



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

SharePoint System

US Army Communication Electronics Command (CECOM)

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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.

10 U.S.C. 3013, Secretary of the Army;  
Department of Defense Directive 8500.1, Information Assurance (IA);  
DoD Instruction 8500.2, Information Assurance Implementation;  
AR 25-1, Army Knowledge Management and Information Technology;  
Army Regulation 25-2, Information Assurance; and E.O. 9397 as amended (SSN).

**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.

The SharePoint System is an application that maintains unclassified electronic files. Some files contain personally identifiable information, such as budget/financial information, evaluations, time & attendance, organizational charts, etc. The intent is to use this system to maintain both working and finalized official records. The application is comprised of a number of screens for capturing data and sharing information both internally and externally.

Type of PII that will be stored on the SharePoint System includes: personal, military, educational, employee, financial, medical and work-related information.

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

Risk: PII location  
Mitigation: PII data is maintained internally within restricted folders, which can only be accessed by a selected group of people.

Risk: Electronic access to records  
Mitigation: 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. Access to computerized data is role-based and further restricted by passwords, which are changed periodically.

Risk: PII Physical location  
Mitigation: PII data is maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Facility is equipped with alarms, cameras, and personnel on around the clock.

**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.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

Lockheed Martin Integrated Systems - "The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

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

Specify.

**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.

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

The system is used to maintain official electronic records that are required, such as budget/financial, evaluations, time & attendance, etc. Records containing PII information such as Budget/Finance and Time & Attendance are pulled from other systems which collect PII information.

**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.

There are specific personnel records that are required to be maintained, which contain PII information. Such information is necessary for their employment with the Government (i.e., payroll, time & attendance, etc.).

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 is provided with the online registration form. Users can not access their information without reading first.

Privacy Act Statement:

Authority: 10 U.S.C. 3013, Secretary of the Army; Department of Defense Directive 8500.1, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; AR 25-1, Army Knowledge Management and Information Technology; Army Regulation 25-2, Information Assurance; and E.O. 9397(SSN).

PRINCIPAL PURPOSES: Information is created and maintained for routine business operations. The types of Personally Identifiable Information collected is personal information and employment information.

Routine Use: None. The DoD 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

DISCLOSURE: Voluntary. However, if the user fails to provide the information requested, access will not be granted.

**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.

**SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW**

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

**(1) What PII will be collected?** Indicate all individual PII or PII groupings that apply below.

- Name  Other Names Used  Social Security Number (SSN)
- Truncated SSN  Driver's License  Other ID Number
- Citizenship  Legal Status  Gender
- Race/Ethnicity  Birth Date  Place of Birth
- Personal Cell Telephone Number  Home Telephone Number  Personal Email Address
- Mailing/Home Address  Religious Preference  Security Clearance
- Mother's Maiden Name  Mother's Middle Name  Spouse Information
- Marital Status  Biometrics  Child Information
- Financial Information  Medical Information  Disability Information
- Law Enforcement Information  Employment Information  Military Records
- Emergency Contact  Education Information  Other

If "Other," specify or explain any PII grouping selected.

**(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?**

Information is collected from the Army Time and Attendance Pay System (ATAPS) and from the General Fund Enterprise Business System (GFEBS). New information may be collected from email or paper necessary for employment and employee records.