PRIVACY IMPACT ASSESSMENT (PIA)

For the

Document Automation Content Service Records Management

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: 17525
- ☐ **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 This is DLA's implementation of the OpenText Document and R

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

44 U.S.C. Chapters 21, 29, 31 and 33, Federal Records Act (FRA);
44 U.S.C. 2108, Responsibility for custody, use and withdrawal of records;
44 U.S.C. 2906, Inspection of agency records;
36 CFR Chapter XII, Subchapter B - Records Management;
36 CFR Chapter XII, Subchapter C - Public Availability and Use
OMB Circular A-130, "Management of Federal Information Resources"
DoD Directive 5015.02, Records Management Program

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Document Automation Content Service Records Management Application (DACS RM) is a records management application solution that allows individuals who have a need for the records in the performance of their official duties (as confirmed by DD 2875) to store and retrieve electronic files. The system serves as a primary agency records repository and does contain personally identifiable information (PII), as identified by individual data owners. Data owners are responsible to both identify, and approve access for, individuals that require the PII data within DACS RM to perform their official duties. The DACS RM administrator(s) are responsible for ensuring appropriate permissions are assigned. In no case will access be granted to an individual who does not have an authorized need for the record in the performance of their official duty, or for whom a routine use under the Privacy Act does not exist.

Privacy information contained in DACS RM varies greatly depending on the individual data owner's administrative and functional work requirements.

a. Employees - Individual e-mail and/or documents that may contain personally identifiable information, including, but not limited to, social security numbers, banking information and/or home addresses.

b. Audit trail information (including employee log-in information) - Audit trails are in place to track the action of users on DACS RM. These audit mechanisms help to ensure that users are responsible for their actions.

c. Job Candidates - Individuals who are not currently a Federal employee but who have applied to DLA to become a Federal employee may provide PII as part of the job application and selection process.

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

Ensuring the confidentiality, integrity, availability, and accountability of PII is of critical concern to DLA and its employees. The DACS-RM Program Manager has configured the system in such a way as to manage the risk of unauthorized access and/or use of PII in the system. However, the management of risk is not solely the DACS-RM Program Manager's responsibility. Managing the risk to prevent the unauthorized use or disclosure of PII is also the responsibility of the data owners (also referred to as Supervisors, Program Managers and data process owners) as well as those who have been granted authorized access to the information in their section of DACS-RM. In part, the DACS-RM system mitigates risk by the application of strict access (permissions) based on a role-based security model. The number of necessary users with access to documents that contain PII is kept to a minimum by account monitoring as well as by requiring a supervisor signed copy of the DD Form 2875, "System Access Authorization Request" for any individual being granted access to a folder within the DACS-RM infrastructure.

Account management ensure only authorized users can gain access to information in accordance with DoD 5015.02-STD Electronic Records Management Software Applications Design Criteria Standard. Account management includes:

a. Identifying types of accounts (individual and group, conditions for group membership, associated privileges (permissions).

b. Establishing an account (i.e., required identification, approval, and documentation procedures)

c. Activating an account

d. Modifying an account (e.g., disabling an account, changing privilege level (permissions), group memberships, authenticators)

e. Terminating an account

Information data owners identify authorized users and their respective access authorizations. Emergency

and temporary access authorizations to the information system are approved by designated organization officials, monitored, and removed when no longer required. Administrators set parameters to provide access as authorized and restrict accesses that have not been authorized.

To access DACS RM all users must have access to Defense Logistics Agency (DLA) controlled network via a common access control (CAC) card and Public Key Infrastructure ((PKI) enabled authentication. All DLA employees (to include contractors) receive mandatory annual DoD-sponsored Privacy Act and PII protection and spillage training to help safeguard the PII. All DLA employees (to include contractors) must annually sign the DLA Privacy Safeguards and Responsibilities Certification which specifies possible civil, criminal, and administrative penalties for violation of its requirements.

DLA requires mandatory Information Awareness training for all employees and all contractors. This training includes safe handling procedures that cover receiving, viewing, printing, forwarding, storing, and shredding/ destruction of PII 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. To authorized individuals with a need for the information in the performance of their official duties.

☒ **Other DoD Components.**

Specify. To DFAS, DCAA, DoD OIG, and DCIS for the purpose of Financial Transactions, Audits, Inspections, or Investigations.

☐ **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.

DLA, per the Privacy Act, requires any collection of PII to contain a Privacy Act Statement which provides the user the option of not providing the information requested. However, per the applicable Privacy Act SORN, a user may be denied access (or some other like consequence) for failure to provide the requested data.

Once the user has elected to provide the PII, that information is protected by the Privacy Act. When or if those records are placed into DACS-RM, there is no secondary opportunity to object to the PII's collection.

(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.

DLA, per the Privacy Act, requires any collection of PII to contain a Privacy Act Statement which provides the user the option of not providing the information requested. However, per the applicable Privacy Act SORN, a user may be denied access (or some other like consequence) for failure to provide the requested data.

Once the user has elected to provide the PII, that information is protected by the Privacy Act. When or if those records are placed into DACS-RM, there is no secondary opportunity to object to the PII's collection.

(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.	DLA, per the Privacy Act, requires any collection of PII to contain a Privacy Act Statement which provides the user the option of not providing the information requested. However, per the applicable Privacy Act SORN, a user may be denied access (or some other like consequence) for failure to provide the requested data. Once the user has elected to provide the PII, that information is protected by the Privacy Act. When or if those records are placed into DACS-RM, there is no secondary Privacy Act Statement. However, all users must acknowledge a Privacy Advisory when accessing the DACS-RM 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.