PRIVACY IMPACT ASSESSMENT (PIA)

For the

Officer Selection Support System (OSSS)

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: 3710 (APMS ID DA01828)
- ☐ **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 007-21-01-20-02-2395-00

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 A0600-8-104 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.

Title 10 US Code Section 3013, Secretary of the Army, Chapter 36, Subtitles I-V (Sections 612-646); Executive Order 9397 as amended (SSN); DODD 1310.1, Rank and Seniority of Commissioned Officers; DODI 1300.19, Joint Officer Management Program; DODI 1300.20, DOD Joint Officer Management Program Procedures; DODI 1320.4, Military Officer Actions Requiring Approval of the Secretary of Defense or the President, or Confirmation by the Senate; DODI 1320.12, Commissioned Officer Promotion Program; DODI 1320.14, Commissioned Officer Promotion Program Procedures; Under Secretary of Defense Memo, General and Flag Officer Boards - Adverse Information of a Credible Nature, 19 July 2006; AR 135-155, Promotion of Commissioned Officers and Warrant Officers Other Than General Officers; AR 600-8-29, Officer Promotions; AR 600-8-104, Military Personnel Information Management Records; DA Memo 600-2, Policies and Procedures for Active Duty List Officer Selection Boards; and DA G-1 Memo, Personnel Suitability Screening Policy (Enlisted and Officer), 9 March 2006.

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 Officer Selection Support System (OSSS) supports and provides information for the centralized Officer Promotion Selection System. Through menu driven programs, OSSS allows the Promotions Branch to: create eligible files; verify selection board results; publish promotion lists; and issue promotions. The application runs on both the NIPR and SIPR networks.

Personal information maintained by the system includes identification data and military personnel 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. Staff principals in the chain of command, the Department of the Army Inspector General, the Army Audit Agency, the US Army Criminal Investigation Command, the US Army Intelligence and Security Command, the Provost Marshall General, and the Assistant Secretary of the Army for Financial Management and Comptroller.

☒ **Other DoD Components.**

Specify. The Defense Finance and Accounting Service (DFAS), the Department of Defense Inspector General, and the 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 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 a work day. Contractual language directs and requires each SAIC employee in support of the 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 US 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.

N/A

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

Since data are not collected directly from individual Soldiers they are not provided an opportunity to object to its collection by OSSS. However, Soldiers implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army.

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.

N/A

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

Since data are not collected directly from individual Soldiers they are not provided an opportunity to consent to its use by OSSS. However, Soldiers implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army.

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.

OSSS only extracts existing PII data from other Army information systems. Since data are not collected directly from individual Soldiers they are not provided either a Privacy Act Statement or Privacy Advisory. However, Soldiers implicitly consent to capture and use of that information at the time of employment or enlistment in the Department of the Army, at which time they are provided a Privacy Advisory.

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.