PRIVACY IMPACT ASSESSMENT (PIA)

For the

Exchange Credit Program
Army & Air Force Exchange Service (Exchange)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

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

☐ **New DoD Information System** ☐ **New Electronic Collection**

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

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐ **Yes, DITPR** Enter DITPR System Identification Number

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☒ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

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**

If "Yes," enter Privacy Act SORN Identifier AAFES SORN 0702.34

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(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 DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(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) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Title 10 U.S.C. §3013, Secretary of the Army; Federal Claims Collection Act of 1966 (Pub.L. 89-508, as amended); Debt Collection Act of 1982 (Pub.L. 97-365, as amended), as amended by the Debt Collection Improvement Act of 1996 (Pub.L. 104-134, section 31001); 31 CFR 285.11, Administrative Wage Garnishment; DoD 7000.14-R, Volume 13 Department of Defense Financial Management Regulation, "Nonappropriated Funds Policy"; Army Regulation 215-8/Air Force Instruction 34-211(I), Army and Air Force Exchange Service Operations;, and E.O. 9397 (SSN), as amended.

g. Summary of DoD 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 DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose: To process, monitor, and post audit accounts receivable, to administer the Federal Claims Collection Act, and to answer inquiries pertaining thereto. To collect indebtedness and determine customer's patron's eligibility to cash checks at Exchange facilities.

Types of Personal Information Collected in System: Individual's name, address, SSN, telephone number, cell number, work number, date of birth, gender, number of dependents, military branch of service, pay grade, and ETS/EOS date, bank and saving account numbers, bank names, Magnetic Ink Character Recognition Number (MICR), e-mail address, Exchange credit account number, monthly salary, other monthly income; name of spouse, spouse's monthly income and spouse's SSN; representative name, address and telephone number; authorized user's names, address, SSN, date of birth, gender, and relationship to account holder; returned checks, transaction data including items purchased, ATM/Debit/ Credit card numbers and receipts; credit scores from credit reporting bureaus; salary/travel advances; military commander's name and business address; pecuniary liability claims; pay adjustment authorizations; and account statements.

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

Risk involved includes data leakage. Safeguards in place to protect PII include the following. Records are maintained 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. Access to computerized data is role-based and further restricted by passwords, which are changed periodically. Credit card information is also subject to the Data Security Standards (DSS) promulgated by the Payment Card Industry (PCI) Security Council.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Exchange Directorates/Associates: Fraud, Attorneys, Paralegals, FA Associates/Mgr., HRM, HRSC, Loss Prevention, Inspector General

☒ **Other DoD Components.**

Specify. DOA IG, DOAF IG; Office of Special Investigators

☒ **Other Federal Agencies.**

Specify. Dept of Justice, US Attorney, Internal Revenue Service, Dept of Treasury, FBI, U.S. Postal Service Inspectors

☒ **State and Local Agencies.**

Specify. Employers, State and Local Government, State Employment Offices, Child Support Services

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

Specify. Transworld Systems, Inc. (TSI); Special Provisions provided in contract to safeguard personally identifiable information.

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

Specify. Private collection agencies; employers; consumer reporting agencies, former spouses for use in payments under Title 10 U.S.C. 1408; Legal Authorities, Civilian attorneys, U.S. Bankruptcy Courts

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

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

Individuals are provided a Privacy Act Statement along with the routine disclosures. Individuals have an option of halting application process. This is available through the on-line, paper application, or through an authorized/designated Exchange point of sale register. Failure to provide all the requested information or halting the application process may result in the denial of credit.

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

n/a

j. 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.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Pursuant to the Privacy Act of 1974, information collected may be disclosed and used for government debt

purposes, legal issues, regulated reporting to the credit bureaus, to the Department of Treasury for tax purposes and treasury offsets relative to debt.

Individuals must consent in writing to the disclosure of their information to non-exempt third parties. Information may be disclosed to exempt third parties for appropriate reasons pursuant to the Privacy Act of 1974.

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

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

☒ **Other** ☐ **None**

Describe each applicable format.

Privacy Act Statement:
AUTHORITY: Title 10 U.S.C. §3013, "Secretary of the Army"; "Federal Claims Collection Act of 1966" (Pub. L. 89-508, as amended); "Debt Collection Act of 1982" (Pub. L. 97-365, as amended); 31 CFR 285.11, "Administrative Wage Garnishment"; DoD 7000.14-R, "Department of the Defense Financial Management Regulation"; Army Regulation 215-8/AFI 34-211(I), "Army and Air Force Exchange Service Operations"; and Executive Order 9397 (SSN), as amended.

PRINCIPAL PURPOSES(S): To process, monitor, and post audit accounts receivable, to administer the Federal Claims Collection Act, and to answer inquiries pertaining thereto. To collect indebtedness and determine patron's eligibility to cash checks at Exchange facilities. To collect indebtedness and determine patron's eligibility to cash checks at Exchange facilities.

ROUTINE USE(S): Your 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 the Department of the Treasury, and a debt collection agency with which the United States has contracted for collection services to recover debts owed to the United States. To any employer (person or entity) that employs the services of others and that pays their wages or salaries, where the employee owes a delinquent nontax debt to the United States. The term employer includes, but is not limited to, State and local governments, but does not include any agency of the Federal Government. To consumer reporting agencies pursuant to 5 U.S.C. 552a(b)(12) as defined in the Fair Credit Reporting Act (14 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). The purpose of this disclosure is to aid in the collection of outstanding debts owed to the Federal government; typically to provide an incentive for debtors to repay delinquent Federal government debts by making these debts part of their credit report. The disclosure is limited to information necessary to establish the identity of the individual, including name, address, and taxpayer identification number (Social Security Number); the amount, status, and history of the claim; and the agency or program under which the claim arose for the sole purpose of allowing the consumer reporting agency to prepare a commercial credit report. This disclosure will be made only after the procedural requirement of 31 U.S.C. 3711(f) has been followed.

DISCLOSURE: Voluntary, however, failure to provide all the requested information may result in the denial of your application for inadequate data.

Agency Disclosure Notice:
The public reporting burden for this collection of information is estimated to average 6 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 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, Information Management Division, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100 (0702-XXXX).

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 your local Exchange retail facility, to the Exchange office whom provided you the application or the update, or to the Exchange Military Star at the Army and Air Force Exchange Service, 3911 South Walton Walker Blvd., Dallas, TX 75236-1598.

NOTE:

Sections 1 and 2 above are to be posted to the Component'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.

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