PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Biometric Identification System (DBIDS)

2. DOD COMPONENT NAME:

Department of Defense Human Resources Activity

3. PIA APPROVAL DATE:

06/10/24

Defense Manpower Data Center (DMDC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

The records support DoD physical security programs, to issue individual facility/installation access credentials, and for identity verification purposes. The system records 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 be used to ensure compliance with host nation agreements and to ensure rations and supplies are readily available to support facility/installation personnel and visitors. Records may also be used for law enforcement purposes.

Types of personal information include: name, Social Security Number (SSN), demographics, contact information, biometrics.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Data collected is used to enter personnel data into a database, capture biometric information, and retrieve that data and biometric information for verification and validation at a later time, especially when the individual requires installation access.

In the case of non-DoD individuals who require base access, a DBIDS access card is produced. The records are maintained to support DoD physical security and information assurance programs and are used for identity verification purposes, to record personal property registered with the Department, and for producing facility management reports.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

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 to DoD facilities or installations.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

It is the responsibility of each registration center to provide Privacy Act Statements, as required by 5 U.S.C 552a(e)(3), at the collection point. The statement should provide 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 DoD card or visitors pass and denial of access to the

installation or facility, the name and number of the Privacy Act system notice governing the collection, and an electronic link to the system notice.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

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 compilation 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.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] 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.
[X] Other DoD Components *(i.e. Army, Navy, Air Force)*	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.
[X] Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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.
[X] State and Local Agencies	Specify.	Data may be provided to state and local agencies in accordance with the DoD Law Enforcement Routine Use.
[ ] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
[ ] Other *(e.g., commercial providers, colleges)*.	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

[X] Individuals [X] Databases

[X] Existing DoD Information Systems [ ] Commercial Systems

[ ] Other Federal Information Systems

Data is collected from the individual, the Defense Enrollment Eligibility Reporting System (DEERS), the Identity Management Engine for

Security and Analysis (IMESA), the Military Services, and the DoD Components.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [x] In-Person Contact
- [x] Paper
- [ ] Fax
- [ ] Telephone Interview
- [x] Information Sharing - System to System
- [x] Website/E-Form
- [x] Other *(If Other, enter the information in the box below)*

Existing DoD databases, the Military Services, DoD Components.

k. 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 must be consistent.

- [x] Yes
- [ ] No

If "Yes," enter SORN System Identifier DMDC 10

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. N1-330-08-005, item 1

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Cut off record on deactivation or confiscation of card. Destroy 3-5 years after cutoff or when no longer needed for security purposes, whichever is applicable.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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.

[X] Yes [ ] No [ ] Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0704-0455
Expiration: 8/31/2024 , this is in public review in the Federal Registry to renew expiration date.