EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

Exchange Security Clearance Web-Based Portal/Storage
Executive Group - Force Protection

Questions relative to this document should be directed to the Exchange Office of General Counsel, Compliance Division, ATTN: Privacy Manager by mail to 3911 S. Walton Walker Blvd., Dallas, TX 75236 or through e-mail to PrivacyManager@aafes.com.

OBJECTIVE: The objective of a PIA is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing, or processing sensitive, personal data that may be concerned to be private. **A PIA should be completed prior to development/procuring any new IT system which collects/maintains such information or updated when a significant change is made to the system.** The OGC-C Privacy Manager for the Exchange will track, monitor, and approval all finalized PIA and compliance with the E-Government Act of 2002. Completed and approved PIAs will be forwarded to the system owner and to the IT-Government (IT-G) representative.

SECTION 1: IS A PIA REQUIRED?

A. Will this Exchange information system or electronic collection of information collect, maintain, use, and/or disseminate Personal Identifiable Information (PII) about members of the public, federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? (Mark all that apply).

☒ **Members of the General Public.**

☒ **Foreign Nationals**

☒ **Federal Personnel / Exchange Associates**

☒ **Federal Contractors and/or Vendors**

B. If no items are marked in question A, you may stop here. Have this PIA signed and return it to the Privacy Manager.

C. If any item in A is marked, proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

A. Why is this PIA being created or updated? Choose one:

☐ **New Information System** ☒ **New Electronic Collection**

☒ **Existing Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified Information System**

If unsure, consult OGC-C Privacy Manager.

B. Does this information system or electronic collection require a Privacy Act System of Records Notice (SORN)? [if unknown, please contact OGC-C]

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, a SORN is not required for this system.**

If "Yes," enter Privacy Act SORN Identifier 1703.03 AAFES

Date of submission for approval to Defense Privacy Office
Consult the OGC-C Privacy Manager for this date. May 2019

C. Does this information system or electronic collection have an Office of Management & Budget (OMB) Control Number? [If unknown, contact OGC-C Privacy Manager].

☒ **Yes**

Enter OMB Control Number 0702-0135

Enter Expiration Date June 30, 2019

☐ **No**

D. Authority to collect information. Please list the Federal law, Executive Order of the President (EO), or regulation which authorizes the collection and maintenance of a system of records. [If unknown, contact OGC-C Privacy Manager]

(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 information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.) i.e. Title 10 U.S.C. § 7013, "Secretary of the Army".

(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) The Exchange may use Exchange Operating Procedures, Exchange Standards of Operations, or CEO Guidance as the primary authority. The requirement, directive, or instruction implementing the statute within the Exchange should 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.

E. Summary of 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 information system or electronic collection.

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 sensitive positions.

(2) Briefly describe the types of personal information about individuals collected in this system.

Pending and completed personnel security clearance actions; briefing/debriefing statements for special programs, sensitive positions; other related information and documents required in connection with personnel security clearance determinations to include the individual's full name, Social Security Number (SSN), DoD ID Number, job location, position, and supervisor's name, home address and phone number, mobile number, personal financial information, reason for departure, and clearing offices' approval.

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

Data leakage of information is low. The Exchange has implemented the highest level of security controls and the system is assessed against Center for Internet Security (CIS) Configuration Baselines. Configuration scans are conducted monthly to monitor compliance. the Exchange secures information in secured buildings and behind controlled areas accessible only to employees with a right-to-know who have been screened, cleared for access, and have a role-based position for which places them in an arrangement that requires servicing, reviewing, or updated records.

F. With whom will the PII maintained in this system be shared? (i.e., other DoD Components, Federal Agencies)? Indicate all that apply. Questions should be coordinated with OGC-C Privacy Manager.

☒ **Within the Exchange.**

Specify. Exchange Executive Group Force Protection; Attorney Staff, Office of the Inspector General, Loss Prevention

☒ **Other DoD Components.**

Specify. Department of Defense; U.S. Criminal Investigation Command, Inspector Generals

☒ **Other Federal Agencies.**

Specify. Office of Personnel Management

☒ **State and Local Agencies.**

Specify. State/Local/Federal Law Enforcement Agencies/Attorneys

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

Specify. National Background Investigation Bureau (NBIB)

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

Specify. Private Attorneys and Staff; Foreign Law Enforcement, Intelligence and/or security agencies, Previous Employers, Financial Institutions and Credit Bureaus.

G. Do individuals have the opportunity to object to the collection of their PII (opt-out)?

☒ **Yes** ☐ **No**

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

Web-based environments provide individuals with the Privacy Act Statement showing the routine uses of disclosure. 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 for the Exchange.

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

n/a

H. 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.

Information is provided 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. information provided is not used in a means for which is not collected.

I. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

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

☐ **Exchange Privacy Policy** ☐ **None**

☒ **Other**

Describe each applicable format listed above.	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 sensitive positions. 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 http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx. Information may be released to Federal agencies based on formal accreditation as specified in official directives; regulations; to Federal, State, Local, and Foreign Law Enforcement, Intelligence, or Security agencies in connection with a lawful investigation under their jurisdiction. 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. A copy of the Privacy Impact Assessment (PIA) for the collection of information may be located at https://www.aafescom/about-exchange/public-affairs/FOIA/assessments.htm. SYSTEM OF RECORDS NOTICE (SORN): 1703.03, "Personnel Security Clearance Case Files;" https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/Army-Article-List/ 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. AUTHORIZATION AND CONSENT TO CRIMINAL HISTORY INVESTIGATION I hereby authorize the investigative agency conducting my background to obtain such reports from other federal, state, local entities, previous employers, references, or other businesses or individuals to be used for verification. I hereby authorize the investigative agency to obtain reports from any consumer reporting agency for my employment purposes or contractual relationships with the Exchange. I realize that any security freeze on my consumer or credit report may affect the completion of this investigation. To avoid such occurrences, I should request that freezes be lifted while the investigation is pending. I realize that collection of my Social Security Number (SSN) is authorized by United States

Executive Order 9397. My SSN is needed to identify my unique records I realize that I am not required to disclose my SSN, but failure to do so may prevent or delay the processing of my background investigation.

I hereby acknowledge that the voluntary completion of the following information will be used with my requesting access to a Department of Defense (DOD) facility in accordance with HPD-12 credentialing and the Exchange EOP 66-04. I understand that assignment exceeding 6 (six) months require re-verification by Force Protection and every 6 (six) months thereafter until my service is no longer required.

NOTE:

Sections 1 and 2 above will be posted to the Exchange'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.

The Exchange may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.