PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Biometric Identification System (DBIDS)
Defense Manpower Data Center (DMDC)

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: 1391
- ☐ **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 007-97-01-15-01-4035-00-403-254

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 DMDC 10

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 0704-0455

Enter Expiration Date 08/31/13

☐ **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.

10 U.S.C. 113, Secretary of Defense; Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources; DoD 5200.08-R, Physical Security Program; and E.O. 9397 (SSN), as amended.

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 records support DoD physical security and information assurance programs, to issue individual facility/ installation access credentials, and for identity verification purposes. The system also is used to record personal vehicles and property registered with the DoD, and for producing facility management reports. The records may be accessed by other physical access control systems for further verification at other sites. Records may also be used for law enforcement purposes.

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

PII data is only accessible via the application by provisioned users (managed by each individual site). The database itself is hosted by DMDC and no other applications can access the data. Some data is cached on the local access control point workstations to support off-line operations but the workstations are completely locked down and the caches/hard drives are encrypted.

The one exception to the above paragraph is that in DBIDS 4.0 Cognos is used for generating and storing reports. Access to the reports is controlled through access to the application or through Security Online. These reports have name and last 4-SSN and can include up to the last 30 days of registration.

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. Used by security offices to monitor individuals accessing DoD installations and/or facilities. Data may be viewed by or shared with civilian employees, military members, and contractors assigned to DMDC DBIDS software/ database technical support, by operators responsible for registering individuals into the database, by Installation Access Control Point (ACP) personnel, and by Installation Law enforcement personnel.

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Data may be provided to other Federal agencies under any of the DoD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/ notices/blanket-uses.html.

☒ **State and Local Agencies.**

Specify. law enforcement agencies

☐ **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.

The Office of the Secretary of Defense rules for accessing records, for contesting contents, and appealing initial agency determinations are published in Office of the Secretary of Defense Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

(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.

Every registration workstation has the privacy act notification posted (responsibility of each institution) and an individual requesting access to that installation may decline to be registered - however, they will likely be rejected from receiving physical access.

(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 Statements, as required by 5 U.S.C 552a(e)(3), are provided at the collection point. The statement provides the following: collection purpose, authorities, external uses, the voluntary nature of the program, the fact that no consequences accrue for those who choose not to participate beyond denial of a DBIDS card or visitors pass and denial of access to the installation, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. The DBIDS Privacy Act Statement reads as follows: AUTHORITY: Executive Order 9397; The Privacy Act of 1974, 5 U. S. C. 552a; DODD 8500.1 PRINCIPAL PURPOSE(S): To provide necessary information to DoD installations to determine if applicant meets access control requirements. Use of SSN is necessary to make positive identification of an applicant. Records in the DBIDS system are maintained to support Department of Defense physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the DoD, and for producing facility management reports. Used by security offices to monitor individuals accessing DoD installations and/or facilities. SSN, Drivers License Number, or other acceptable identification will be used to distinguish individuals who request entry to DoD installations and/or facilities. ROUTINE USE(S): The "DoD Blanket Routine Uses" are set forth at the beginning of the DoD compliation of systems of records notices. DISCLOSURE: Voluntary. However, failure to provide the requested information will result in denial of a DBIDS card or visitors pass and denial of entry to DoD installations and/or facilities.

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.