PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

EXCHANGE SECURITY CLEARANCE CASE SYSTEMS

2. DOD COMPONENT NAME:

If Other, enter the Component name in the box below.

3. PIA APPROVAL DATE:

Army and Air Force Exchange Service (the Exchange)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☒ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

To assist in the processing of personal security clearance actions for adjudication of clearance.
To record security clearances issues or denied.
To verify facility access, and access to classified, sensitive, or other controlled information positions and use of security systems
To assign associates to sensitive positions.
Used by Exchange executives for adverse personnel actions which may include removal from sensitive positions, duties, or employment.
To deny access to sensitive positions, duties, or systems.
To decide on revocation of security clearance of any of the above, and used in connection with removal of clearance during out-processing.

Collective documents may include Individual's full name, date of birth, Social Security Number (SSN); fingerprints; Department of Defense Identification Number (DoD ID Number), and ID card bar code value; Military Unit Identification Code (UIC); sex, and marital status; addresses (home, billing, and shipping); e-mail address (personal and/or business) and telephone number (personal and/or business); personal automobile license plate number; military or civilian branch of service identifier and employment grade level; military or civilian status (active, reserve, retired, veteran, civilian, officer, enlisted, family member, survivor, foreign, local national, etc.); privilege identifier; financial information (bank account routing number and account number); job location; supervisor's name and contact information (phone and e-mail address); reason for departure; clearing office approval. This system also maintains pending and completed security clearance actions; briefing/debriefing statements for special programs, sensitive positions and other related information and documents required in connection with personnel security clearance adjudication, background investigation results, and security approvals or denials.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Verification of Identity, Identification in other systems to verify data for adjudication of security clearance to facilities, position, or systems, Authorization of individual access to such items, and mission-related administrative use that may be used by management for other purposes for access, removal, or separation from employment.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individual have access to deny specific information being collected,. Web-based environments provide individuals with the Privacy Act Statement showing the routine uses of disclosure, also available on collective forms. Individuals have the option to stop processing the on-line communication at any time prior to pressing submission. However, choosing so will deny proper clearance to work on government property or access to positions of sensitive nature for the Exchange.

f. 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.

Data collected is used to administer security clearance for accessing government facilities and systems. The collected information is required in order for an individual (employee, contractor, vendor) to work for or with the Exchange. Additional uses as described within this document may be used for appropriate business operations. Data is provided is not used for any other means that that for which is was collected.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

PRIVACY ACT STATEMENT
AUTHORITY: 10 U.S.C. §7103, "Secretary of the Army"; 10 U.S.C. §9013, "Secretary of the Air Force"; United States Presidential Executive Order (E.O.) 13526, "Classified National Security"; E.O. 10450, "Security Requirements for Government Employment"; Department of Defense Instruction (DoDI) 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmental Information"; DoDI 5200.02, "DoD Personnel Security Program (PSP)"; Army Regulation (AR) 380-67, "Personnel Security Program"; Air Force Instruction (AFI) 31-501, "Personnel Security Program Management"; AFI 31-401, "Information Security Program Management"; AR 215-8/AFI 34-211(I), "Army and Air Force Exchange Service Operations"; and E.O. 9397, (SSN), as amended.

PRINCIPAL PURPOSES: To assist in the processing of personnel security clearance actions; to record security clearances issued or denied, and to verify for access to classified information or assignment to a sensitive position.

ROUTINE USES: Records may be disclosed outside of DoD pursuant to Title 5 U.S.C. §552a(b)(3) regarding DoD "Blanket Routine Uses" published at https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/

DISCLOSURE: Voluntary, however, failure to provide information may result in denial of a Common Access Card; non-enrollment in the Defense Enrollment Eligibility Reporting System (DEERS); refusal to grant access to DoD installations, buildings, facilities, computer systems and networks; and denial of DoD benefits if otherwise authorized.

AGENCY DISCLOSURE NOTICE
The public reporting burden for this collection of information, 0702-0135, is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

Consent to Criminal History
I hereby acknowledge that with the voluntary completion of this form, I am requesting access to a Department of Defense (DoD) facility in accordance with HSPD-12 credentialing and the Exchange EOP 66.04. I understand that assignments exceeding 6 (six) months require reverification by Force Protection and every 6 (six) months thereafter until my service is no longer required.

TASS Request Collection
Information collected on this form will be used by AAFES Force Protection for input into the Trusted Associate Sponsorship System (TASS) owned and controlled by the Defense Manpower Data Center (DMDC) allowing sponsorship in the Defense Enrollment and Eligibility Reporting System (DEERS).

Request for E-QIP Access
The information collected on this form will be used by AAFES Force Protection to facilitate the pre-screening selection process and electronic access into the United States Office of Personal Management Electronic Questionnaires for investigative Processing (e-QIP).

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Exchange Executive Group Force Protection, Attorney Staff, Office of the Inspector General, Loss Prevention, and Executive Management.
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Department of Defense to include Army, Air Force, Navy, Marines, DeCA as needed and authorized; U.S. Criminal Investigation Commands, Inspector Generals.

☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Department of Justice, Office of Personnel Management.
☒ State and Local Agencies	Specify.	State/Local/Federal Law Enforcement Agencies and Attorneys.
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	National Background Investigation Bureau (NBIB)
☒ Other *(e.g., commercial providers, colleges).*	Specify.	Privacy Attorneys and Staff, Foreign Law Enforcement, Intelligence and/or Security Agencies, Previous Employers, Financial Institutions, Credit Bureaus.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- ☒ Individuals
- ☒ Existing DoD Information Systems
- ☒ Other Federal Information Systems
- ☒ Databases
- ☒ Commercial Systems

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- ☒ E-mail
- ☒ In-Person Contact
- ☒ Fax
- ☐ Information Sharing - System to System
- ☒ Other *(If Other, enter the information in the box below)*
- ☒ Official Form (*Enter Form Number(s) in the box below)*
- ☒ Paper
- ☐ Telephone Interview
- ☒ Website/E-Form

The Exchange ROBA system collects 100% of data. However, in certain situations and rarely used, specifically in areas for which are in areas with no access to computer system, physical collection may be used for the collection of information. Data collected on physical forms is either mailed or security transferred by fax or email to the Exchange Force Protection who will delegate input into ROBA. Physical forms used is based on the security requested and my include Exchange Forms 3900-002, Request for TASS; 3900-006, Background Request; 3900-013, Request for previous e-QIP; and 3900-025, NACIT1 Fingerprint Request Form. Alternatively fingerprints may be submitted by local law enforcement entities or other government agencies by the individual. Access to any Web-Collection or forms is used to consolidate data and present to the proper DoD or Federal Authority to approve/deny security clearance.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier: 1703.03 AAFES

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

1703.03 AAFES is currently being reviewed for updates and consideration of rescindment to be replace with an applicable Government Wide or DPCLTD SORN which covers Exchange Security collections and maintenance.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.	DAA-GRS-2017-0006, Sections 0001, 0003, 0011, 0015, 0016, 0018. 0024. 0025, and 0026
(2) If pending, provide the date the SF-115 was submitted to NARA.	

(3) Retention Instructions.

Varies. GRS Record Retention ranges from temporary, no longer needed, or up to 50 years dependent on the document involved. Information on paper media is destroyed by cross shredding and/or burning at the time the data is input into a secured system. Electronic information is destroyed by removing from database and deleting all sources of data within electronic format, including backup data based on the proper retention section. System owners and security operators in the Exchange Force Protection are responsible for reviewing and properly destroying records as allocated in the Exchange Administrative Manual.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 7103, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; United States Presidential Executive Order (E.O.) 13526, Classified National Security; E.O. 10450, Security Requirements for Government Employment; Department of Defense Instruction (DoDI) 5200.01, DoD Information Security Program and Protection of Sensitive Compartmental Information; DoDI 5200.02, DoD Personnel Security Program (PSP); Army Regulation (AR) 380-67, Personnel Security Program; Air Force Instruction (AFI) 31-501, Personnel Security Program Management; AFI 31-401, Information Security Program Management; AR 215-8/AFI 34-211(I), Army and Air Force Exchange Service Operations; and E.O. 9397, (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0702-0135, Exchange Security Verification for Contractors/Vendors, 31 DEC 2025.