PRIVACY IMPACT ASSESSMENT (PIA)

For the

IPPS-A INC 2 - INTEGRATED PERSONNEL AND PAY SYSTEM - ARMY INCREMENT 2

HQDA G1 - PEO EIS PD IPPS-A

U.S. Army Program Executive Office (PEO) Enterprise Information Systems (EIS)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate 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) why 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: 16188 DA302337
- ☐ **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**
- ☐ **No**

If "Yes," enter UPI 007-000000599

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

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0600-8a PEO EIS

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.

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 provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute 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.

10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 37 U.S.C., Pay and Allowances of the Uniformed Services; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness USD (P&R); and E.O. 9397 (SSN), as amended.

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.

To provide Soldiers, Commanders, and HR professionals an integrated HR and pay system to support personal management activities for all components. IPPS-A will streamline Army Human Resources (HR), enhancing the efficiency and accuracy of Army personnel and pay procedures. IPPS-A will be a web-based tool, available 24 hours a day, and accessible to the Soldiers, HR professionals, Combatant Commanders, personnel and pay managers, and other authorized users throughout the Army. IPPS-A will provide each Soldier with a single personnel record and a self-service capability allowing the Soldier to update selected personal information. Personally Identifiable Information (PII) data collected will include military, employment, financial, educational, personal, law enforcement, medical, and beneficiary information.

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

IPPS-A will be accredited under the Risk Management Framework (RMF) and the Confidentiality, Integrity, and Availability (CIA) levels have been determined to be Moderate/Moderate/Moderate. PII requirements that serve as the foundation for IPPS-A privacy practices are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Appendix J, and DoDD 5400.11, dated October 29, 2014. Additional security controls specific to PII are defined within the enterprise Mission Assurance Support Service (eMASS) tool via the Privacy overlay.

The Program Management Support Contractor, Booz Allen Hamilton, and the System Integrator contractor, CACI International Inc, have access to the system for the purpose of establishing a functional baseline. Once the system is fielded, access will be reviewed and restricted to only those personnel who require access for purposes of maintenance and emergency response. Both contracts contain language which reference the requirements to protect PII. Contractors working on the project are required to sign Non-Disclosure Agreements (NDA), Privileged-Level Access Agreements (PAA) and Acceptable Use Policy (AUP) documents.

All IPPS-A personnel that utilize PII will be required to complete PII handling and protection awareness training, and sign consent forms to acknowledge user responsibilities for protecting data. IPPS-A will also have an auditing process to track the actions of any user with privileged access.

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. Army Audit Agency, Army Human Resources, All Army Major Commands, the Army Installation Management Command, Army Recruiting Command, Army National Guard, U.S. Army Reserves, Department of Army Inspector General, Department of the Army Staff, and United States Military Academy

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC), Defense Finance and Accounting Service (DFAS), Office of the DoD Inspector General, Defense Criminal Investigative Service, Office of the Secretary of Defense Personnel and Readiness, Office of the Secretary of Defense

☒ **Other Federal Agencies.**

Specify. Department of Veterans Affairs, Office of Personnel Management, Social Security Administration, Department of the Treasury, Department of Homeland Security, Department of Justice, Department of Health and Human Services, Internal Revenue Service, Selective Service Administration, U.S. Citizenship and Immigration Services, Department of Labor

☒ **State and Local Agencies.**

Specify. Joint Forces Headquarters - State

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Only authorized IPPS-A support contractors (CACI, BAH and subs) and system integrators will have access to the PII. The PII will be safeguarded with Appendix J security controls as required by the NIST Risk Management Framework. IPPS-A contract references 52.239-1 "Privacy Act Notification", "Privacy Act" and "Privacy or Security Safeguards"

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

Specify. America Red Cross, National Academy of Sciences, and Widow/Widower, Dependent, or Next -of-Kin (NOK) of deceased members.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

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

(2) If "No," state the reason why individuals cannot object.

IPPS-A Production system will contain the individual's personnel and pay file and all information needed to process related actions. If an individual objects to the collection of PII and refuses to provide it, this would preclude personnel or payroll processing such as a promotion or pay adjustment.

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.

IPPS-A obtains data from various hire/rehire databases. All individuals requesting entrance into the Army must provide the requisite information in order to gain entrance into the service. An individual may refuse consent to specific use of PII; however the PII is required for the personnel and pay processes. Refusal to provide the information may negate Soldier's enlistment/reenlistment option.

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.

Information has already been collected by a system in which IPPS-A is subsuming.