

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:

Human Resources Information Systems

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

01/12/22

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.

Human Resources Information Systems (HRIS) provide organizations, Defense Finance and Accounting Service (DFAS) senior management, DFAS employees and the human resource (HR) community with access to the business intelligence needed to make strategic human capital decisions. HRIS is comprised of Human Resources Business Intelligence Datamart (HRBID), Request for Personnel Actions (RPA) Builder/Tracker, Electronic Data Interchange Person Identifier (EDIPI) system, Personnel Accountability Tracker (PAT), Employee Voluntary Early Retirement Authority/Voluntary Separation Incentive Pay (eVERA/VSIP), Learning Management System (LMS), and Cognos Business Intelligence (BI).

The HRBID uses Personally Identifiable Information (PII) data collected strictly for data matching while allowing users, with a validated need to know, the ability to run standard reports and ad-hoc queries against the HRBID data via the web. HRIS maintains this information for potential audit purposes and destroys it when no longer needed. The LMS system allows authorized users the capability to manage their learning and development activities while the Equal Employment Opportunity (EEO) reports require the use of demographics. The RPA application gives authorized DFAS users the ability to initiate and manage requests for personnel actions. Applications throughout DFAS use EDIPI to uniquely and unambiguously identify Department of Defense (DoD) personnel, including agency information, while reducing the use of the Social Security Number (SSN). PAT is a tool that helps track the status of all DFAS employees in the event of a planned exercise, a real world event, or natural disaster. The eVERA/VSIP application contains employee retirement and separation data. DFAS may use this system to restructure the workforce to meet mission objectives without reducing the overall number of personnel. Cognos BI is a web-based application that renders reports and allow users to create ad-hoc queries on data. The HRBID database feeds the Cognos-HRBID database. The HRIS applications collect PII data from the Defense Civilian Personnel Data System (DCPDS) and feed it into the HRIS applications and vice versa.

PII elements within HRIS include birth date, citizenship, disability information, DoD identification (ID) number, education information, employment information, financial information, gender/gender identification, home/cell phone, legal status, mailing/home address, marital status, military records, name(s), official duty address, official duty telephone phone, other ID number, personal e-mail address, position/title, race/ethnicity, rank/grade, records, security information, SSN, and work e-mail address.

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)

Data matching, verification, identification, administrative use, and reporting.

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.

HRIS applications do not collect PII directly from individuals; however supervisors and representatives enter PII data into RPA for employment status and capturing onboarding information. DCPDS, the system of record, receives the data.

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.

HRIS applications do not collect PII directly from the individual; however, DCPDS, the system of record, receives this information from RPA for onboarding.

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

THIS SYSTEM CONTAINS PRIVACY ACT DATA

AUTHORITY: EXECUTIVE ORDER 10450, 9397, AND PUBLIC LAW 99-474, THE COMPUTER FRAUD AND ABUSE ACT
PURPOSE OF USE: TO RECORD NAMES AND SOCIAL SECURITY NUMBERS FOR THE PURPOSE OF VALIDATING THE TRUSTWORTHINESS OF INDIVIDUALS REQUESTING ACCESS TO DEPARTMENT OF DEFENSE (DOD) SYSTEMS AND INFORMATION.

ROUTINE USES: THOSE GENERALLY PERMITTED UNDER THE 5 UNITED STATES CODE 522A(B) OF THE PRIVACY ACT AS REQUIRED.

DISCLOSURE: DISCLOSURE OF THIS INFORMATION IS VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THE REQUESTED INFORMATION MAY IMPEDE, DELAY OR PREVENT FURTHER PROCESSING OF THIS REQUEST.

NOTE: RECORDS MAY BE MAINTAINED IN BOTH ELECTRONIC AND/OR PAPER FORM.

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.

DFAS - Payroll Services and DFAS - HR Innovation and Information Solutions Directorate (ISSD).
--
- Other DoD Components (i.e. Army, Navy, Air Force) Specify.

Civilian pay officials in the Office of the Under Secretary of Defense and Defense Manpower Data Center.
--
- Other Federal Agencies (i.e. Veteran's Affairs, Energy, State) Specify.

--
- 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.

--

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

DCPDS provides PII data.

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.

Cutoff at the end of fiscal year. Destroy 10 years after cutoff.

AUTH: (N1-507-93-2, Item 12) (1400/R1)

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.

Executive Order (E.O.) 9397 as amended authorizes solicitation and use of the SSN as a numerical identifier for federal personnel identified in most federal record systems; E.O. 12862, dated September 11, 1993, concerning customer service; and DoD Financial Management Regulation 7000.14-R, Volume 5, Chapter 20.

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.

An Office of Management and Budget (OMB) control number is not required because the HRIS applications do not collect data from the public.