



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Business System (EBS)

Defense Logistics Agency (DLA)

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.

Authority: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 31 U.S.C. 3512, Executive Agency Accounting and other Financial Management reports and plans, as amended by Published Law 104-208, Federal Financial Management Improvement Act of 1996; and E.O. 9397 (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 purpose of the DoD information system or electronic collection is to facilitate interconnection and transfer data biweekly from the Defense Civilian Payroll System (DCPS) to EBS for internal accounting and labor processing. The interface files contain personally identifying information such as Social Security Number (SSN) and name as well as financial information. Other information required for accounting and labor processing that will be included in the interface includes Federal and State tax information, time and attendance data, employee address, and information on payroll deductions.

Records are used to initiate reimbursements to enable the Defense Finance and Accounting Service (DFAS) to distribute payments to DLA employees for certain miscellaneous out-of-pocket expenses (training, tuition, Permanent Change of Station, etc). Records are also used to identify employee-related costs associated with reimbursable orders received by DLA and to enable accurate billing of those reimbursable orders.

Records are used to create a general ledger file containing the accounts necessary to reflect DLA operational costs. Operations costs consist of operating accounts, liability accounts, budgetary accounts, and statistical accounts, maintained for the purposes of establishing, in summary form, the status of the DLA accounts and to provide an audit trail to verify accuracy of reports.

Records are used by financial management offices to validate and accurately record employee-labor operational expenses.

Records are used to determine DLA civilian payroll budgetary requirements.

Records are used by internal auditors to conduct audits or investigations into the DLA accounting and financial management process.

Records are used by the DOD Components who receive accounting and financial management support from DLA under an administrative support agreement for accounting and financial management purposes.

Records devoid of personal identifiers are used for extraction or compilation of data and reports for management studies and statistical analyses for use internally or externally as required by DOD or other government agencies.

Statistical data, with all personal identifiers removed, may be used by management for program evaluation, review, or oversight purposes.

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

The risk associated with the PII collected is the unauthorized disclosure of stated information. The sensitivity categorization of data exchanged between EBS and DCPS based on FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and the guidance in NIST SP 800-60 is Moderate. Therefore, the security of the information being passed between EBS and DCPS is protected through the use of, at a minimum, FIPS 140-2 approved encryption algorithms. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

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.

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 information is vital for internal accounting and labor processing.

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.

The sources of the data are DLA and DFAS databases. Data does not come from the individual.

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

Describe each applicable format.

Data does not come from the individual.

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.