EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

Sensitive Personal Health Data
Safety, Security, Human Resources

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	AAFES 0409.01 and AAFES 0405.11
Date of submission to Army Privacy for coordination of approval from the Defense Privacy Office Consult the OGC-C Privacy Manager for this date.	June 2013 and April 2003 respectfully

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	0702-0138
Enter Expiration Date	10/31/2022

☐ **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. 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); 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, 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.

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.

Data maintained in this electronic system is collected through other AAFES approved systems, such as time records or incident reports. The purpose for the collection of basic health issues on associates, patrons, vendors, contractors /vendors is to provide "need to know" information to Official DoD officers or local/state/ federal Health authorities who are responsible for the health and welfare of individuals for the purpose of attaining statistical date or to trace infectious diseases and/or illnesses.

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

Information maintained within this system contain the individual's name; gender; contact information, including mail address, e-mail address, home and cell phone numbers; name of injury or illness; estimated date or actual date of exposure or onset of injury of illness; duty station or area for which the individual was exposed or contracted injury/illness/disease; doctor's diagnosis including data on testing and treatment; and associated notes relative to the illness/disease.

(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 spillage to individuals without an official right-to-know. AAFES has implemented high levels of security protocols and they system is routinely checked against the Center for Internet Security (CIS) Configuration Baselines. Configuration scans are conducted monthly or more frequently to monitor compliance.

Records are maintained in secured buildings and behind controlled areas restricted by the use of locks, guards, access cards, and accessible only to authorized personnel. Access to records is limited to person(s) with an official "need to know" who have been screened, cleared for access, and have a role-based position which places them in an arrangement that requires servicing, reviewing, or updating data.

This system has been protected to avoid unauthorized access. Users access is secured to reveal only partial data. Only a small handful of designated and approved individuals have access to complete information for administrative and reporting purposes.

F. With whom will the PII maintained in this system be shared? (i.e., other DoD Components, Federal Agencies)? Indicate all that apply. Please list directorates or positions, not names. Questions should be coordinated with OGC-C Privacy Manager.

☒ **Within the Exchange.**

Specify. HR Staff; LP Staff; Health and Security; Office of GC; General Managers

☒ **Other DoD Components.**

Specify. Army, Air Force,

☒ **Other Federal Agencies.**

Specify. Department of Labor, Department of Health and Human Services, Department of Justice, Office of Management and Budget, Department of Veterans Affairs

☒ **State and Local Agencies.**

Specify. Local, State, Foreign Health and Human Service Agencies

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

Specify.

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

Specify. Contract Claims Services, Inc.; Insurance Providers, Physicians, Hospitals, and Medical Care Facilities

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.

n/a

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

Information is already within AAFES systems. Data is not collected for the purpose of this electronic system directly from the individual.

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.

Disclosures are minimal containing only specific data required for the purpose of statistical analysis or health and human service protocols approved by either an United States Presidential Executive Order or other applicable federal regulation. Statistical releases and notices to possible affected individuals will be disclosed without personal identifiable information.

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 Privacy data was originally supplied to the individual during the original onset of the collection

each applicable format listed above.	for this data under other AAFES collections. This data is maintained through those systems vice directly provided by the individual. These systems are covered under AAFES SORN 0409.01 "Incident and Accident Reports", AAFES SORN 0405.11 "Individual Health Records", and AAFES HR SORNS to include but not all exclusive to AAFES SORN AAFES 0703.07 "AAFES Employee Pay System Records".