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:

REDS-U-ICAN - Redstone Arsenal Unclassified Installation Campus Area Network

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

09/23/20

Regional Network Enterprise Center Central - Redstone

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

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

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

The PII transmitted by various Unclassified ICAN network components or processed by and stored on RNECC-R managed computer clients and servers (e.g., SharePoint portal, Storage Area Network, etc.) is used for all aspects of civilian and military personnel management (e.g., hiring, administering, paying, rating, recall rosters, etc.), for day-to-day business processes and operations of various Division, Garrison, or tenant organizations, and for preparing for military and civilian deployment and redeployments. The PII is protected through both technical and procedural mechanisms/processes. Technical mechanisms/processes include strong boundary defense to detect and deter unauthorized access to the Unclassified ICAN or other anomalous behavior, proactive application of software updates and security settings to preclude exploitation of client and server application vulnerabilities, the use of machine and account enforced two-factor authentication (e.g., the use of National Security System (NSS) Token enabled client computers), Army approved Data-At-Rest (DAR) encryption on all client computers, access control for devices and storage locations where PII resides based on trust and need to know, and the availability of encryption for any electronic mail containing PII. In addition to the technical controls, users are required to complete annual training that addresses Information Assurance and protection of PII and organization data owners have the ability to limit access to any PII via the technical access control mechanisms (e.g., file permissions, encrypted storage, etc.) provided by the RNECC-R or inherent in the applications employed to support business processes. This combination of technical controls, effective business processes, and a trained and educated workforce all combine to ensure, to the greatest extent possible, that PII is properly protected.

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)*

The PII is being used for a variety of official functions including all aspects of military and civilian personnel management, installation and restricted area access control, security clearance verification, and other functional area business processes that rely on PII.

The intended use of collected PII is primarily for administrative use to facilitate management of assigned personnel and security actions.

e. Do individuals have the opportunity to object to the collection of their PII? [x] 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.

Individuals are provided appropriate Privacy Act Statements at the time of collection. These statements outline the methods for objecting to the collection of PII. PII is required to support employment, payroll, security clearance and access, and the authorized use of government computing systems. The individual is provided the opportunity to deny the disclosure of PII at the point of collection by the Army agent. Additionally, the individual is advised that the failure to provide the requested information may impede, delay, or prevent the further processing of the action which the information supports.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Individuals are provided appropriate Privacy Act Statements at the time of collection. These statements outline the purposes for collecting PII and give the opportunity for refusal. Since the information is collected and used as part of their employment, payroll, security clearance and access to classified information, and their access and use of DoD computing systems, the user signs an attestation element on the information collection form.

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

Whenever personal information is requested from an individual that will become part of a system of record retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act Statement.

Army Regulation 25-22 details individual's rights to access PII and rules for disclosure to third parties.

The various DoD, Army, and OMB forms used contain a privacy act statement. Web resources collecting or storing PII have a Privacy and Security link for the site. Some common examples an individual may encounter are as follows:

Privacy Act Statement
Chapter 87, title 5, U.S. Code, Federal Employees' Group Life Insurance, authorizes the solicitation of this information. The Office of Federal Employees' Group Life Insurance and your agency will use the data you furnish to determine your eligibility to receive benefits under the FEGLI Program. This information may be shared and is subject to verification, via paper, electronic media, or through the use of computer matching programs, with national, state, local or other charitable or social security administrative agencies in order to determine benefits under their programs or to obtain information necessary for determination or continuation of benefits under this program. It may also be shared and verified with law enforcement agencies when they are investigating a violation or potential violation of civil or criminal law. Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal government furnish a Social Security number or tax identification number. This is an amendment to title 31, Section 7701. If you don't furnish the requested information, you may not have the level of insurance protection you want.

Page 1, Top right corner of DA Form 67-9 and DA Form 2166-8: For Official Use Only (FOUO) See Privacy Act Statement in AR 623-3

Privacy and Security Notice

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

All forms used at Redstone Arsenal containing PII have a Privacy Act statement that states the authority for collecting the data, the principal purpose for the collection, any routine uses, and whether or not the disclosure is voluntary or mandatory.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Army Material Command (AMC) and its subordinate organizations, Army Futures Command, Garrison, CECOM, CPAC, PEO Aviation, PEO Combat Support and Combat Service Support, PEO Enterprise Information Systems, PEO Simulation, Training and Instrumentation, Redstone Test Center, US Army Corps of Engineers, DMPO
☐ Other DoD Components	Specify.	
☐ Other Federal Agencies	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

PII is collected directly from individuals as well as from DOD personnel and security databases.

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)*
☒ Face-to-Face 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://dpcld.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.

l. 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. Infrastructure

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

(3) Retention Instructions.

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 statue 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.

10 U.S.C. 3013, Secretary of the Army; and E.O. 9397, as amended (SSN).

Information collected supports official business processes for the lawful operation of the military installation and unit mission area; the management of civilian and military staff executing official duties at the military installation; and the lawful controls associated with granting access to contractors or other members of the civilian community demonstrating a valid need to access the military installation. Additionally, users access, update, route, and execute process actions for records maintained in various official web-based resources. The provisions and controls established for those systems are inherited and apply to the operations of the computing devices connected to the RNECC-R Unclassified ICAN.

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.