



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Security Control and Administrative Tool (SCAT)
---

Defense Logistics Agency (DLA) / Defense Logistics Information Service (DLIS)
---

### 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.

S500.55, entitled "Information Technology Access and Control Records."

Authority to collect information: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; 18 U.S.C. 1029, Access device fraud; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees, 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 SCAT program facilitates management of user accounts for DLA / DLIS applications.

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

Users, including individuals responsible for system maintenance, receive initial and periodic refresher Privacy Act and Information Assurance training. Users are trained to lock their workstations when leaving them unattended, to shut down computers when leaving at the end of the duty shift and to be alert to third parties entering the workspace.

SCAT servers are kept in a secure, limited access, or monitored work areas accessible only to authorized personnel. Data is backed up daily for reconstruction of the records should the system fail. Access to the servers is Public Key Infrastructure (PKI) controlled.

Computers are Common Access/Smart Card (CAC) enabled requiring a valid certificate and a Personal Identification Number (PIN). Computer screens automatically lock after a preset period of inactivity. Systems manually locked by the user can only be unlocked by inserting the Common Access/Smart Card (CAC) and entering the Personal Identification Number (PIN).

**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.

The records may also be used by law enforcement officials to identify the occurrence of and assist in the prevention of computer misuse and/or crime.

**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.

**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.

In the privacy act statement the disclosure states, "Disclosure is voluntary; however, if you fail to supply all the requested information you will not gain access to the DLA/DLIS Applications. Your identity/security clearance must be verified prior to gaining access to the DLA/DLIS Applications, and without the requested information verification can not be accomplished.

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

**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.

In the privacy act statement the disclosure states, "Disclosure is voluntary; however, if you fail to supply all the requested information you will not gain access to the DLA/DLIS Applications. Your identity/security clearance must be verified prior to gaining access to the DLA/DLIS Applications, and without the requested information verification can not be accomplished.

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

[Empty rectangular box]

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:** 5 U.S.C. 301, Departmental regulations; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; 18 U.S.C. 1029, Access device fraud; E.O. 10450 Security Requirements for Government Employees, as amended; and E.O. 9397 (SSN).

**Purpose(s):** Information is used to control and track access to DLA-controlled networks, computer systems, and databases. The records may also be used by law enforcement officials to identify the occurrence of and assist in the prevention of computer misuse and/or crime. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation, or reporting purposes.

**Routine Uses:** Data may be provided under any of the DoD "Blanket Routine Uses" published at <http://www.defenselink.mil/privacy/notices/blanket-uses.html> .

**Disclosure:** Disclosure is voluntary; however, if you fail to supply all the requested information you will not gain access to the DLA/DLIS Applications. Your identity/security clearance must be verified prior to gaining access to the DLA/DLIS Applications, and without the requested information verification can not be accomplished.

**Rules of Use:** Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S500.55, entitled "Information Technology Access and Control Records" available at <http://www.defenselink.mil/privacy/notices/dla> .

**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.