PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

EMPLOYEE ACTIVITY GUIDE FOR LABOR ENTRY (EAGLE)

2. DOD COMPONENT NAME:

Defense Logistics Agency

3. PIA APPROVAL DATE:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and 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.; for costing capabilities; and for processing of Human Resources requests from employees and serviced agencies. Information is provided through database feeds from Defense Civilian Payroll System (DCPS) and Defense Civilian Personnel Data System (DCPDS) for the purpose of issuing payroll, servicing human resource requests, and providing information required for the approval and maintenance of telework requests. Civilian Employee 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, official worksite address / phone number, home address, and retirement/benefit information. 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. Additionally, as part of the leave request process, users complete all data elements of the DLA leave request forms which includes leave hour codes, reason codes, date, time, and total hours requested. 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.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Verification, identification, authentication, data matching, and mission-related use as described above.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The EAGLE application screens that collect personal data 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. If no objections are received, consent is presumed. Individuals may raise an objection with the DLA Privacy Office during the before or during data collection, or any time thereafter.

For data entered by HR Specialists on behalf of employees requesting assistance: employees have the option to not provide the necessary information which would result in the their issue not being addressed.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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 EAGLE application screens that collect personal data 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. The Privacy Act Statement describes the authorized purposes (or uses) of the information being collected. If no objections are received, consent is presumed. Individuals may raise an objection with the DLA Privacy Office during the before or during data collection, or any time thereafter.

For data entered by HR Specialists on behalf of employees requesting assistance: employee may decline to provide contact information which would prevent HR from conducting follow-up actions with the employee.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

1. 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 the 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 our 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 of Records Notice S340.10, entitled "DLA Civilian Time and Attendance, Project and Workload Records" available at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570251/s34010/

2. On the EAGLE Web Application for DLA Civilian Employee Alternate Worksite / Telework Records:

Authority: 5 U.S.C. Chapter 65, Telework, as added by Public Law 111-292 "Telework Enhancement Act 2010"; DOD Instruction 1035.01, "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 annual data call. Portions of the records may also be used to validate and reimburse participants for costs associate with telephone and Internet usage.

Routine Uses: 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 identifiable 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 the DLA Privacy Act System of Records Notice S375.80, entitled "DLA Alternate Worksite/Telework Records" available at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Wide-SORN-Article-View/Article/570255/s37580/

3. 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 64, Leave; 41 U.S.C. 405a, Uniform Federal Procurement Regulations and Procedures; and FAR Part 16.601(b)(1).

Purpose(s): For the purposes 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 the 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 and Routine Uses" set forth at http://dpclo.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 the DLA Privacy Act System of Records Notice S900.50 entitled "Labor Hours, Project and Workload Records" available at http://dpclo.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570277/s90050/

OMB CONTROL NUMBER: 0704-0452
OMB EXPIRATION DATE: 2/29/2020

AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information is estimated to average 15 minutes per response, including 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 reducing the burden, to the Department of Defense, Washington Headquarters Services, Executive Services Directorate, 4800 Mark Center Drive, East Tower, Suite 02G09, 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 current valid OMB Control Number.

4. On the EAGLE web application for DLA civilian employee HR work order records:

Authority: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 & 10 U.S.C. Part II, Personnel; and 5 U.S.C. 301, Departmental Regulations.

Purpose: Information about current and former Federal employees is collected to conduct routine Human Resources operations. We will use the data to process HR requests from employees and serviced agencies; and for reporting, financial forecasting, tracking, monitoring, assessing, and payment reconciliation purposes. Statistical data, with all personal identifiers removed, may be used by management for program evaluation and review.

Routine Uses: In addition to those disclosures generally permitted by 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/BlanketRoutineUses.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 OPM Gov-1 entitled "General Personnel Records" available at http://dpclo.defense.gov/Privacy/SORNs.aspx

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X]	Within the DoD Component	Specify.	Defense Logistics Agency
[X]	Other DoD Components	Specify.	Defense Finance and Accounting Service, Defense Civilian Personnel Advisory Service
[X]	Other Federal Agencies	Specify.	Office of Personnel Management, Department of Labor

☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	External to DLA/DOD: Records regarding contractor information is disclosed outside DLA/DOD for the purpose of resolving any discrepancy in hours billed to DLA with the contractor 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.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☐ Databases
☒ Existing DoD Information Systems
☐ Commercial Systems
☐ Other Federal Information Systems

Using the EAGLE Web site, the DLA Payroll Centers of Excellence Customer Service Representatives add DLA civilian employee records to EAGLE (Name, SSN). EAGLE automatically generates a unique identifier (User ID). Other data is automatically transferred from the Defense Finance and Accounting Service Defense Civilian Payroll System to EAGLE (birth date, citizenship, and financial information to include annual salary, hourly rate, and leave balances.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Face-to-Face Contact
☐ Paper
☐ Fax
☐ Telephone Interview
☒ Information Sharing - System to System
☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier S340.10, S375.10, S900.50, and OPM/GO

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 2.4, Item 030 (DAA-GRS-2016-0015-0003), GRS 2.3, Item 081

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Time & attendance, leave requests, and leave approvals are destroyed after GAO audit or when 3 years old, whichever is sooner (DLA Record Schedule 5300.16, GRS 2.4 Item 030 (DAA-GRS-2016-0015-0003). Alternate worksite / telework records are destroyed 1 year after

employee's participation in the program ends; unapproved requests are destroyed 1 year after the request is denied (DLA Record Schedule 8120.11.02, GRS 2.3 Item 081 (DAA-GRS-2015-007-0022). Labor Hours and Metrials Surveillance Records are destroyed when 6 years 3 months old or when no longer needed (DLA Record Scheduled 5000.79 (N1-361-08-5). Human Resources work orders are destroyed when no longer needed.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN S340.10 - 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, Department 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).

SORN S375.10 - Authority: 5 U.S.C. Chapter 65, Telework; DOD Instruction 1035.01, Telework Policy; and DLA Instruction 7212, DLA Telework Program.

SORN S900.50 - Authority: 5 U.S.C. 301, Department 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).

OPM Gov-1, General Personnel Records - Authority: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107 & 10 U.S.C. 301, Departmental Regulations.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0452, exp. 2-28-2017 (Renewal is currently pending).

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)**?** (Check all that apply)*

☐ Biometrics	☒ Birth Date	☐ Child Information
☒ Citizenship	☒ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☐ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☐ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☒ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☐ Place of Birth	☒ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☒ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

Foreign Nationals - Foreign Nationals (aka Local Nationals) may only have the following information stored in EAGLE and they may only have the system role of "Timekeeper and Certifier." Foreign National permissible information is: a system-generated unique identifier, CAC ID Number, and system role in EAGLE (Timekeeper and Certifier). NOTE: Foreign Nationals may not have their Time and Attendance tracked within EAGLE.

Employee official duty station, alternate worksite address, telephone numbers.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☒ Yes ☐ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

February 15, 2018.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Interaction with Financial Institutions - Financial institutions may require that individuals provide the SSN as part of the process to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions.

Computer Matching - Systems, processes, or forms that interact with other government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

Visibility has been minimized through encryption and displaying the SSN in plain text to DLA Human Resources payroll customer service representatives (CSR) only. As DLA employees, CSRs are made aware of the restrictions on secondary uses of the data records through initial and refresher Annual Information Assurance and Privacy training.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

While visibility of the SSN has been minimized, until such time as other systems to which EAGLE interfaces with eliminate their use of the

SSN, the SSN will be required in EAGLE.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☒ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☐ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☐ If Other, enter the information in the box below

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☐ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☒ Firewall
- ☐ Role-Based Access Controls
- ☒ Virtual Private Network (VPN)
- ☒ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☐ Used Only for Privileged (Elevated Roles)
- ☐ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☐ External Certificate Authority Certificates
- ☒ Least Privilege Access
- ☒ User Identification and Password

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Physical: Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel requiring badges.
Technical: The system on which the EAGLE application resides has been fully certified and accredited under DOD 8500.01, Cybersecurity. Security and privacy controls, in accordance with DLA policy, are documented in the Electronic Mission Assurance Support Service (eMASS) system. In compliance with the DISA Database STIG (System Technical Information Guidance), audit event logs are maintained on the databases for user accountability and activity. 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 CAC.
Administrative: EAGLE restricts application access by using a group access policy managed by EAGLE system administrators. Each user has an account defined which identifies the user's access level which include general users, administrators, supervisors, timekeepers, and managers. Users, including individuals responsible for system maintenance, are to have received initial and periodic refresher Privacy Act and Information Assurance training. Users are warned through logon procedures of the conditions associated with access and the consequences of improper activities. Users are required to accept those conditions/consequences before logon completes. 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. Only those with a need-to-know actually get access to the Privacy data maintained within the system.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	8561
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[ ]	Yes, RMF tool	RMF tool Identification Number	
[ ]	No		

If “No,” explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, “Risk Management Framework for DoD Information Technology”.

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	10/3/2017
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[ ] Yes [X] No

If "Yes," Enter UII _____ If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.e., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Rebecca Landstreet	(1) Title	EAGLE Program Manager
(2) Organization	DLA Information Operations, J62FA	(3) Work Telephone	(571) 767-3988
(4) DSN	392-767-3988	(5) E-mail address	Rebecca.Landstreet@dla.mil
(6) Date of Review	08/21/18	(7) Signature	LANDSTREET.REBECCA.ANNE.1245178464 Digitally signed by LANDSTREET.REBECCA.ANNE.1245178464 Date: 2018.08.21 14:21:51 -04'00'
b. Other Official *(to be used at Component discretion)*	Frank Yacono	(1) Title	Supervisory HR Specialist
(2) Organization	DLA Human Resources, Systems	(3) Work Telephone	717-770-5280
(4) DSN	771-5280	(5) E-mail address	Frank.Yacono@dla.mil
(6) Date of Review	08/29/18	(7) Signature	YACONO.FRANK.S.1263590143 Digitally signed by YACONO.FRANK.S.1263590143 Date: 2018.08.29 10:59:26 -04'00'
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Lewis Oleinick	(1) Title	Chief Privacy and FOIA Officer
(2) Organization	J67C, Information Governance & Compliance	(3) Work Telephone	571-767-6194
(4) DSN		(5) E-mail address	Lewis.Oleinick@dla.mil
(6) Date of Review	10/17/18	(7) Signature	OLEINICK.LEWIS.W.1286751934 Digitally signed by OLEINICK.LEWIS.W.1286751934 Date: 2018.10.17 10:30:58 -04'00'

e. Component Records Officer	Cecilia Wiker	(1) Title	DLA Records Officer
(2) Organization	DLA Information Operations, J67C, Strategic Data Services	(3) Work Telephone	269-961-4846
(4) DSN	661-4846	(5) E-mail address	Cecilia.Wiker@dla.mil
(6) Date of Review	08/06/18	(7) Signature	WIKER.CECILIA.M.1032295130 Digitally signed by WIKER.CECILIA.M.1032295130 Date: 2018.08.06 08:53:24 -04'00'
f. Component Senior Information Security Officer or Designee Name	Gregory Crowell	(1) Title	Information System Security Manager
(2) Organization	Cybersecurity Program Management , J612	(3) Work Telephone	(385) 519-8344
(4) DSN	(313) 350-8344	(5) E-mail address	gregory.crowell@dla.mil
(6) Date of Review:	08/29/18	(7) Signature	CROWELL.GREGORY.LEWIS.1170662888 Digitally signed by CROWELL.GREGORY.LEWIS.1170662888 Date: 2018.08.29 05:08:49 -10'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name	Kathy Cutler	(1) Title	Chief Information Officer
(2) Organization	DLA Information Operations	(3) Work Telephone	571-767-2100
(4) DSN		(5) E-mail address	Kathy.Cutler@dla.mil
(6) Date of Review		(7) Signature	CUTLER.KATHY.D.1229501662 Digitally signed by CUTLER.KATHY.D.1229501662 Date: 2018.10.25 11:08:45 -04'00'

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.