PRIVACY IMPACT ASSESSMENT (PIA)

For the

CRTC-ICAN - COLD REGIONS TEST CENTER CAMPUS AREA NETWORK

U.S. Army Cold Regions Test Center

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: 17763 DA303258
- ☐ **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

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

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.

AR 25-1; Army Knowledge Management and Information Technology, AR 25-2; Information Assurance.

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 Cold Regions Test Center Campus Area Network (CRTC-ICAN) is the test data collection network at Fort Greely, Alaska. The CRTC-ICAN resides on the Defense Research Engineering Network (DREN) and passes authentication traffic to the NIPRNET. The CRTC-ICAN also consists of various Army Approved appliance products which include; Routers, Firewalls, Switches, IDS, IPS, etc. The current configuration of the CRTC-ICAN network infrastructure consists of 1 router that is locally administrated and 1 router on the DREN that is managed by the DREN Network Operation Center (NOC) team. There is 1 Firewall that is locally managed, and there are approximately 35 switches that are locally managed. There is also an Intrusion Prevention System (CounterAct) that is utilized on the DREN.

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

Access to these files by non-authorized personnel would cause the leak of PII. Data is saved on removable hard drives for which are protected by Data At Rest (DAR) which is BitLocker for which encrypts the entire drive and restricts access to authorized personnel only by their CAC credentials. Also drive shares on network servers are utilized as well for which the file folders are encrypted and only access by authorized personnel with their CAC credentials is possible.

Also within the Intelligence & Security Office (G2/S2) security clearance information as well as electronic finger prints are maintained as well.

Network is protected by boundary defense to include Firewall, IDS/IPS, HBSS HIDS, etc. that restricts outside access to the internal network. Also As CRTC is on the Defense Research Engineering Network (DREN) there are network defense devices maintained by Army Network Command (NETCOM) at the top of the network stack that maintains the TECHCON 9 crossover from DREN to NIPRNet.

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. Only access by appropriate and approved CRTC personnel. No outside access is shared nor authorized. Data is only stored.

☐ **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.

☐ **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.

IF personnel do not want their data within the RM or CPAC offices stored they can follow the applicable local Privacy Program process that outlines how to request this does not occur.

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

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.

IF personnel do not want their data within the RM or CPAC offices stored they can follow the applicable local Privacy Program process that outlines how to request this does not occur.

Consequences of withholding their consent could result in removal from work position due to requirement of data being shared. This could revolve around Clearance information, Civilian Personnel Information, Performance Rating information, etc.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

All personnel are required to sign a privacy act statement per Army and DoD requirements. Also a non-disclosure agreement and a consent to monitoring. All these documents outline the requirement for the use of their PII for DoD/Army requirements only.

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