



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Employee Activity Guide for Labor Entry (EAGLE)

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 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

0704-0452

Enter Expiration Date

02/28/2017

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.

S340.10 -- 5 United States Code (USC) Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 31 U.S.C., Chapter 35, Accounting and Collection; and E.O. 9397 (SSN), as amended.

S375.80 -- 5 United States Code (U.S.C.) Ch. 65 "Telework," as added by Public Law 111-292 "Telework Enhancement Act 2010"; DoD Instruction 1035.1, "Telework Policy for Department of Defense"; and DLA Instruction 7212, "Defense Logistics Agency Telework Program."

S900.50 -- 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 41 U.S.C. 405a, Uniform Federal Procurement Regulations and Procedures; and FAR Part 16.601(b)(1), Time-and-Materials, Labor-Hour, and Letter Contracts.

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.

EAGLE provides DLA with a single IT system to collect data on DLA Civilians for the purpose of tracking time and attendance and alternate worksite / telework records to include overtime and leave hours, to track accounting information and workload / project activity for analysis and reporting purposes; for statistical reporting on leave and overtime use patterns, number of employees teleworking, etc.; and for costing capabilities.

Information is provided through database feeds from the Defense Finance and Accounting Service (DFAS) and the Defense Civilian Personnel Advisory Service (DCPAS) for the purpose of issuing payroll and providing information required for the approval and maintenance of telework requests. Civilian employee personally identifiable information (PII) maintained includes the individual's name, social security number, user ID, date of birth, citizenship, pay rate, leave balances, position, title, series, grade, last performance rating, telework eligibility, and official worksite address / phone number.

Additionally, as part of the telework request process, users complete all data elements of the DLA telework request forms which includes their alternate worksite address and phone number.

For DLA Military members and DLA contractors data is collected for the purpose of tracking workload / project activity for analysis and reporting purposes, time and attendance, and labor distribution data against projects for management and planning purposes; to maintain management records associated with the operations of the contract; to evaluate and monitor the contractor performance and other matters concerning the contract. Military employee and contractor PII maintained include individual's name and User ID.

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

Threats: Records and disks are maintained in limited access or monitored work areas with access limited to those individuals requiring access to perform official duties. Physical entry by unauthorized persons is restricted by the use of locks, guards, or administrative procedures. Computer terminals are controlled with Common Access Cards (CAC), and computer screens automatically lock after a preset period of inactivity with re-entry controlled by Common Access Cards (CAC). Individuals accessing this system of records are to have taken Information Assurance and Privacy Act training.

Dangers: There are no dangers in providing notice of the collection or allowing an individual to object/ consent. Therefore, individuals are given this opportunity at times of notice publication and data collection via a Privacy Act Statement. Individuals are free to raise objections if new threats are perceived.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

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.

Privacy Act systems of records notices have been published in the Federal Register with a 30 day public comment period. The EAGLE application screen that collects personal data will contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. Individuals may raise an objection with the HQ DLA Privacy Act office during the comment period, during data collection, or at any time thereafter.

(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.

Privacy Act systems of records notices were published in the Federal Register with a 30 day public comment period. Forms that collect personal data will contain a Privacy Act Statement, as required by 5 U.S.C. 552a (e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the HQ DLA Privacy Act office during the comment period, during data collection, or at any time after the program is launched.

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

Describe each applicable format.

On the EAGLE web application for DLA civilian employee time and attendance:

Authority: 5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 31 U.S.C., Chapter 35, Accounting and Collection; and E.O. 9397 (SSN).

Purpose(s): Records are used to prepare time and attendance records, to record employee pay rates and status, including overtime, the use of leave, and work absences; to track workload, project activity for analysis and reporting purposes; for statistical reporting on leave and overtime use/usage patterns, number of employees teleworking, etc.; and to answer employee queries on leave, overtime, and pay. Information from this system of records is provided to the Defense Finance and Accounting Service for the purpose of issuing payroll to DLA civilian employees.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: The DoD "Blanket Routine Uses" set forth at <http://dpclo.defense.gov/Privacy/SORNsIndex/DODComponentNotices/Preamble/DLAPreamble.aspx> apply to this system.

Disclosure is Voluntary: Providing the requested data is voluntary. However, failure to provide all the data requested may result in the inability to prepare civilian time and attendance records for payroll purposes.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S340.10, entitled "DLA Civilian Time and Attendance, Project and Workload Records."

~~~~~

On the EAGLE web application for DLA civilian employee alternate worksite / telework records:

Systems of Record Notice S375.80  
Authority: 5 United States Code (U.S.C.) Ch. 65 "Telework," as added by Public Law 111-292 "Telework Enhancement Act 2010"; DoD Instruction 1035.1, "Telework Policy for Department of Defense"; and DLA Instruction 7212, "Defense Logistics Agency Telework Program."

Purpose(s): Information may be used by supervisors, program coordinators, DLA Information Operations and DLA Human Resources Services, Human Resources Information Systems for managing, evaluating, and reporting DLA Alternate Worksite/Telework Record activity/participation. Information on participation in the Telework Program, minus personal identifiers, is provided in management reports and to the DOD for a consolidated response to the Office of Personnel Management (OPM) annual data call. Portions of the records may also be used to validate and reimburse participants for costs associated with telephone and internet usage.

Routine Use: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To the Department of Labor when an employee is injured while teleworking, e.g., details of the arrangement may be disclosed. To DLA-affiliated unions to provide raw statistical data on the program. Disclosed information may include number of positions designated as eligible for telework by job title, series and grade; number of employees requesting telework; number approved for Telework by the local activity. No personal identifiers or personally identifying data is provided. Pursuant to DOD Blanket Routine Uses 1, 4, 6, 9, 12, 13 and 15.

Rules of Use: Rules for collection, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S375.80, entitled "DLA Civilian Time and Attendance, Project and Workload Records" available at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570255/s37580.aspx>

~~~~~  
On the EAGLE web application for DLA Contractors and Military Personnel:

Authority: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 5 U.S.C. Chapter 61, Hours of Work; Chapter 53, Pay Rates and Systems; Chapter 57, Travel, Transportation, and Subsistence; and Chapter 63, Leave; 41 U.S.C. 405a, Uniform Federal Procurement Regulations and Procedures; and FAR Part 16.601(b)(1).

Purpose(s): For the purpose of tracking workload / project activity for analysis and reporting purposes, time and attendance, and labor distribution data against projects for management and planning purposes; to maintain management records associated with the operations of the contract; to evaluate and monitor the contractor performance and other matters concerning the contract.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To the contractor's employer for the purpose of resolving any discrepancy in hours billed to Defense Logistics Agency in accordance with FAR Clause 16.601 (b)(1). Records released include individual's name, User ID, position, company, project and workload records, time and attendance, regular and overtime work hours and leave hours. The DoD "Blanket Routine Uses" set forth at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DODComponentNotices/Preamble/DLAPreamble.aspx> apply to this system.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in DLA Privacy Act System Notice S900.50, entitled "Labor Hours, Project and Workload Records."

Office of Management and Budget (OMB): In accordance with the Paperwork Reduction Act, EAGLE has received OMB approval; control number: 0704 – 0452 Title: Project Time Record System.

AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information.

Send comments regarding this burden estimate or any other aspect of this collection of information,

including suggestions for reduction the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, Information Management Division, 4800 Mark Center Drive, Alexandria, VA 22350-3100 (0704-0452).

Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

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.