PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Loss Prevention (DLP) System
Defense Logistics Agency

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 SORN not required. PII not retrieved by personal 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 PII not directly collected from any individual.

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.

5 USC 552a, Sections (e)(6) and (e)(10) , and Pub. L. 112-81, div. A, title IX, Sec. 922, Dec. 31, 2011, 125 Stat. 1537.

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.

In order to detect and remediate unsecured PII throughout its information life-cycle -- whether on share drives, in e-mails, or transmitted through websites -- DLA has implemented a risk reduction strategy using Data Loss Prevention (DLP) technologies. DLP technology aids the DLA Enterprise in enforcing existing DLA and DoD policies for the safe and secure collection, maintenance, use, and dissemination of personal information (PII).

The DLP technologies, as an incidental by-product during the detection and prevention processes, will provide the information assurance and/or privacy officer with a "snap shot" of the detected PII to facilitate remediation and appropriate safeguard measures are implemented.

The DLP technologies core components include "Data-at-Rest" to minimize the risk of PII being lost, stolen, or compromised while that PII is controlled, maintained, or stored on an applicable information system operated by DLA such as an unencrypted spreadsheet on a share file system. Another core component of DLP is "Data-in-Motion" to detect and prevent loss of PII by way of e-mail or by websites such as common social networking sites.

The purposes of the DLP technology are to:
(1) Minimize the risk of unsecured PII being stored on shared spaces within the DLA internal network and thereby minimize the risk of that PII ever being lost, stolen, or compromised to anyone outside of DLA.
(2) Minimize the risk of unsecured e-mail and internet communications both within the DLA internal network and to external recipients; thereby minimizing the risk of that PII being lost, stolen or compromised to anyone outside of DLA.
(3) Minimize the risks of unsecured storage and management of sensitive files residing on information system endpoints that reside internally within the DLA office locations and externally to support our mobile workforce; thereby minimizing the risk of that PII being lost, stolen or compromised to anyone outside of DLA.
(4) Maximize DLA compliance with the Privacy Act of 1974, as amended; the Federal Information Security Management Act of 2002; OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information;" DoD 5400.11-R, "DoD Privacy Program Regulation," Appendix 1, "Safeguarding Personally Identifiable Information;" DoDI 8500.2, "Information Assurance (IA) Implementation;" NIST SP 800-53, Rev 3., "Recommended Security Controls for Federal Information Systems and Organizations;" and CNSS Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems."

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

DLA has applied administrative, physical, and technical safeguards to address the privacy risks associated with the collection of unsecured PII the DLP technologies detect.

ADMINISTRATIVE

DLA is limiting the DLP technology to detect only unsecured instances of SSNs -- DLP technologies are not accurate enough to detect other types of PII with sufficiently high accuracy and to search for other types of PII would result in unnecessary collection, storage and maintenance of associated PII in the DLP system. DLA has ensured that access to the DLP technology is controlled through a documented and controlled administrative process whereby only those Privacy and Information Assurance Officers with a need to access the DLP as a part of their remediation duties are granted access -- all requests for access must be approved by a supervisor responsible for the Privacy or Information Assurance Officer.

PHYSICAL

The DLP technical infrastructure is located in secured DLA data centers. These data center use a combination of Physical Security Controls such as Security Guards, advanced locks, personal identity verification, and remote back-up to protect the system.

TECHNICAL

All access to DLP system, including any of the remediation information (and its associated PII) is managed through DoD CAC authentication to the DLP systems and strict role based access which further limits access to DLP case details. In addition, all detected instances of unsecured PII are stored by the DLP system in encrypted format, via FIPS certified encryption modules.

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. DLA Information Assurance, DLA General Counsel / Privacy Office, and the DLA Computer Emergency Response Team / Network Operations & Security Center.

☐ **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. Peart-Hannon Consulting Group, LLC -- (52.204-9000, "CONTRACTOR PERSONNEL SECURITY" (MAR 2012), and 252.239-7001, "INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION." (JAN 2008)

☐ **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.

Data Loss Prevention detects instances of (1) unsecured PII in transit, i.e., Data-in-Motion to prevent loss of PII through e-mail or the web; and of (2) unsecured PII at rest, i.e., Data-at-Rest to prevent loss of PII on shared file storage space (for example files stored on internal DLA information systems such as a network drive or in the proprietary storage technology of Microsoft's SharePoint). When an unsecured instance of PII is detected, there may be additional associated PII from within those files or e-mail, e.g., SSN, plus full name, home address, and birth date, provided to the information assurance or privacy officer as part of the "snap shot" during the remediation phase. However, if the individual has complied with all data security policies and not left PII unsecured, then no PII is detected or "collected."

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.

Data Loss Prevention detects instances of (1) unsecured PII in transit, i.e., Data-in-Motion to prevent loss of PII through e-mail or the web; and of (2) unsecured PII at rest, i.e., Data-at-Rest to prevent loss of PII on shared file storage space (for example files stored on internal DLA information systems such as a network drive or in the proprietary storage technology of Microsoft's SharePoint). When an unsecured instance of PII is detected, there may be additional associated PII from within those files or e-mail, e.g., SSN, plus full name, home address, and birth date, provided to the information assurance or privacy officer as part of the "snap shot" during the remediation phase. However, if the individual has complied with all data security policies and not left PII unsecured, then no PII is detected or "collected." Once unsecured PII is detected it will be remediated and secured per DLA PII Policies and Procedures.

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.

When an employee or contractor starts to work at DLA they are required to acknowledge receipt of and sign that they understand DLA's "Information Assurance (IA): General Rules of Behavior." These Rules of Behavior state:

Users will:

- Not transmit sensitive information [NOTE: PII is "sensitive information"] over the internet unless it has been encrypted and digitally signed using a Common Access Card-based DOD Public Key certificate. See the titled "For Official Use Only Material" for identification of those categories of

information deemed sensitive.

- Not use shared drives to relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those authorized to access the data.

By signing the Rules of Behavior, the user consents to the following:

o The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.

o At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.

o Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and search.

o Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.

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.