognizable and beyond reconstruction (e.g., burning, melting, chemical decomposition, pulping, pulverizing, shredding, mutilation, degaussing, striping) in accordance with Reference (d).

## **8.0 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, the wrong DoD recipient, or when individuals have access to PII without an official need to know.

Federal reporting requirements established by the Federal Information System Management Act of 2002 and updated procedures established in OMB Memorandum 07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” (Reference (p)) require incidents involving PII to be reported to the Federal incident response center, United States Computer Emergency Readiness Team, (US-CERT) within one hour of discovery. If an individual suspects a PII breach has occurred, he/she should follow the reporting procedures in subsection 8.1.

### **8.1 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,” available at: <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2959.pdf>. The DD Form 2959 will be used by the DHRA HQ Privacy Office to report and analyze the breach or suspected breach and document notification to US-CERT, or the individual, and 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 (q)). All Component Privacy Officials or responsible designees should comply with the following procedures when reporting a breach of PII:

- 1) The individual discovers a PII incident and coordinates with their Component Privacy Official to submit the DD Form 2959 by email to the DHRA HQ Privacy Official immediately upon discovering the incident.
- 2) The DHRA HQ Privacy Office reviews the DD Form 2959 and coordinates with DHRA Office of General Counsel (OGC) and the OSD/JS Privacy Office as necessary. The DHRA HQ Privacy Office will provide next steps to the Component Privacy Official.
  - a. If the DHRA HQ Privacy Office determines that notifying US CERT is unnecessary based on the Component recommendations, the reporting Component Privacy Official, or responsible designee, 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 Privacy Official.
  - b. If no further actions are requested by the DHRA HQ Privacy Office, the incident will be closed.
- 3) If the DHRA-HQ Privacy Office determines that notifying US CERT is necessary, then the Component Privacy Official, or responsible designee, must report the breach within one hour to the US-CERT by filling out the form at their website: <https://forms.us-cert.gov/report/>.
- 4) The responsible Component Privacy Official conducts a PII breach investigation, as advised by the DHRA HQ Privacy Office. The DD Form 2959 should be updated with the US-CERT number and any new information discovered and provided to the DHRA HQ Privacy Official. The DHRA HQ Privacy Official will notify the OSD/JS Privacy Office within 24 hours in order to provide notification to DPCLC within 48 hours.
- 5) The Component Privacy Official submits a recommendation to the DHRA HQ Privacy Office regarding the need to notify the affected individual(s). The recommendation should be based on the five factors to assess harm, in accordance with Reference (q):
  - a. Nature of the data elements breached;
  - b. Number of individuals affected (not necessarily a factor in determining whether to notify but may affect how notification is delivered);
  - c. Likelihood the information is accessible and usable;
  - d. Likelihood the breach may lead to harm; and,

- e. Ability of the Department to mitigate the risk of harm.
- 6) Based on the Component Privacy Official's investigation of the incident, the DHRA HQ Privacy Office will notify the Component Privacy Official whether notification to the affected person(s) is required.
    - a. If notification is not required, the Component Privacy Official updates section 2.b. of the DD Form 2959, to include all actions taken and lessons learned from the incident, and submits the form to the DHRA HQ Privacy Official.
    - b. If no further actions are requested by the DHRA HQ Privacy Office, the incident will be closed.
  - 7) If the Director, DHRA, determines notification to the affected person(s) is required, the Component Privacy Official will provide a notification plan to the DHRA HQ Privacy Office. The notification plan should include a template of the notification, anticipated notification date, and method of notification. All applicable parties should be notified within ten days of the breach. This timeline may vary based on the severity of the breach. In certain cases credit monitoring may be offered at the determination and cost of the Component, or a determination made by the Director, DHRA.
  - 8) The Component Privacy Official updates section 2.b. of the DD Form 2959, to include all actions taken and lessons learned from the breach, and submits the form to the DHRA HQ Privacy Official. If no further actions are requested by the DHRA HQ Privacy Office the incident will be closed.

## **8.2 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 and fines in accordance with Reference (a). Any administrative actions taken should be coordinated with DHRA OGC.

## **9.0 TRAINING**

All new federal employees and contractors are required to take Privacy Act/PII training and IA training prior to gaining access to the DoD network. All employees and contractors are required to refresh this training annually. Privacy Act/PII training and IA training are available at the following sites:

- DoD Privacy Act/PII training: <http://iase.disa.mil/eta/piiv2/launchpage.htm>
- DoD IA Awareness: <http://iase.disa.mil/eta/>

All DHRA Components are responsible for reaching 100% compliance with these training requirements by the end of each Fiscal Year. Privacy Officials will be responsible for reporting training compliance to the DHRA HQ Privacy Office quarterly, or as requested. The

DHRA HQ Privacy Office will be responsible for consolidating all requirements and providing them to the OSD/JS Privacy Office. Designated Component Privacy Officials may be required to take additional privacy training, as determined by the DHRA HQ Privacy Office, with consensus of the other Component Privacy Officials at the beginning of each fiscal year.

## 10.0 REFERENCES

- (a) Section 552a of title 5, United States Code
- (b) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 28, 2000
- (c) Department of Defense Directive 5400.11, "DoD Privacy Program," May 8, 2007
- (d) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
- (e) Administrative Instruction 81, "OSD/Joint Staff (JS) Privacy Program," November 20, 2009
- (f) Office of Management and Budget Memorandum, "Information Collection under the Paperwork Reduction Act," April 7, 2010
- (g) Section 208 of Public Law 107-347, "E-Government Act of 2002," December 17, 2002
- (h) DoD Instruction 5400.16, "DoD Privacy Impact Assessment Guidance," February 12, 2009
- (i) DoD Instruction 1000.30, "Reduction of SSN Use within DoD," August 1, 2012
- (j) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014.
- (k) Office of Secretary of Defense Memorandum 13798-10, "Social Security Numbers Exposed on Public Facing and Open Government Websites," November 23, 2010
- (l) Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001
- (m) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (n) Administrative Instruction 15, "OSD Records and Information Management Program," May 3, 2013
- (o) Section 1236 of title 36, Code of Federal Regulations
- (p) Office of Management and Budget Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007
- (q) Director, Administration and Management Memorandum, "Use of Best Judgment for Individual Personally Identifiable Information Breach Notification Determinations," August 2, 2012

## 11.0 ACRONYMS

CIO	Chief Information Officer
CMO	Chief Management Officer
DHRA	Defense Human Resources Activity
DPCLO	Defense Privacy and Civil Liberties Office
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