PRIVACY IMPACT ASSESSMENT (PIA)

For the

DLA Physical Access Control System (Diamond II)
Defense Logistics Agency (DLA Headquarters)

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 S500.50, Facility Access Control

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	Published in FR for comment on August 20, 2013.
Enter Expiration Date	Final is pending.

☐ **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 U.S.C. 301, Departmental Regulations, 5 U.S.C. 6122, Flexible schedules, agencies authorized to use; 5 U.S.C. 6125, Flexible schedules, time recording devices; 10 U.S.C. 133, Under Secretary of Defense for Acquisition,Technology, and Logistics; 23 U.S.C.401 et seq., National Highway Safety Act of 1966; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees.

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 DLA Diamond II is used to enroll DLA employees (federal and contractors) to allow unescorted access access to the DLA Headquarters McNamara Complex.

The system collects the following personal information from visitors to create a temporary physical access visitor's badge: individual's name, home address (City, State, and zip code), date of birth, gender, and Driver's license number.

Some States issue Driver's Licences utilizing the individual's Social Security Number as the Driver's License Number. On December 17,2004,Public Law 108-458 was signed amending Title 42 of the U.S. Code. As amended, 42 U.S.C.§ 405(c)(2)(C)(vi)(II) strictly prohibits the display of the Social Security Number (SSN),or any derivative of such number, on any State's Drivers License (See Public Law 108-458"Intelligence Reform and Terrorism Prevention Act of 2004,"effective date of Dec. 17,2005).Typical Driver License validity periods are 2 years from issuance, with some States offering mail renewal options for an additional 1 or 2 years. The DLA G-Badge system does not collect SSNs and, per DLA Records Schedule157.20B (2 year destruction schedule),will be free of Driver License numbers which were based on SSN's by the end of December 2013.

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

Several privacy risks associated with PII collection were identified for Diamond II: (1) unauthorized access (compromise of data resulting in identity theft would be devastating and threaten DLA's reputation), (2) inaccurate information can affect management decisions, an individual's reputation, etc., and (3) unauthorized disclosure can result in identity theft.

In response to the risk that unauthorized access to the PII data contained in Diamond II records, Diamond II is protected under the the defense-in-depth approach being taken by DLA Headquarters Information Technology System (HQITS) to protect this data. The Diamond II system is on the DLA HQITS network. Physical, technical (common access card (CAC) and personal identification number (PIN) are required for Diamond II. Procedural and safeguards are employed in series to ensure only those personnel that have a validated need-to-know can access this sensitive information.

In response to the risk presented by unauthorized disclosure of data within Diamond II records, DLA is taking a multi-pronged approach to mitigating this concern involving 1) Required (for new hires and all personnel at least annually) and repetitive security and privacy training as needed; 2) Requirement to execute formal nondisclosure agreements by any and all parties with direct system access to Diamond II; and 3) commitment by management to enforce stated penalties for not complying with Privacy Act requirements.

All DLA employees are required to take an Information Assurance Awareness and Privacy Act Training refresher course annually. Training emphasizes the importance of protecting personal information from loss, theft, and compromise.

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 Physical Security Offices, Security Assistant, General Counsel, Defense Criminal Investigation Service (DCIS).

☒ **Other DoD Components.**

Specify. Department of the Army's Criminal Investigation Division with a need to know.

☒ **Other Federal Agencies.**

Specify. Federal Law Enforcement Agencies with a need to know.

☒ **State and Local Agencies.**

Specify. State and Local Law Enforcement Agencies with a need to know.

☐ **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.

At the point of collection, individuals are provided a form with a Privacy Act Statement explaining the Authority to collect the data; the uses that will be made of the data within DLA/DoD; the disclosures that may be made outside DLA/DoD; and that the disclosure of their information is voluntary. Individuals are also provided with the consequences of not providing their personal data i.e., denied access to the DLA installation, building, and/or facility. The form used is the DLA Form 1815. A standardized form for all DLA components is currently being developed.

(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.

At the point of collection, individuals are provided a form with a Privacy Act Statement explaining the Authority to collect the data; the uses that will be made of the data within DLA/DoD; the disclosures that may be made outside DLA/DoD; and that the disclosure of their information is voluntary. Individuals are also provided with the consequences of not providing their personal data i.e., denied access to the DLA

installation, building, and/or facility. The form used is the DLA Form 1815. A standardized form for all DLA components is currently being developed.

(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.

PRIVACY ACT STATEMENT

Authority: 5 U.S.C. 301, Departmental Regulations, 5 U.S.C. 6122, Flexible schedules, agencies authorized to use; 5 U.S.C. 6125, Flexible schedules, time recording devices; 10 U.S.C. 133, Under Secretary of Defense for Acquisition,Technology, and Logistics; 23 U.S.C.401 et seq., National Highway Safety Act of 1966; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees.

Purpose(s): Information is collected and maintained to control access into DLA-managed installations, buildings, facilities, and parking lots.

Routine Use(s): Data may be provided under any of the DoD "Blanket Routine Uses" available at: http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html.

Disclosure: Voluntary; however, failure to provide the requested information may result in denial of a DLA Badge and access to DLA installations, buildings, facilities.

Rules of Use: Rules for collecting, using, retaining, and safeguarding this information are contained in the DLA Privacy Act System of Records Notice S500.50, entitled "Facility Access Records" available at http://dpclo.defense.gov/privacy/SORNs/component/dla/index.html.

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.