



PRIVACY IMPACT ASSESSMENT (PIA)

For the

PEO STRI MC - PEO STRI MANAGEMENT CENTER

Program Executive Office for Simulation, Training and Instrumentation (PEO STRI)

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;
Army Regulation 25-1, Army Information Technology;
Army Regulation 25-2, Information Assurance;
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 STRI Management Center is a web-based, secure knowledge management system linked from the AKO to facilitate the collection, organization, and distribution of explicit and tacit knowledge throughout the Army's systems acquisition community. It is a vehicle for sharing and innovation. Functional work-flowed applications, along with a robust search engine, COTS e-mail, team tools, PDAs and instant messengers provide internal/external users with an encrypted site for conducting business based on access-level controls. Primarily the Management Center is the repository for PEO STRI's Share Point collaboration center.

The ORLD_FL_ALT_01 PEO STRI IPN is the server room which provides unclassified automation support to the STRI Management Center. It includes a portion of the leased space in the Research Commons Building, utilities, file servers, SAN storage and backup servers, network infrastructure, hardware and software maintenance, technical refresh of data center components, NIPRNET circuits, and network operations personnel who operated and support the Data Center. The Data Center houses Sun Servers driving the MC web Servers and the Oracle database engine. Windows servers provide LAN support and drive PEO STRI specific training and simulation support applications. In addition to supporting the STRI Management Center, the Data Center supports Share Point, PD2/PRweb, APIMs, MOSS CDRLvue and other applications required by the PEO STRI acquisition workforce.

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

Every system has the potential for information to become compromised and accessible by individuals without an official need-to-know, whether through conventional hacking techniques, lost media, or intentionally by an insider. The system has implemented the latest cyber security safeguards to reduce an outside attack and lower the risk of lost electronic media. Every individual who has access to the system, with regards to using the entered data, has undergone a security background review and privacy and security training. Access to the system is controlled by the Common Access Card (CAC).

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.

NCI Inc - Contractor performing IT sensitive duties subject to investigative and assignment requirements IAW AR 25-2 and affiliated regulations.
ECS Inc. - SETA contractor assisting the PEO STRI government staff manage and administer programs within the PEO.
All PEO STRI Staff, including these and other contractor employees who have appropriate clearances and access to the SKC in support of PEO STRI operations.

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.

This is a requirement of their job and related information is needed especially since all personnel working for PEO STRI require a minimum Secret Clearance. This would be an requirement by the owner of the users information and a Privacy notice or any other related information that is required to notify the users about their information being requested. There is NO requirement to give any PII information to operate on the PEO STRI network.

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.

PII fields in the user site are optional fields that they can share with others if they would like.

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

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

- | | |
|--|--|
| <input type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Use/access to the PEO STRI IPN does ask users or require users to supply any PII information to operate on the system and validation that they possess a Secret Clearance.

If any PII information is requested from their leadership or organization a Privacy Act Statement and any other required documentation should be supplied to the user before any information is taken. This information should be stored on a site that that is permission based to be protected.

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.