EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

AAFES Asset Protection Information System (APIS)
AAFES Loss Prevention

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	0409.01
Date of submission for approval to Defense Privacy Office Consult the OGC-C for this date.	07 OCT 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	0702-0138
Enter Expiration Date	30 SEP 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.

10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; 29 CFR, Part 1960, Basic Program Elements for Federal Employee OSHA and Related Matters; Army Regulation 215-8/AFI 34-211(I), Army and Air Force Exchange Service Operations; Title 29 CFR, Part 1960, Basic Program Elements for Federal Employee OSHA and Related Matters; Federal Claims Collection Act of 1966 (Pub.L. 89-508, as amended); Debt Collection Act of 1982 (Pub.L. 97-365, as amended), as codified in 31 U.S.C. §3711, Collection and Compromise; 31 CFR 285.11, Administrative Wage Garnishment; E.O. 12196, Occupational Safety and Health Programs for Federal Employees; DoD Instruction 1330.21, Armed Services Exchange Regulations; DoD 7000.14-R, Department of Defense Financial Management Regulation Volume 13, Nonappropriated Funds Policy and Volume 16, Department of Defense Debt Management; Army Regulation 27-20, Chapter 4, Legal Service Claims; Air Force Instruction 51-501 implementing Air Force Policy Memorandum AFPD51-5, Section A, Administrative Claims; 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.

The primary purpose of this collection is to gather all the required data and details from individuals at the time, or soon thereafter, of an alleged incident occurring at or on an Exchange facility/property. This may include accidents, injuries, illnesses, mishaps, fires, shoplifting, or issues involving damages to government property involving Exchange employees, patrons (customers), guests, visitors or contractors. The Exchange uses information collected to complete the investigation relative to the incident, provide victim medical treatment, pay claims, recoup damages to assets and property, correct deficiencies, and probable civil or criminal prosecution action. Information may be included in managerial and statistical reports which are used in maximizing Exchange earnings by reducing losses through proper security measures and prevention of shoplifting and employee thefts.

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

This system maintains personal information on employees which is accessed through Exchange HR databases or personal information on patrons, visitors, contractors, or individuals who may be near or close to Exchange locations which are either involved or witnesses to incidents. Personal information may include the individual's facial appearance, video surveillance coverage, full names, home addresses, home phone numbers, e-mail addresses, Social Security Numbers or other number which identifies the individual, DOD ID number, physician reports, witness statements, and investigatory reports/notes. Information may also include other personal information for which may be included within an accident or incident report.

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

The Exchange has reviewed the safeguards established for the system to ensure they are compliant with DoD requirements. Data leakage of information is low. The highest level of security controls and system were implemented and accessed against the Center for Internet Security (CIS) Configuration Baselines. Configuration scans are conducted monthly to monitor compliance. Information is 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 updating the 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.

☒ **Within the Exchange.**

Specify. Office of Loss Prevention, Office of General Counsel, Inspector General, Human Resources, Hearing Examiner, EEOC, Approved Supervisors/ Managers

☒ **Other DoD Components.**

Specify. Department of the Army, Department of the Air Force, Inspector General Offices, Office of the Special Investigations.

☒ **Other Federal Agencies.**

Specify. Department of Justice, Federal Bureau of Investigations, Department of Labor, US Attorney and his/her staff, National Archives and Records Administration

☒ **State and Local Agencies.**

Specify. State and Local Law Enforcement Agencies and Attorneys; courts

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

Specify. Aetna, Fidelity, Contract Claims Holdings, Inc.

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

Specify. Private attorney offices, insurance providers, Congress

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.

When individuals are in a face-to-face interview for information they maintain an option of withdrawing their consent to provide personal information. In the event information is provided that is either not completely true or intentionally misrepresents the facts could constitute grounds for employment separation or disciplinary action. In severe cases, not providing information or providing false information may lead to civil or criminal prosecution.

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

Individuals hired for a federal civilian position with the Exchange have a duty to cooperate with investigations and a duty to avoid impeding investigations as a condition of employment. (Exchange Operating Procedures 16-1)

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 a requirement for use in procedures relative to internal and external investigations, court proceedings, and health issues. The system contains individually identifiable health information. The DoD Health Information Privacy Regulation (DoD 6025.18-R) issued pursuant to the Health Insurance Portability and Accountability Act of 1996 applies to most such health information. This regulations may place additional procedural requirements on the uses and disclosures beyond those found in the Privacy Act of 1974 or mentioned in the system of records notice associated with this system.

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.	When providing information on statements, individuals are provided an Agency Disclosure Notice which includes the Privacy Act Statement and instructions on completion of their statement. The Privacy Act Statement may also be provided to the individual through verbal communication by an official Exchange associate such as a Loss Prevention Officer or management staff. Individuals who are employed by the Exchange may be directed to review the Exchange Operating Procedures 16-1 regarding the Confidentiality Statement and Witness Advisory Warning. Individuals, whether employed or not, who submit a written statement will sign after reading the following text: "I have made this statement freely without hope of benefit or reward, without the threat of punishment and without coercion, influence or inducement. I further states that I have read the entire statement, initialed all pages and corrections, and that it is correct and true as written. Furthermore, I understand that refusal to provide information/concealment or misrepresentation of material facts in a report of statement will constitute grounds for separation for cause or other disciplinary action." A copy of the individual statement (unless it would impede an open investigation) is provided to the individual upon request. Individuals may also request their statement by placing a Privacy Act Request with the Exchange Office of General Counsel.

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.