PRIVACY IMPACT ASSESSMENT (PIA)

For the

POTBSCS - POSITION OF TRUST BACKGROUND SCREENING COLLABORATION SYSTEM
US Army Deputy Chief of Staff for Personnel / Human Resources Command (HRC)

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 | 12580   DA197443 |

☐ **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 <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes**   ☐ **No**

If "Yes," enter Privacy Act SORN Identifier | A0680-31b AHRC |

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.

10 United States Code 3010, Secretary of the Army; Army Regulation (AR) 600-8-104, Military Personnel Information Management/Records; AR 614-200, Enlisted Assignments and Utilization Management; and Executive Order 9397 as amended (SSN) as amended.

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 Position of Trust Background Screening Collaboration System (POTBSCS) provides the Department of Defense Consolidated Adjudication Facility (DOD CAF) with a daily list of Soldiers who are being nominated for positions of trust (Drill Sergeant, Recruiter, Advanced Individual Training (AIT) Platoon Sergeant, etc.). The DOD CAF retrieves existing information on each Soldier from other systems and uploads a report to POTBSCS. HRC retrieves the report, which assists HRC in determining if the Soldier is eligible to be placed in a position of trust. Previous name: Enlisted Background Screening Web CCF Pending Program (EBSS-WEB-CCF-PEND).

Types of PII collected includes personal identification and military information.

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

All systems and environments have threats that seek to exploit and cause harm to the information. Some threats are natural, some are inherent in the system design, some can be attributed to unauthorized personnel, and some to authorized personnel who make mistakes. Four general categories of threats exist: human-intentional, human-unintentional, structural, and natural. The system is maintained in a controlled facility. Appropriate technical, personnel, physical and operational safeguards are in place for the access, collection, use and protection of information. Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal.

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. | Army Audit Agency, Assistant Secretary of the Army for Financial Management and Comptroller, Department of the Army Inspector General, Provost Marshal General, US Army Criminal Investigation Command, and US Army Intelligence and Security Command.

☒   **Other DoD Components.**

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

☐   **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 contractual language acknowledges the sensitivity of PII and describes the importance of protecting and maintaining the