PRIVACY IMPACT ASSESSMENT (PIA)

For the

United States Army Operational Test Command (USAOTC)
United States Army

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: 12858 AITR number DA184970
- ☐ **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 K890.21 DoD and A0690-200 DAPE

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.

U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN).

5 U.S.C. 301, Departmental Regulations; Pub. L. 106-229, Electronic Signatures in Global and National Commerce; OASD (C3I) Policy Memorandum, subject: Department of Defense (DoD) Public Key Infrastructure (PKI); and OASD (C3I) Memorandum, subject: Common Access Card (CAC).

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 concept of operations of the OTCNET is to provide information technology and communication services to OTC users in supporting OTC's mission. It includes file transfer, web servers, file storage, VPN, email, etc. Authorized OTCNET users are authenticated through the use of the CAC as a two-factor authentication means.

The purpose is to generate draft PII (e.g.; social security numbers) data for evaluations prior to uploading in DFAS, NSPS, DTS; to complete security checks on required forms and to retain a call back roster on personnel during disasters, contingencies or outages.

Types of information collected and stored in restricted folders with limited access on network devices for Command Group, HHC, Budget (RM) and Personnel (Civilian Liaison): alert rosters (military), evaluations (military & civilians); PDF copies of SF50s (civilians), security checks (e.g.; NAC, visitor requests, network access forms, common access cards, RCERT if it involves child pornography).

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

Risks are safeguarded by NTFS (BitLocker), local security permissions and restricting data file access to " need to know." Global Administrators for example cannot access the data; only System Administrators for NASW organizational group containers and local Resource File Server with privilege access can perform data back ups.

PII data to be shared outside DoD include for example FBI & SBI would involve severe Information Assurance incidents (hacking), breaking local laws (e.g., homicide investigations), child pornography or espionage.

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. Defense Finance and Accounting Service, Office of Personnel Management, Criminal Investigation Department.

☒ **Other DoD Components.**

Specify. Dept. of Defense High Performance Computing Modernization Program
Defense Research and Engineering Network

☒ **Other Federal Agencies.**

Specify. Federal Bureau of Investigation

☐ **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.

Users have the option to object, but it may impact the outcome. For example if a civilian employee is on jury duty and they work at Fort Hood they are required to sign the check from TX and turn it over to CPO with full social security number on the back under their signature; they can refuse, but if they do they have to amend their time sheet and take personal leave versus paid admin time off. Another example is clearance verification/validation; full SSN is required and can delay processing without it.

(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.

Users have the option to only use the last 4 SSN unless the form requires the full social. They are also given the opportunity based on why it's being collected to talk directly to the System Owner (e.g., AKO).

(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.

- [x] **Privacy Act Statement**
- [ ] **Privacy Advisory**
- [ ] **Other**
- [ ] **None**

Describe each applicable format.

PRIVACY ACT: The information contained in this roster is subject to the provisions of the Privacy Act of 1974. Disclosure of contents to persons other than those that have an official need-to-know is strictly prohibited. Officials listed in the distribution block will ensure that this roster and the information it contains are protected against unwarranted disclosures, loss, or tampering. DISPOSAL: Destroy when updated.

"Phone numbers will ONLY be given to USAOTC command group directly. In response to a request for information or numbers by anyone other than the command group, the number will NOT be provided. The SDNCO will take a message and number, then will notify person needing to be contacted."

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.