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 8561

☐ **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 S340.10 and S900.50

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	02/29/2012

☐ **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 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), as amended.

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 tracking time and attendance data 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/usage patterns, number of employees teleworking, etc.; and for costing capabilities. Information is provided through database feeds from the Defense Finance and Accounting Service for the purpose of issuing payroll to DLA civilian employees. Civilian employee personally identifiable information (PII) maintained includes the individual's name, Social Security Number, User ID, date of birth, citizenship, pay rate, and leave balances.

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 area 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. Defense Logistics Agency

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. External to DLA/DoD: Records regarding contractor information is disclosed outside of DLA/DoD for the purpose of resolving any discrepancy in hours billed to DLA with the contractor's 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. 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. If no objections are received, consent is presumed.

(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. If no objections are received, consent is presumed.

(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.

- ☒ **Privacy Act Statement**
- ☐ **Privacy Advisory**
- ☐ **Other**
- ☐ **None**

Describe each applicable format.

On the EAGLE web application for DLA Civilian Employees:

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://www.defenselink.mil/privacy/notices/dla/dla_preamble.shtml 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 Notice S340.10, entitled "DLA Civilian Time and Attendance, Project and Workload Records" available at http://www.defenselink.mil/privacy/notices/dla/S340-10.shtml

~~~~~~

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://www.defenselink.mil/privacy/notices/dla/dla_preamble.shtml 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" available at http://www.defenselink.mil/privacy/notices/dla/S900-50.shtml

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.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☐ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☒ Birth Date	☐ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☒ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.	Foreign Nationals – Foreign Nationals (aka, Local Nationals, LN) may only have the following information stored in EAGLE and they may only have the system role of "Timekeeper & Certifier." Foreign National permissible information is: a system generated unique identifier, the Foreign National's CAC identification number, and the Foreign National's system role in EAGLE (i.e., "Timekeeper & Certifier.") NOTE: Foreign Nationals may not have their time and attendance tracked within EAGLE.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Using the DLA EAGLE website. the DLA Payroll Centers of Excellence (COE) Customer Service Representatives (CSRs) 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 (DFAS) Defense Civilian Payroll System (DCPS) to EAGLE (Birth Date, Citizenship, and Financial Information to include Annual Salary, Hourly Rate, and Leave Balances).

Using the DLA EAGLE Web site, the COEs or EAGLE Site Administrators can add contractor or military employee records to EAGLE (Name). EAGLE automatically generates a unique identifier (User ID).

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☒	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

DLA Civilian Social Security Numbers (SSNs) are required for payroll processing in the Defense Civilian Payroll System (DCPS). DLA Civilian pay rates are used to support costing capabilities in EAGLE. DLA Civilian leave balances are available to the employee and to the employee's supervisor for verification of leave usage before certification of the time and attendance records.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

The use of this PII data is for mission-related use and DLA Civilian payroll processing.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☐ **Contractors**

☒ **Other**

The DLA Payroll Centers of Excellence (COEs) have access to DLA Civilian employee's social security numbers for payroll processing. DLA individuals with the approved roles have access to DLA Civilian reports on workload, hours, and costs. Costs are determined using the employee's pay rate.

NOTE: Developers assist with trouble-shooting, improvements, and enhancements. Therefore they may have access to live data during the process of repair or upgrades. Developers are authorized IT personnel who have the appropriate Security Clearance.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒	**Security Guards**	☒	**Cipher Locks**
☒	**Identification Badges**	☐	**Combination Locks**
☒	**Key Cards**	☐	**Closed Circuit TV (CCTV)**
☐	**Safes**	☐	**Other**

(2) Technical Controls. Indicate all that apply.

☒	**User Identification**	☐	**Biometrics**
☐	**Password**	☒	**Firewall**
☐	**Intrusion Detection System (IDS)**	☒	**Virtual Private Network (VPN)**
☒	**Encryption**	☒	**DoD Public Key Infrastructure Certificates**
☐	**External Certificate Authority (CA) Certificate**	☒	**Common Access Card (CAC)**
☐	**Other**		

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☐ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	April 16, 2009
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Individual's information is collected during the course of normal resource management functions throughout their employment.
Use, Retention, and Processing: Only those with a "need to know" can access an individual's PII data. Information is used for planning and establishing program goals and requirements, accounting, workload and project tracking, life cycle management, and time and attendance activities. This system provides the ability to quickly collect automated data and statistics reflecting program and project metrics, and facilitate the analysis and reporting of the data. Information is also used to identify tasks against projects or monitor contract phases for management purposes.
Disclosure: No other personnel other than those with a "need to know" can access an individual's PII information.
Destruction: Data/records are destroyed after 6 years as per DLA Records Schedule.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Data Controls:

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: System on which the EAGLE application resides has been fully certified and accredited under DoD 5200.40, DoD Info Technology Security Certification and Accreditation Process. Information Assurance (IA) controls, in accordance with DLA policy, are documented in the Mission Assurance Support Service (eMASS) for Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). In compliance with DISA DATA BASE STIG (System Technical Information Guidance), audit event logs are maintained on the data bases 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 Common Access Cards (CAC).

Administrative: EAGLE restricts application access by using a group access policy which is managed by EAGLE's system administrators. Each user has an account defined which identifies the user's access level which include general users, administrators, supervisors, timekeepers, and managers, etc. 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 log-on 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.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	HILBISH.JANET.Z.1229151696 Digitally signed by HILBISH.JANET.Z.1229151696 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=HILBISH.JANET.Z.1229151696 Date: 2011.11.07 14:55:16 -05'00'
Name:	Janet Hilbish
Title:	EAGLE Project Manager
Organization:	DLA Information Operations at Ogden
Work Telephone Number:	717-770-5500
DSN:	771-5500
Email Address:	janet.hilbish@dla.mil
Date of Review:	10/31/2011
Other Official Signature (to be used at Component discretion)	WESTENSKOW.SHARON.M.1231477159 Digitally signed by WESTENSKOW.SHARON.M.1231477159 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=WESTENSKOW.SHARON.M.1231477159 Date: 2011.11.07 13:24:10 -07'00'
Name:	Sharon Westenskow
Title:	Information Assurance Manager
Organization:	DLA Information Operations at Ogden
Work Telephone Number:	801-586-0325
DSN:	586-0325
Email Address:	sharon.westenskow@dla.mil
Date of Review:	11/4/2011

Other Official Signature (to be used at Component discretion)	CHARLESWORTH.JEFFREY.J.1231479119 Digitally signed by CHARLESWORTH.JEFFREY.J.1231479119 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=CHARLESWORTH.JEFFREY.J.1231479119 Date: 2011.11.07 13:50:47 -07'00'
Name:	Jeff Charlesworth
Title:	Director, DLA Information Operations at Ogden
Organization:	DLA Information Operations at Ogden
Work Telephone Number:	801-586-0300
DSN:	586-0300
Email Address:	jeff.charlesworth@dla.mil
Date of Review:	11/7/2011
Component Senior Information Assurance Officer Signature or Designee	
Name:	Sharon Westenskow
Title:	Information Assurance Manager
Organization:	DLA Information Operations at Ogden
Work Telephone Number:	801-586-0325
DSN:	586-0325
Email Address:	sharon.westenskow@dla.mil
Date of Review:	Signed 2 blocks above
Component Privacy Officer Signature	OLEINICK.LEWIS.W.1286751934 Digitally signed by OLEINICK.LEWIS.W.1286751934 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=OLEINICK.LEWIS.W.1286751934 Date: 2012.02.21 17:07:30 -05'00'
Name:	Lewis Oleinick
Title:	Chief Privacy and FOIA Officer
Organization:	DLA General Counsel
Work Telephone Number:	703-767-6194
DSN:	427-6194
Email Address:	Lewis.Oleinick@dla.mil
Date of Review:	21 Feb 2012

Component CIO Signature (Reviewing Official)	FOSTER.ROBERT.T.1106256027 Digitally signed by FOSTER.ROBERT.T.1106256027 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DLA, cn=FOSTER.ROBERT.T.1106256027 Date: 2012.02.23 22:51:18 -05'00'
Name:	Robert T. Foster
Title:	Acting Director, DLA Information Operations, Chief Information Officer
Organization:	DLA Information Operations (J6)
Work Telephone Number:	703-767-2100
DSN:	427-2100
Email Address:	Robert.Foster@dla.mil
Date of Review:	23 February 2012

Publishing:

Only Sections 1 and 2 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: pia@osd.mil.

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 Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.