



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Communications-Electronics Research, Development, and Engineering Center (CERDEC SharePoint Portal)

US ARMY RDECOM CERDEC

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

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.

A0690-200 DAPE

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 690-200, General Personnel Provisions; and E.O. 9397 (SSN), as amended.

K890.21 DoD

5 U.S.C. 301, Departmental Regulations; Pub. L. 106-229, Electronic Signatures in Global and National Commerce; OASD (C3I) Policy Memorandum, subject: Department of Defense (DoD) Public Key Infrastructure (PKI); and OASD (C3I) Memorandum, subject: Common Access Card (CAC).

A0025-1 CIO G6

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), 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.

The Communications, Electronics, Research, Development, and Engineering Center's (CERDEC) SharePoint implementation is an electronic collection of documents, including existing Personally Identifiable Procedure (PII) information, which is stored across an access-controlled, primary SharePoint site (the Gateway) and numerous "team" sites that offer a collaborative location for smaller groups. This environment replaces CERDEC's shared drives as an electronic repository for information. To safeguard PII, designated sub-repositories (Gateway V-drives and team sites) are locked down to ensure that only authorized users with a 'need to know' will have access to the PII information contained therein.

The PII stored within the CERDEC SharePoint implementation is contained in already existing repositories, and uploaded by Human Resources, Budget, Operations, and various Supervisory personnel within the organization's science and engineering areas. File types include: Microsoft Word, Excel and Access files as well as SharePoint lists.

PII collected includes personal, employment, educational, financial, supervisory, and security clearance information stored within the aforementioned file types.

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

Data is available for view by the members of each PII approved CERDEC SharePoint Portal.

Risk: Physical extraction from PII 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.

Risk: Electronic access by non-approved personnel
Mitigation: Each approved PII site in the CERDEC SharePoint Portal will be locked down to specific personnel with "need to know". Each user will authenticate to the SharePoint Portal using Active Directory (CAC/PKI) or AKO Single Sign On.

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 - Administrators of the SharePoint hosting will have access to all SharePoint sites. "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, as amended, 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.

As an electronic collection of PII any opportunity to object to the collection of PII would already have occurred, and no further objection to the consolidation of PII will be provided.

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.

Individuals cannot give or withhold consent because the Gateway will serve as merely a repository of information already collected. Any consent issues were addressed at the time of collection.

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.

The CERDEC SharePoint Portal is not being used to collect PII from users. It will house information which has been collected through other sources, listed in section 3-a-(2).

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.