EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

Exchange Personnel Systems
Exchange Human Resources

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 0401.04
Date of submission for approval to Defense Privacy Office Consult the OGC-C for this date.	September 2021

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	0702-0129, 0702-0131, 0702-0133, 0702-0139
Enter Expiration Date	01/22/22, 03/31/22, 05/31/22, 10/31/22

☐ **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.

10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; 42 U.S.C. 659, Consent by United States to Income Withholding, Garnishment, and Similar Proceedings for Enforcement of Child Support and Alimony Obligations; 31 CFR 285.11, Administrative Wage Garnishment; DoD Directive 7000.14-R, DoD Financial Management Regulation; DoD Instruction 1400.25, Volume 1408, DoD Civilian Personnel Management System: Insurance and Annuities for Non-appropriated Fund (NAF) Employees; Army Regulation 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.

A. To populate and maintain a repository of documentation of the history and status of an individual's employment relationship with the Exchange . B. To provide a basic source of factual data of a person's Federal employment while as an active Exchange associate and after his or her separation for the purpose of administer, compute, monitor, and report employee personnel actions such as pay entitlements and transactions, grade increases, length of service and incentive/honor awards and recognitions, performance ratings, disciplinary actions, training, benefit enrollment and payouts, annuities and retirement, bonds due and issued, taxes paid, employee debts, leave accrued and usage, and employment separation and outsourcing. C. To determine an employee's qualification and eligibility for promotion and/or transfer. D. To capture and maintain individual job applicants' essential job skills and aptitudes for consideration and hiring determinations for open Exchange positions worldwide. D. To administer proper health care, medical treatment, and processing of claims for employees who become ill or are injured during working hours. E. To process official travel requests for Exchange civilian employees including data to determine eligibility

of associates' dependents for travel, obtain necessary clearance where foreign travel is required, assisting employees in applying for passports and visas, and counseling here proposed travel includes visiting or transiting to communist counties and danger zones.
F. To provide locator and emergency notification data.
G. To maintain information on participates in the Exchange tuition assistance program.
H. To obtain data to verify employment and wages.
I. To provide data in support of Equal Employment Opportunity Program requirements.
J. To answer inquiries, process claims, administer and investigate complaints, grievances, and appeals.
K. To respond and process payments to Court and Regulatory Bodies requests for information or garnishment orders such as Qualifying Domestic Relations Orders (QDRO) or compliance with Child Support, Alimony obligations, Federal and Commercial (civil) debts, or tax levies.
L. To produce managerial report and statistical analysis of Exchange work force strength trends and composition in support of established man-hours, projected staffing requirements, and budgetary programs and procedures

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

A. Personal and Biographical Information, such as individual full name, date of birth, Social security Number (SSN); age; gender; marital status; race, hair color, color of eyes, height and weight; sex; citizenship and place of birth; disability; contact information such as mailing/physical address, e-mail address, phone numbers; emergency contact information; legal representative name and contact data; Drivers' License data and personal automobile license plate number.
B. Employment Information, such as past employer's name and contact information; application for employment and academic transcripts; previous and current position/grade/rank; past and present salary/ wages; Department of Defense Identification Number (DoD ID Number); Military history to include branch of service; mobility plans; travel orders; time records; supervisory approvals and delegations; leave requests; personnel actions such as transfers, pay increases/decreases; awards; disciplinary actions and reprimands, and like documents; time records; training; change of duty documents; security and clearance documents.
C. Financial Information, such as bank name, bank account number, routing number, check numbers; Exchange pay documents such as pay-stubs; tax documents such as W2, W4; Garnishment Orders and payments; unemployment data requests; indebtedness papers.
D. Benefit and Retirement Information, such as benefit enrollment information, 401K balances, retirement estimates, annuities, and like documents.
E. Medical Information, such as physical examination documents, Workers' Compensation Claims; medical diagnosis and treatment plan; prescription documentation; adjuster notes and legal advice; payments for medical services and claims; copies of DOL reports; and regulated documents/reports.
F. Travel Information, such as requests and approvals, Temporary Duty Changes and Official Change of Duty Station documents to include authorized leave in-route, shipment of household and personal goods, travel expense vouchers, Visa and passports information.

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

Risks involve possible data leakage in the form of inappropriate release of information or Cyber Security intrusions attempts to access, manipulate, or even destroy records.

AAFES adopts DoD policies, rules, and procedures to protect data within this system. To secure the data, AAFES use of controls to minimizes the risk of compromise of personally identifiable information (PII) and enforces access to those with the appropriate clearances. AAFES has established security audits and accountability procedures/ policies that support the safeguarding of PII and the detection of potential PII incidences. AAFES routinely employees safeguards such as multi-factor log-in procedures, physical and technological access controls governing access to the data, network and disk encryption, safeguard encryption keys, making sensitive data, mandatory employee training on information assurance and privacy, identification marking, detection and electronic alert and intrusion detective systems for access to services and network infrastructure. Physical access to the network or to

working stations is secured with a two-point access procedure and offices maintaining equipment are further protected by key locks and security guards.

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. Human Resource; Loss Prevention; Financial; Benefits; Office of the General Counsel; Equal Employment Opportunity & Diversity, Supervisors, Management, Hearing Examiner; Inspector General; Time Keepers

☒ **Other DoD Components.**

Specify. Dept of the Army; Dept of the Air Force; Office of Special Investigations; Inspector General Offices

☒ **Other Federal Agencies.**

Specify. Dept of Justice; Federal Bureau of Investigation; U.S. Treasury; U.S. Dept of Labor; Dept of State, Office of Personnel Management; National Archives and Records Administration; U.S. Equal Employment Opportunity Commission; Social Security Administration; United States Forces Korea and Japan; U.S. Garrisons

☒ **State and Local Agencies.**

Specify. Law Enforcement Agencies; State Child Support Agencies; Law Offices; Courts; attaché or law enforcement authorities of foreign countries; Department of Transportation; Host Country Authorities;

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

Specify. IBM, First Advantage®, Kenexa; AETNA, Hartford, and other Insurance/Benefit providers; AAFES Trust; Contract Claims Services, Inc.; Willis Tower Watson; Plus Relocation; Military Airlift Command (MAC) Transportation; Transportation Contractors

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

Specify. Congress; Banking and Financial Institutions; Private Attorney Law Offices; Souse/Ex-Spouse; Dependents; Family Members; Survivors; Medical Providers and Facilities; Educational Institutions; Ticket Services

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.

Information is voluntarily provided. During the collection, individuals are provided a Privacy Act Notice with the consequences of choosing not to provide the information requested. Not providing all the information could result in not being offered a position of employment, not being approved for official travel or change in duty station, having inappropriate or no insurance benefits, excessive time in outsourcing, denied reimbursement funds for tuition, etc.

(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 collected is used for the purposes as listed previously in section E1 of this document and not used in a means for which it was 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.	The Privacy Act provided at the collection may differ based on the collective instrument. Each will contain the appropriate authority to include Title 10 U.S.C. 7013 and 9013, AR 215-8/AFI 34-211(I), and E.O. 9397 (SSN) as amended. Additionally, the following authorities apply to some systems: 42 U.S.C. 659, Consent by United States to Income Withholding, Garnishment, and Similar Proceedings for Enforcement of Child Support and Alimony Obligations; 31 CFR 285.11, Administrative Wage Garnishment; DoD Directive 7000.14-R, DoD Financial Management Regulation; DoD Instruction 1400.25, Volume 1408, DoD Civilian Personnel Management System: Insurance and Annuities for Non-appropriated Fund (NAF) Employees. The Principal purpose per the collected documents is identified in Section E1 of this form and provided as part of the applicable Privacy Act Statement on the collective instrument.

Routine Use(s) may vary slightly on each collective instrument but will minimally consist of the following: 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. This includes disclosure to Federal, State, local, territorial, tribal, international, or foreign agencies.

Additionally, the OMB Agency Disclosure Notice is provided on the collective instrument (form or via electronic means) on any collective instrument which requires an OMB approval.

Lastly, individuals accessing a third party site for which collect information on behalf of AAFES under contract agreements are afforded that contractors Privacy Policy. One such contractor is IBM. Their privacy policy may be viewed at https://www.ibm.com/privacy/details/us/en/.

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.