EXCHANGE

PRIVACY IMPACT ASSESSMENT (PIA)

Workers Compensation Claims
Exchange Office of General Counsel

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 0405.11

Date of submission for approval to Defense Privacy Office
Consult the OGC-C for this date. November 2014

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

Enter Expiration Date Exempted

☒ **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 215-1, "Military Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities "; 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.

To process workers' compensation claims and provide health care and medical treatment to employees who become ill or are injured during working hours.

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

This system contains the name of the associate who was hurt or injured, their Social Security Number, organizational location, date of birth, medical data recorded by treating nurse/physician, information provided by individual's personal physician regarding diagnosis, prognosis, and return to duty status. The system may contain the individual's emergency contact name, phone number (home, cell and work) and address. Information relative to third party names and insurance claim numbers may be provided in investigatory documents pertaining to research of past insurance claims.

This system of records 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. DoD 6025.18-R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in the system of records notice associated with this system.

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

The main privacy risk associated with this system is data leakage. The Third Party Administrator complies with the Privacy Act of 1974 and the Department of Defense rules and regulations issued under this Act for the design, development, or operation of this system. Claim documents are maintained by Contract Claims Services, Inc. (CCSI). Medical records kept at health facilities (OCONUS areas only) are maintained in a dispensary controlled by the medical staff. Access to records is permitted only to assigned case workers, legal professionals, or medical providers. 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. Human Resource Team; Office of the General Counsel, EEODI

☒ **Other DoD Components.**

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

☒ **Other Federal Agencies.**

Specify. Department of Labor, Department of Justice, EEOC, Office of Workers' Compensation Appeals Board, Office of Administrative Law Judges, FBI

☒ **State and Local Agencies.**

Specify. State and Local law enforcement and governmental agencies

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

Specify. Contract Claims Services, Inc. - Contract provides protection of PII

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

Specify. Retained outside legal counsel; foreign governmental officials

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.

Individuals are provided a Privacy Act Statement and HIPAA documents when accessing medical treatment. As government civilian employees, Exchange associates are obligated as part of their duty to provide information so claims can be processed correctly.

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.

PII is used for verification and identity purposes. PII may be disclosed pursuant to applicable rules, statues, or regulations.

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.	Privacy Act Statement: Title 10 U.S.C. 3013, "Secretary of the Army"; Title 10 U.S.C. 8013, "Secretary of the Air Force"; Army Regulation 215-1, "Military Morale, Welfare, and Recreation Activities and Nonappropriated Fund Instrumentalities "; Army Regulation 215-8/AFI 34-211(I), "Army and Air Force Exchange Service Operations"; and E.O 9397 (SSN), as amended. Appropriate Health Insurance Portability and Accountability Act of 1996 (HIPAA) documents: Pursuant to the Privacy Act, 5 U.S.C. §552a and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), I hereby voluntarily authorize the Army and Air Force Exchange Service (hereinafter "the Exchange") or their Third Party Administrator (TPA) to use or disclose my Employment and Personal Health Information (PHI) to the following for the purpose of (description of injury or illness). Appropriate medical providers are regulated by law to provide the associate with specific HIPAA documents.

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.