PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Knowledge Online NIPR (AKO-N)
U.S. Army, Chief Information Officer

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: 2611 (DA04249)
- ☐ **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 A0025-1 CIO G6 (update in progress)

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.

AKO authority to collect information is given by the following: 10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 8500.01E, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance; E.O. 9397(SSN) (As amended); DoD 6025.18-R.

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 purpose of AKO is to perform knowledge management and register users in order to facilitate electronic communications and collaboration among DoD personnel and other authorized (CAC enabled approved) users. This system serves as an Army controlled repository for information needed by DoD personnel necessary for performance of duties and other DoD-related functions. Access is controlled based on individual needs for specific types of information. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation, or reporting purposes.
The AKO Lightweight Directory Access Protocol Data Store (LDAP) & Electronic Data Dictionary (EDD) include the following primary information: Personal, Employment, and Military information. Personal information is provided by authoritative sources ITAPDB and DMDC for non army personnel in support of AKO. In addition, the U.S. Army Accessions Command, U.S. Army Recruiting Command, National Guard Bureau, U.S. Military Academy, and Defense Finance & Accounting Service serve as data sources.
AKO collects PII for authentication, access control to the system and information contained in the system, and general ID management.

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

System data is protected at the Unclassified Sensitive level. All personnel accessing government computer information are required to undergo and receive at the minimum a favorable National Agency Check. The individuals may have access requirements and are limited to specific or general information in the computing environment. The System Administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Currently, only system users and service liaisons (and their authorized contract users) have the capability to connect to the system. With the exception of Systems Administrators, Information Assurance Security Officers and software maintenance personnel, users fall into non-sensitive Information Technology (IT) Category III (non-privileged) positions as designated in DoD Directive 8500.01E and DoD Instruction 8500.2. Persons in IT Category-III positions require a National Agency Check, Entrance National Agency Check, or National Agency Check with Inquiries. All system administrators, information assurance and software maintenance personnel are in non-sensitive IT Category-I (privileged) positions. Persons in IT Category-I positions require a Single Scope Background Investigation (SSBI). Information is made available to users through the application or Enterprise server. Each authorized user must present authorized credentials before accessing the resources. There is daily monitoring, daily notification of inactive accounts, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVAs) and Security Technical Implementation Guides (STIGs). Files transferred across the NIPRNet do not leave the Army domain and are encrypted.

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. Information is available to authorized Army users with a need to know in order to perform official government duties. This includes the following organizations: Army Staff Principals in the chain of command; Department of Army Inspector General; Army Audit Agency; US Army Criminal Investigative Command; US Army Intelligence and Security Command; Provost Marshal General; Assistant Secretary of the Army for Financial Management and Comptroller; Army Civilian Human Resources Agencies; US Army garrisons at installations; and Headquarters, US Army Installation Management Command. Information is available to authorized Army users whose organizations have

signed a Memorandum of Agreement with Army Knowledge Online. These systems include Single Sign On (SSO) and LDAP customers to AKO's Directory Services.

☒ **Other DoD Components.**

Specify. Information is available to authorized DoD users with a need to know in order to perform official government duties. This includes the following organizations: Department of Defense Inspector General, Defense Criminal Investigative Service, Under Secretary of Defense for Personnel & Readiness, Defense Manpower Data Center. In addition, the DoD blanket routine uses apply to this system.

☒ **Other Federal Agencies.**

Specify. Information is available to other authorized Federal agency users with a need to know in order to perform official government duties. This includes the following organizations: Civilian Personnel Operations Centers, Civilian Personnel Advisory Centers.

☐ **State and Local Agencies.**

Specify.

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

Specify. Information is available to authorized contractor personnel in order to perform official government duties. Personnel include System Administrators from Northrop Grumman and its program partners, and AKO Help Desk Customer Service Representatives from United Solutions and Services and its program partners. It should be noted that other contractor personnel may gain authorized access to PII in the future as AKO supports future emerging capabilities. All Contractor personnel with with access to PII are required to sign an Privileged Access Agreement (PAA) and Non-Disclosure Agreement.

☐ **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.

A Privacy Act Statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and is displayed each time the user logs on to the system. System registration and use are voluntary and individuals choose to enter their own PII at which time a privacy act statement is displayed for user confirmation.

(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.

A Privacy Act Statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal and is displayed each time the user logs on to the system. System registration and use are voluntary and individuals choose to enter their own PII.

(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.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

A Privacy Act Statement describing the use, dissemination and collection of information in identifiable form is located on the website at the registration portal. System registration and use are voluntary and individuals choose to enter their own PII.

Privacy Act Statement

• Authority: 10 U.S.C. Section 3013, Secretary of the Army; Army Regulation 25-1, Army Information Management; Army Regulation 380-19, Information Systems Security; E.O. 9397 (SSN).
• Principal Purpose: This information will be used to verify the identity of eligible users of the Army Knowledge Online (AKO) system.
• Routine Uses: None. The "Blanket Routine Uses" set forth at the beginning of the Army's Compilation of Systems of Record Notices also applies to this system.
• Disclosure: Voluntary. However, failure to provide the requested information will result in denial of access to the AKO system.