PRIVACY IMPACT ASSESSMENT (PIA)

For the

RESERVE COMPONENT AUTOMATION SYSTEM (RCAS) Release 7

U.S. ARMY PROGRAM EXECUTIVE OFFICE ENTERPRISE INFORMATION SYSTEMS

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: 75 (DA00063)
- ☐ **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 007-21-01-25-01-1640-00-201-067

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 Integrated Personnel and Pay System—Army

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., Armed Forces: Under Secretary of Defense for Personnel and Readiness;
Executive Order (EO) 9397, as amended (SSN)
And in accordance with DAA for PD RCAS

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.

The RCAS Release 7 accreditation boundary consists of two servers deployed at each gaining organization. Both of these servers are delivered as VMWare virtual images whose baselines are maintained by PD RCAS through a comprehensive Change Management (CM) process. One of the Servers in the set is running on a Windows Server 2008 R2 platform with IIS version 7.5. The other is running Windows Server 2008 R2 with Oracle 11g. There are 58 of these server sets deployed throughout the Army National Guard (ARNG) and the United States Army Reserve Command (USARC). Of these 58 deployments there are two deployment types, one for the NGB/USARC and the other for all of their subordinate sites. RCAS consists of a suite of applications that are unlocked accordingly based on what features are needed by each site.

Reference section 3a that describe the types of personal information about individuals collected in the system.

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

The PII in RCAS has the potential risk of being exposed to unauthorized individuals. Information that is printed must be tracked to ensure that it is exposed only to those that are authorized to view the PII and once the information is no longer needed, those prints must be disposed of securely. The sites are responsible for ensuring that users are trained to protect PII on the screen or in printed form.

A Defense in Depth layered tactic in use are Advanced Security Option (ASO) and Encrypting File System (EFS) technologies. These technologies are being used to encrypt data at rest and data in transit.. RCAS established procedures to ensure the proper handling of PII.

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.

Standard Installation/ Division Personnel System-Army National Guard (SIDPERS-ARNG)
Defense Joint Military Pay System-Reserve Component (DJMS-RC)
Defense Joint Military Pay System (DJMS)
Deployment and Reconstitution Tracking Software (DARTS)
Defense Civilian Personnel Data System (DCPDS) - Army National Guard
Army Training Requirements and Resources System (Course Info) (ATRRS)
Digital Training Management System (DTMS)
Reserve Component Common Personnel Data System (RCCPDS)
Reserve Retirement Repository (RRR)
Interactive Personnel Electronic Records Management System (IPERMS)
Medical Occupational Data System (MODS)
Regional Level Application Software (RLAS)
Defense Manpower Data Center-Defense Enrollment Eligibility Reporting System (DMDC-DEERS)
Engineering Base Operation Support System (ENBOSS)
Army Training Information Systems - System Information Services (ATIS-SIS)

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. L-3 Communications - National Security Solutions (NSS):
Data shall be protected in accordance with the appropriate Program Protection Plans IA guidelines. The contractor shall remain cognizant of Government data standards in order to ensure full compliance with Government data standards. Contractor personnel is required to comply with the Privacy Act of 1974 and Amendments. The contractor shall also comply with federal laws relating to the Freedom of Information Act (FOIA), 5 U.S.C. § 552.

☐ **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 method by which individuals can object to the collection of PII.

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

Not applicable because RCAS does not collect any information directly from individuals.

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.

Not applicable because RCAS does not collect any information directly from individuals.

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.

Not applicable because RCAS does not collect any information directly from individuals.