PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Data Environment - High Side
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	13284
☐	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: 007-97-01-03-02-6516-00

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: F024 AF USTRANSCOM D DOD

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.

Statutory: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 19 U.S.C. 1498, Entry Under Regulations; 37 U.S.C. 406, Travel and Transportation Allowances, Dependents, Baggage and Household Effects; DoD 4500.9-R, Transportation and Traffic Management; E.O. 9397 (SSN); Public Law 100-562, Imported Vehicle Safety Compliance Act of 1988; 5 U.S.C. 5726, Storage Expenses, Household Goods and Personal Effects; Federal Acquisition Regulation (FAR); Joint Federal Travel Regulation (JTR), Volumes 1 and II; DOD Directive 4500.9E, Transportation and Traffic Management; DOD Directive 5158.4 United States Transportation Command; DOD Instruction 4500.42, DoD Transportation Reservation and Ticketing Services; DoD Regulation 4140.1, DoD Materiel Management Regulation; DoD Regulation 4500.0, Defense Transportation Regulation; and DoD Regulation 4515.13-R, Air Transportation Eligibility.

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 Integrated Data Environment (IDE) provides data to consuming systems from providing systems within the DoD Community of Interest. IDE creates a common information technology environment for the management of supply chain, distribution, and logistics information for Combatant Commands and Military Services. IDE also manages a PKI-enabled secure web site that allows Combatant Commands and Military Services to review potential data services with descriptions of information available to them. Privacy information is needed to schedule the movement of DoD personnel (military and civilian) and dependents traveling in the Defense Transportation System; schedule the movement, storage, and handling of personal property; to identify and trace lost shipments; to submit claims for damaged or loss shipments; U.S. customs protection of personal property; payment of commercial transportation providers under contract and tenders of the DoD; and monitor the effectiveness of personal property traffic management functions support. IDE improves end-to-end movement of defense resources in a common information technology environment using an improved DLA supply chain which monitors material assets that are in-transit.

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

Electronic records with privacy information will be maintained in a DISA secure data facility and are accessible only by authorized personnel. All data is encrypted during transmission and is delivered using system-to-system transfers that first validates the identity of the systems receiving or requesting IDE information. System-to-system transfers are the only method available to receive or send data to IDE. Persons do not have access to IDE records or data. Persons can only read information or meta data about the information available in IDE using the IDE Discovery Portal. Access to IDE is limited to person(s) responsible for administering the IDE application or the operating system of the IDE servers. These duties are official administrative duties that is performed by persons who have been properly screened and cleared for system need-to-know. Access to computerized data is restricted by DOD public key infrastructure (PKI), which is PIN protected.

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. USTRANSCOM, Military Services, and other Combatant Commands

☒ **Other DoD Components.**

Specify. Military Services

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Lockheed Martin is the external service provider (ESP) of the IDE system. In support of existing and future IDE resources, the ESP shall establish an IA Program to implement and sustain appropriate IA management, operational, and technical controls and processes as required to ensure compliance with DOD and Chairman,

Joints Chiefs of Staff (CJCS) requirements, and Joint Task Force -- Global Network Operations (JTF-GNO) taskings. The ESP shall submit for Government approval an overarching security plan that describes their strategy for implementation of IA and Industrial Security requirements (RFQ Section 5.0) throughout the life of the contract. The contractor shall prevent unauthorized access to Government sensitive unclassified and classified data and IT resources supporting IGC. The Contractor shall ensure appropriate IA controls are designed, developed, and implemented to provide for non-repudiation, confidentiality, integrity, and availability of Government systems, applications, and data. As a minimum, the Contractor shall ensure compliance with applicable provisions of DOD Directive (DODD) 8500.1, Information Assurance; DOD Instruction (DODI) 8500.2, Information Assurance Implementation; Federal Acquisition Regulations (FAR); DODD 8570.1, Information Assurance Training, Certification and Workforce Management; CJCS Manual 6510.01, Defense-In-Depth: IA and CND; DODI 8520.2, PKI and Public-Key (PK) Enabling; DODI 8551.1, Ports, Protocols, and Services Management (PPSM); and DODI 8510.01 Defense Information Assurance Certification and Accreditation Process (DIACAP). IDE has been designated as a Mission Assurance Category (MAC) III, sensitive (low-side) and MAC III classified (high-side) for the purposes of applying IA controls.

☐ **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.

IDE does not provide data to individual users. IDE only provides other systems with subscribed data services. If a person objects to the use of their personal information, individuals are referred to the providing and consuming systems that process this information.

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.

IDE only performs system-to-system data transfers. IDE has no method of providing individuals with their personal data. This can only be done by the publishing or subscribing end-user systems. Individuals are referred back to subscribing or publishing systems.

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.

IDE was not designed to respond to individuals queries regarding personal data collected to support the DOD supply and distribution chain or DOD food services. IDE only supports system-to-system interfaces. Persons are referred to the providing and consuming systems who have an archiving capabilities in the records that they process.

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.