PRIVACY IMPACT ASSESSMENT (PIA)

For the

Federal Logistics Information System Portfolio Data Warehouse (FLIS FPDW)
Defense Logistics Agency (DLA) Logistics Information Service

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: 286
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☐ **Yes**
- ☒ **No**

If "Yes," enter Privacy Act SORN Identifier

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

or

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

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

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

☐ **Yes**

Enter OMB Control Number

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.

FLIS FPDW operates as part of the Federal Catalog Program (FCP) and is authorized by Public Law 82-436, Cataloging and Standardization Act; 10 U.S.C. 145, Cataloging and Standardization; 40 U.S.C. 487, Surveys of Government property and management practices; and DoD Directive (DoDD) 4140.1-R, DoDI 4041.0, DoD Supply Chain Materiel Management Procedures: Delivery of Materiel; DoDD 5134.12, Materiel Management; DoD Manual 4140.01, DoD Supply Chain Materiel Management Procedures: Operational Requirements; DoD 4100.39-M, Federal Logistics Information System (FLIS) Procedures Manual

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.

FLIS FPDW is a Department of Defense (DoD) read only system. The FLIS FPDW is a data warehouse data dissemination capability with the mission to provide/share DoD master data from a single source to the multiple systems and applications within DoD and other Federal agencies that may require it. FLIS FPDW automatically collects data from an authoritative source, System for Award Management (SAM) for DoD items such as National Stock Number, Vendor data such as taxpayer ID and customer master data which includes DoD customer codes for delivery of business.

Within the vendor master data set there are four business data elements. Taxpayer ID Number (TIN), Bank Account Number, and Employer ID Number (EIN). If the vendor does not have a TIN, they may elect to use their Social Security Number (SSN) in lieu of TIN. These data elements are used by the financial community to validate, award, pay and report financial transactions required as part of doing business with the DoD.

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

Risks identified for the FLISFPDWsystem occur if a user does not follow propersecurity requirements, such as leaving acomputer unsecured allowing someone to accessthis information then, the information could be used for identity theft and fraud. In order to prevent this, users, including individuals responsible for system maintenance, receive initial and periodic refresher Privacy Act and Information Assurance training. Usersare trained to lock their workstations when leaving them unattended, toshut down computers when leaving at the end of the dutyshift, and to bealert to third partiesentering the workspace.

Another risk identified is that of unauthorized accessto the FLISFPDWservers. In order to prevent this,FLISFPDW serversare kept in asecure, limited access, or monitored work areasaccessible only to authorized personnel. Data is backed up daily for reconstruction of the recordsshould thesystem fail. Access to theservers isPublic Key Infrastructure (PKI) control.

Unauthorized access tosystem information on thesystem isanother risk associated with FLISFPDW. In order to prevent logical access, computers with accessto FLISFPDW information must be Common Access/Smart Card (CAC) enabled.CACenabling requiresa valid certificate and aPersonal Identification Number (PIN). Another risk identified is that of insider threat and unauthorized accessby DLA employees. To combat this threat, computer screens automatically lock after a preset period of inactivity or when a user removes his or her CACfrom.the card reader. Locked systems only be unlocked by inserting the CACand entering a valid Personal Identification Number (PIN). To combat the risk of "sniffers" being placed on communication lines, the businessinformation in the FLISFPDW system isencrypted.Businessinformation cannot be retrieved unlessaccessed using the correct encryption key with the decryption package to accessthe information.

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. Within DLA, information from the FLIS FPDW system is only available to J62 FLIS FPDW PMO employees.

☒ **Other DoD Components.**

Specify. Information from SAM may be accessed in the FLIS FPDW system by Army, Marine Corps, Air Force, and Defense Finance and Accounting Service.

Information created by these customers may be stored by and provided back to the data owner by the system.

☒ **Other Federal Agencies.**

Specify. Information collected from SAM by FLIS FPDW may be accessed by Federal agencies such as General Services Administration, Department of Treasury, Department of Justice, and United States Department of Agriculture, that require the data from SAM. Information that is created by these customers may be stored and provided back to the data owner.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

The FLIS FPDW does not collect data from individuals or create new data about or relating to individuals. The FLIS FPDW collects data from an authoritative source system, SAM, for data sharing purposes. Vendors/suppliers must enter their business information in the System for Award Management (SAM) when registering. If they do no not they will not be able to register in SAM.

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.

The FLIS FPDW system does not collect data from individuals or create new data about or relating to individuals. FLIS FPDW collects data from authoritative source system, SAM, for data sharing purposes. Vendors/suppliers must enter their business information in the System for Award Management (SAM) when registering. If they do no not they will not be able to register in SAM.

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.

The vendor/supplier provides the business information when they register in the SAM system. A TIN or EIN is required for registration. If the vendor/supplier does not have a TIN or EIN, they may choose to provide an SSN.

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.