PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Human Resources Information Systems (HRIS)

DoD Component Name:

Defense Finance and Accounting Service

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel * and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ New DoD Information System ☐ New Electronic Collection

☐ Existing DoD Information System ☒ Existing Electronic Collection

☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐ Yes, DITPR Enter DITPR System Identification Number

☐ Yes, SIPRNET Enter SIPRNET Identification Number

☒ No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ Yes Enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☒ No

d. Does the DoD information system or electronic collection have 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 should be consistent.

☐ Yes Enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at:
http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

☒ No

e. Does this DoD information system or electronic collection have an 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

Enter OMB Control Number

Enter Expiration Date

☒ No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

Executive Order 9397 authorizes solicitation and use of SSNs as a numerical identifier for Federal personnel that are identified in most Federal record systems; Executive Order 12862, dated September 11, 1993, concerning customer service; 5 USC Section 301, Departmental Regulations; and DoD Financial Management Regulation 7000.14-R, Volume 5, Chapter 20

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

HRIS provide organizations, DFAS Senior Management, DFAS employees and the HR community with access to the business intelligence needed to make strategic human capital decisions. HRIS is comprised of Human Resources Business Intelligence Dashboard (HRBID), Resumix Warehouse, Request for Personnel Actions (RPA) Builder, RPA Tracker, Electronic Data Interchange Person Identifier (EDIPI) system and Learning Management System (LMS).

HRBID personally identifiable information (PII) data collected is used strictly for data matching while allowing users who have a validated need to know ability to run standard reports and ad hoc queries against the HRBID data via the web. PII elements within HRBID include Pern number for the employee, employee name, address, employment information, business email, home phone number, office phone number, and spouse information.

Resumix Warehouse maintains the resume data from the decommissioned DISA server utilized to hire from Resumix and Delegated Examining Unit (DEU) registers. The DISA server was decommissioned in mid March 2011 and data is to be maintained in HRIS until 2013. This information is to be maintained for potential audit purposes only and is no longer collected. PII data consists of SSN, citizenship, mailing/home address, home phone number, demographics, employment information, education information, gender, personnel email address, military records, and race/ethnicity.

The LMS module allows authorized users the capability to manage their learning and development activities while the Equal Employment Reports (EEO) reports require the use of demographics PII information such as: age, race/national, employee name, home address and employment information.

RPA application gives authorized DFAS users the ability to initiate and manage requests for personnel actions. The RPA module gathers PII information (employee name, employment information) to track and report the progress of personnel actions.

EDIPI is used by applications throughout DFAS to uniquely and unambiguously identify DoD personnel, including agency information. PII information collected by EDIPI is person's name, social security number, service, rank, pay plan, work email, date of birth, and government agency code.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The result of mishandling personal data may lead to lost, stolen or compromised PII which could be harmful to the individual in many ways (e.g., identify theft, damage to the individual's reputation and /or financial hardship). Such incidents could also cast DFAS in an unfavorable light to the public. Hence, access is limited to persons authorized to service or to use the system in performance of their official duties (requires screening and approval for need to know). DFAS adheres to physical protections of PII as described in accordance with DFAS 5200.1-R. IA policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include PII, Sor all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8500.1."

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.** Specify

DFAS – Corporate Systems, DFAS – eSolutions, DFAS- HR Information Systems and Services Division (ISSD)

☒ **Other DoD Components.** Specify

Civilian pay officials in the Office of the Under Secretary of Defense, Defense Manpower Data Center

☐ **Other Federal Agencies.** Specify

☐ **State and Local Agencies.** Specify

☐ **Contractor** (enter name and describe the language in the contract that safeguards PII.) Specify

☐ **Other** (e.g., commercial providers, colleges). Specify

i. 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.

HR Information System does not collect PII directly from the individual.

j. 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.

HR Information System does not collect PII directly from the individual.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement

☐ Privacy Advisory

☐ Other

☒ None

Describe each applicable format.

HR Information System does not collect PII directly from the individual.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.