PRIVACY IMPACT ASSESSMENT (PIA)

For the

USARC SHAREPOINT - USARC SHAREPOINT 2013 ENVIRONMENT FOR TMT

OCAR - HQ, USARC - Headquarters, US Army Reserve Command

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: DA307735
- ☐ **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.

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.

USARC personnel will use the Task Management Tracker (TMT) to process actions for staffing collaboration and senior leader approvals, including Human Resource (HR) actions. TMT uses SharePoint as its document repository. TMT will have a separate SharePoint Site Collection for this purpose. Only personnel who have access to both SharePoint and TMT will be able to access the data collected - both require access to the ARNET and user authentication (CAC access and active directory accounts).

PII required to process Human Resource (HR) actions for Army Reserve Soldiers varies by action type per USAR personnel Action Guide.

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

Privacy risk for this system is low due to the level of safeguarding. USARC will maintain this system in a controlled facility. Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Access to the system is controlled by access permissions and further restricted from within TMT utilizing security settings. Staffing actions which contain PII will be restricted to only those personnel within the system who are a part of the particular routing (need to know).

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. Staff principals in the chain of command, personnel managers within Active Army, Army Reserve, and Army National Guard, Department of the Army Inspector General, Army Audit Agency, US Army Criminal Investigation Command, US Army Intelligence and Security Command, Provost Marshall General, and Assistant Secretary of the Army for Financial Management and Comptroller.

☒ **Other DoD Components.**

Specify. Department of Defense Inspector General and Defense Criminal Investigative Service.

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. Science Applications International Corporation (SAIC). SAIC contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the confidentiality and security of a Soldier's PII. The contractual language keys on training as a fundamental element in creating awareness and understanding of PII and why it is important to control and safeguard. The language also stresses securing PII material and equipment housing PII at the end of each work day. Contractual language directs and requires each SAIC employee in support of this system to have a valid Secret clearance prior to working on the program. The contract specifically states that contractor personnel will adhere to the Privacy Act, Title 5 of U. S. Code Section 522a, and all applicable agency rules and regulations.

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

Specify. N/A

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.

Anytime a system collect directly from the individual, the individual has the right to object. However, there can be consequences to the objection. If the PII is collected directly from other IT system, consent is implied.

(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.

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

Individuals may either submit or decline to submit the requested information. Anytime a system collects directly from the individual, the individual has the right to object. However, there can be consequences to the objection. If the PII is collected directly from other IT systems, there is implied consent.

In general, applications are intended to collect information for specific and clearly defined purpose. Collection of PII is mandatory for military personnel; they do not have the opportunity to object. Refusal to provide required information would result in administrative sanctions or punishment under the Uniform Code of Military Justice.

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.

SharePoint has general access web pages and restricted web pages. Certain areas of SharePoint, such as sites where personnel can upload or download files, may allow posting of content which can be accessed and viewed by others; these areas may impose additional usage guidelines, rules, and restrictions. Users agree to comply with published USAR SharePoint governance and Army Privacy Regulation 32 CFR 505.

1. Access to SharePoint and the ability to login to the portal does not automatically grant access to all areas of available information.
2. Access to SharePoint requires Common Access Card (CAC) authentication and role-based user permissions based on official need to know. Only authorized users required to perform the stated mission will be grated right to access and post data on respective SharePoint sites.
3. Site Administrators utilize the Deny-All-Allow-By-Exception access to Personally Identifiable Information(PII) and sites. No one will gain access to a site unless specifically granted access by the Site Administrator.
4. Each FOUO and Privacy Act Data document or site must be appropriately labeled.
5. PII is restricted to users on a need-to-know basis.

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.