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:

FEUS U-ICAN - FORT EUSTIS UNCLASSIFIED-INSTALLATION CAMPUS AREA NETWORK

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

08/25/20

South Atlantic Regional Network Enterprise Center (RNEC) Fort Eustis

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 the various ICAN network components or and stored on NEC 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 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 Common Access Card 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 NEC 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 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.

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

Organization and Office Rosters

In Accordance with Title 5, U.S.C. § 552a (Privacy Act of 1974) as implemented by the Federal Register, Department of Defense, Department of the Army, 32 CFR Part 505, The Army Privacy Program; Final Rule, protected personal information will not be disclosed from this roster to any commercial enterprise or representative thereof or to any individual outside the Department of Defense. This roster will be safeguarded IAW paragraph § 505.2, of the Federal Register named above. When updated, obsolete copies will be destroyed as required by paragraph 4-501, AR 25-55, The Department of the Army Freedom of information Act Program.

Or

In Accordance with Title 5, U.S.C. § 552a (Privacy Act of 1974) as implemented by the Federal Register, Department of Defense, Department of the Army, 32 CFR Part 505, The Army Privacy Program; Final Rule, protected personal information will not be disclosed from this roster to any individual outside the Department of Defense except to (specify the exceptions, e.g., Officers Wives Club, Enlisted Wives Club and/or the <<XX Organization Social Roster, as appropriate). As to the preceding, excepted individual and organizations, consent to disclosure is expressly given by personnel listed below. This roster will be safeguarded IAW paragraph § 505.2, of the Federal Register named above. When updated, obsolete copies will be destroyed as required by paragraph 4-501, AR 25-55, The Department of the Army Freedom of information Act Program.

Alert Rosters

In Accordance with Title 5, U.S.C. § 552a (Privacy Act of 1974) as implemented by the Federal Register, Department of Defense, Department of the Army, 32 CFR Part 505, The Army Privacy Program; Final Rule, protected personal information (home address and home telephone numbers) will not be disclosed from this roster to anyone outside the Department of Defense. This alert roster will be kept in a secure place at all times. When updated, obsolete copies will be destroyed as required by paragraph 4-501, AR 25-55, The Department of the Army Freedom of information Act Program.

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.	NETCOM, TRADOC HQ,TRADOC G27 Operational Environment Training Support Center, Joint Base Langley/Eustis 733d/633d, 7th Sustainment Transportation Brigade, IMCOM, DFAS
☐ 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

ADPAS, CPOL (MyBiz), DCPDS, IMCOM Orders Processing Application

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [x] E-mail
- [x] Official Form (*Enter Form Number(s) in the box below)*
- [x] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [ ] Website/E-Form
- [x] Other *(If Other, enter the information in the box below)*

DD2875, DD2842, SF 182

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
- [x] 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.

No System of Records that retrieve information using unique identifiers.

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.

0 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 RNEC U-ICAN. These systems include, but are not limited to Army Knowledge Online (AKO), Army Records Information Management System (ARIMS), Army Benefits Center Civilian (ABC-C), Go Army Education (GoArmyEd), Total Officer Personnel Management Information System II (TOPMIS II), Army Defense Integrated Military

Human Resources System (Army DIMHRS), Digital Training Management System (DTMS), and Electronic Military Personnel Office (eMILPO).

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.

The Fort Eustis RNEC Unclassified Internal Campus Area Network (U-ICAN) system does not collect data from 10 or members of the public in a 12 month period.