

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Personnel Security Breach Notification and Mitigation Services Records

2. DOD COMPONENT NAME:

Department of Defense Human Resources Activity

3. PIA APPROVAL DATE:

Defense Manpower Data Center

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- ☐ From members of the general public ☐ From Federal employees
- ☒ from both members of the general public and Federal employees ☐ Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one.)

- ☐ New DoD Information System ☐ New Electronic Collection
- ☒ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To provide breach notification and facilitate the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases. DoD will also use the data to respond to breach verification inquiries received from individuals using the link on OPM's website that redirects individuals to a DoD website where they can enter their information to find out if they have been affected by this breach. These records may also be used for tracking, reporting, measuring, and improving the Department's effectiveness in implementing this data breach notification.

Types of personal information being collected are last, first, and middle name, Social Security Number (SSN), date of birth, place of birth, citizenship status, country of citizenship, home and/or business addresses, phone numbers, and e-mail addresses.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII is collected for verification and identification purposes in order to appropriately notify individuals that were affected by the OPM Breach.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individual's are informed that providing the information is voluntary. This voluntary disclosure is given on the SF-85, 85P, Questionnaire for Position of Public Trust; SF-86, Questionnaire for National Security Position; as well as the website where individuals can enter their information to find out if they have been affected by this breach.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Yes. By signing and/or submitting the SF-85, SF-85P, SF-86 or information to the website, individuals are consenting to the specific uses identified in the Privacy Act Statement and System of Records Notice.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- ☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

AUTHORITY: The E-Government Act of 2002 (Pub. L. No. 107-347); the Federal Information Security Modernization Act of 2014 (Pub.

L. No. 113-283) (44 U.S.C. 3551-3559); 10 U.S.C. 113, Secretary of Defense; 50 U.S.C. 3038, Responsibilities of Secretary of Defense Pertaining to National Intelligence Program; E.O. 12333, United States Intelligence Activities, as amended; E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft, as amended; E.O. 13526, Classified National Security Information; White House Memorandum dated September 20, 2006, Subject: Recommendations for Identity Theft Related Data Breach Notification; and E.O. 9397 (SSN), as amended.

PURPOSE: To provide breach notification and facilitate the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases. DoD will also use the information to respond to breach verification inquiries received from individuals using this DoD website. These records may be used for tracking, reporting, measuring and improving the Department's effectiveness in implementing this data breach notification.

ROUTINE USE: In addition to disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD to commercial entities for address verification purposes. Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, Disclosure to the Office of Personnel Management Routine Use, Counterintelligence Purpose Routine Use and Data Breach Remediation Purposes Routine Use. 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 may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>

DISCLOSURE: Voluntary. However, failure to provide requested information may prevent or delay DoD's ability to verify and/or notify an individual affected by the breach of information in the OPM background investigation database.

This Privacy Act Statement is currently under legal review

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?

(Check all that apply)

☐ Within the DoD Component

Specify.

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify.

☒ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify.

Office of Personnel Management, National Background Investigation Bureau

☐ State and Local Agencies

Specify.

☐ Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Specify.

☒ Other (e.g., commercial providers, colleges).

Specify.

Commercial entities under contract with DoD for the sole purpose of verifying addresses of affected individuals for notification purposes.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☒ Individuals

☐ Databases

☐ Existing DoD Information Systems

☐ Commercial Systems

☒ Other Federal Information Systems

Source of information includes: the Individual; the Office of Personnel Management; Employee address information from Federal employers (e.g. OPM, Defense Finance and Accounting Service, Defense Manpower Data Center, Department of State, U.S. Postal Service, Library of Congress, General Accountability Office, Death master files, Executive Office of the President, Former President's Office, etc); and address verification from cleared contractors and commercial vendors.

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

☐ E-mail

☐ Official Form (Enter Form Number(s) in the box below)

☐ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☒ Information Sharing - System to System

☒ Website/E-Form

☐ Other (If Other, enter the information in the box below)

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

I. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

TEMPORARY. Cut off upon completion of mitigation services, destroy 3 years after cut off.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII.
(If multiple authorities are cited, provide all that apply).

- (a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.
(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

The E-Government Act of 2002 (Pub. L. No. 107-347); the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) (44 U.S.C. 3551-3559); 10 U.S.C. 113, Secretary of Defense; 50 U.S.C. 3038, Responsibilities of Secretary of Defense Pertaining to National Intelligence Program; E.O. 12333, United States Intelligence Activities, as amended; E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft, as amended; E.O. 13526, Classified National Security Information; White House Memorandum dated September 20, 2006, Subject: Recommendations for Identity Theft Related Data Breach Notification; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ Yes ☐ No ☐ Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0545 , Collection of Required Data Elements to Verify Eligibility, expires on February 28, 2026