PRIVACY IMPACT ASSESSMENT (PIA)

For the

EROSTER - EMERGENCY RELOCATION STAFF ROSTER

HQDA, G-3/5/7 (Army Continuity of Operations (COOP) Program Office

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: 17184 DA303507
- ☐ **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 A0500-3c DAMO

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.

Section 2-10 of U.S. Army Continuity of Operations Program Policy and Planning (AR 500-3) requires all ERG personnel to be cleared for entry into a continuity facility (CF) or emergency relocation facility (ERF). The execution of this requirement is facilitated through the use of the EROSTER application to store PII data elements that are normally submitted or recorded on an access roster. For example, access rosters for all CF site orientations are generated via EROSTER and sent to the Site R Security Office for coordination. Personnel not on the access roster can be denied entry to the site.

Other cited authorities include: Executive Order 12656 and National Security and Homeland Security Presidential Directive/NSPD 51, National Continuity Policy, and Homeland Security Presidential Directive/HSPD-20, National Continuity Policy.

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.

Description:
EROSTER is used to identify members of the HQDA Emergency Relocation Group (ERG), the continuity facilities they deploy to; and to manage contact information and COOP training for each ERG member. The types of personal information collected and stored in the encrypted EROSTER SQL database are identified in Section 3 of this PIA.

Accreditation:
EROSTER inherits the accreditation for the HCEN-HQDA Classified Enterprise Network (AITR #DA198995). The HCEN-HQDA has been approved by the ITA DAA via email reply to Army G-6:

Ref. Email, AAIT-ES, Mr. Gregory L. Garcia, HCEN v3.0 IATO, 5 Sep 14, subject: RE: HCEN v3.0 - IATO (UNCLASSIFIED), effective 05 Sept 2014 with an ATD of 04 Mar 2015.

APMS:
A child-parent relationship has been updated and reflected in APMS under the Dependencies folders for the capabilities of the following systems:

EROSTER (AITR #198995) is a child of GCCSLAN (AITR #02168) which is a child of HCEN-HQDA (AITR #198995). Likewise, HCEN-HQDA is listed as a parent of GCCSLAN which is a parent of EROSTER.

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

The disclosure of privacy information is mitigated by hosting EROSTER on the SIPRNET and controlling the exposure of the information to a controlled group of persons, e.g., CPOCs and EROSTER administrators. Each CPOC and administrator can only view the records of their ERG personnel, they cannot view the personnel records of other organizations.

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. PII information is collected to verify security clearances, facilitate COOP operations and to track training. The PII data elements in EROSTER are only shared with those with authority to access within Headquarter, Department of the Army (HQDA).

☒ **Other DoD Components.**

Specify. The Pentagon Force Protection Agency is tasked in DODI 5110.11, Raven Rock Mountain Complex, 4 October 2010 to provide for access control. Their current procedure requires submission of complete SSN as well as other security clearance related information obtained in the Joint Personnel Adjudication System (JPAS). JPAS requires use of SSNs to verify security clearance information.

☐ **Other Federal Agencies.**

Specify. Not Shared

☐ **State and Local Agencies.**

Specify. Not Shared

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

Specify. Not Shared

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

Specify. Not Shared

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.

By virtue of being designated an ERG member by their organization's leadership and the duties that are to be performed, individual consent is inferred. PII information is required to create continuity facility access rosters.

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.

By virtue of being designated an ERG member by their organization's leadership and the duties that are to be performed, individual consent is inferred. PII information is required to generate continuity facility access rosters.

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.

When ERG members are asked to provide PII data they are advised that their information will only be used to verify security clearance, facilitate COOP operations and to track training. ERG members are informed that PII data is protected on a secured network and only authorized users with an official need to know will have access.

Also, a Privacy Advisory describing the use, dissemination and collection of PII in identifiable form will be located on the website.

Privacy Advisory Statement

AUTHORITY: Section 2-10 of U.S. Army Continuity of Operations Program Policy and Planning, Army Regulation 500-3, Executive Order 12656 and National Security and Homeland Security Presidential Directive/NSPD 51, National Continuity Policy, Homeland Security Presidential Directive/ HSPD-20, National Continuity Policy, Paragraph 6.1.4.2, DODD3030.42 Defense Continuity Plan Development, and Paragraph 3.b, DODI 5110.11 Raven Rock Mountain Complex.
PRINCIPAL PURPOSE(S): To provide means to verify security clearance information.
ROUTINE USE(S): Social Security Numbers are used to verify security clearance information to facilitate access into the Continuity Facility.
DISCLOSURE: Mandatory. Information is required to verify clearance information. Failure to provide Social Security Numbers will result denial of access to the Continuity Facility.