EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

Exchange Security Clearance Web-Based Portal/Storage
Army & Air Force Exchange Service - Force Protection

Questions relative to this document should be directed to the Exchange HQ Information Technology Governance Risk Management or to the Exchange Office of General Counsel, Compliance Division by mail to 3911 S. Walton Walker Blvd., Dallas, TX 75236.

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 completed PIA should be directed to the system owner, to the IT-Government (IT-G) representative, and to the Office of General Counsel, Compliance Division (OGC-C).

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 system owner. A copy should also be directed to IT-G and to OGC-C.

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 IT-G or OGC-C.

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 AAFES 1703.03

Date of submission for approval to Defense Privacy Office
Consult the OGC-C for this date. July 2016

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

☒ **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]

(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. § 3013, "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.

Title 10, U.S.C. 3013, Secretary of the Army; Title 10 U.S.C. 8013, Secretary of the Air Force; Army Regulation 215-8/Air Force Instruction 34-211(I), Army and Air Force Exchange Service Operations; Army Regulation 380.67, Personnel Security Program; Air Force Instruction 31-501, Personnel Security Program Management; Department of Defense 5200.02-R, Personnel Security Program (PSP); 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 eligibility for access to classified information or assignment to a sensitive position. Records are used by Exchange executives for adverse personnel actions to include removal from sensitive duties, removal from employment, denial to a restricted or sensitive area, and revocation of security clearance. Records are also used to ensure that departing employees have been properly out-processed.

(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.

The main risk is data leakage. In order to address such a risk the Exchange maintains the records in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) with an official "need to know" who are responsible for servicing the record in performance of their official duties. Persons are properly screened and cleared for access.

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.

☒ **Within the Exchange.**

Specify. Exchange Force Protection, Attorney Staff, IG Staff

☒ **Other DoD Components.**

Specify. Department of Defense; Defense Manpower Data Center (DMDC)

☒ **Other Federal Agencies.**

Specify. National Background Investigations Bureau (NBIB)

☒ **State and Local Agencies.**

Specify. State/local law enforcement entities and attorneys.

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

Specify.

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

Specify. Private attorneys, authorized third parties, foreign law enforcement, intelligence security agencies.

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.

Individuals are provided the Privacy Act Statement which includes the use and routine disclosures of the information they voluntarily provide to the Exchange. The individual has the authority to stop processing or completion of the on-line form at any time prior to pressing submission. Choosing not to divulge their personal information will deny that individual proper clearance to work with 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 an individual's security clearance to access governmental facilities and systems. The collected data is required in order for a vendor or contractor to work for or with the Exchange. Information provided is not used in a means for which it was not collected. Inaccurate or incomplete data may affect or delay the clearance of the individual.

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	AGENCY DISCLOSURE NOTICE The public reporting burden for this collection of information is estimated to average 40 minutes per response, including the time for reviewing instructions, searching existing data

listed above.

sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Directives Division, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100 (0702-0135). 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.

PLEASE DO NOT RETURN YOUR RESPONSE TO THE ABOVE ADDRESS.

Responses should be sent to the Exchange EG-FP at 3911 South Walton Walker Blvd., Dallas, TX 75236-1598.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, U.S.C. 3013, Secretary of the Army; Title 10 U.S.C. 8013, Secretary of the Air Force; Army Regulation 215-8/Air Force Instruction 34-211(I) Army and Air Force Exchange Service Operations; Army Regulation 380.37, Personnel Security Program; Air Force Instruction 31-501, Personnel Security Program Management; Department of Defense 5200.2-R, "Personnel Security Program; Air Force Instruction 31-401, Information Security Program Manager; E.O. 12065 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 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. Disclosures pursuant to 5 U.S.C. 552a (b)(12) may be made from this system to "consumer reporting agencies" as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) for use in verification purposes in fitness for Federal employment, clearance to perform contractual services and/or eligibility, and for sensitive positions or access to classified information.

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.

INSTRUCTIONS

Information collected on the following pages will be used to determine your acceptability as an individual working under a Federal contractual relationship, Federal employment, Federal assignment, or as a result of an interservice support agreement. You may be asked to complete information at any time during the hiring process. Please follow all instructions provided to you by your Exchange contract official, human resource representative, or Exchange Force Protection or Loss Prevention offices.

If selected and before appointed, you will be asked to review, update and recertify that your answers are true. A false statement on any part of this application or submitted attached documents, forms or sheets may be grounds for not hiring you, or for terminating your employment or contractual relationship with the Exchange. In addition, false statements may be punished by a fine or imprisonment. U.S. Code, title 18, section 1001

Type your responses on the proposed web form for any questions containing an asterisk. Should you have questions while completing, please contact your Exchange representative.

We recommend that you keep a photocopy of your completed form for your records.

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 form 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.

I read the preceding and hereby authorize and consent to the investigative agency gathering information for verification of my suitability for employment and/or performance of contractual services.

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.