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:

Identity Matching Engine for Security and Analysis (IMESA)

2. DOD COMPONENT NAME:

Department of Defense Human Resources Activity

3. PIA APPROVAL DATE:

Defense Manpower Data Center

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
- ☒ 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
- ☒ 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.

To continuously screen individuals' seeking eligibility for physical access to DoD facilities or installations and implement security standards controlling entry to DoD facilities and installations. This process includes vetting to determine the fitness of an individual requesting or requiring access, issuance of local access credentials for members of the public requesting access to DoD facilities and installations, and managing and providing updated security and credential information on these individuals. To ensure that identity and law enforcement information is considered when determining whether to grant physical access to DoD facilities and installations.
Types of information collected include: Name, date of birth, Social Security Number, Foreign National ID,
Driver's License, citizenship information, sex, race, contact information, credential information, biometric
information, physical features, information generated from the National Crime Information Center (NCIC) and Terrorist Screening Center (TSC).

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)*

IMESA collects PII to perform mission- related use. (IMESA) is a physical security component specifically designed to support the electronic authentication of Personal Identity Verification (PIV) and Common Access Cards (CAC) against the public key infrastructure certificate revocation lists, verify other Department of Defense (DoD) Identification cards against the Defense Enrollment Eligibility Reporting System (DEERS), and secure access DoD authoritative and other digital identity data and information to support physical access management (i.e. credential authentication, identification card validation, and fitness determinations). IMESA also supports fitness for installation physical access determinations, as well as law and order functions on installations by continuously reinitiating a screen of identities against authoritative data sources for those who have been previously granted access to DoD installations. IMESA uses approved Criminal Justice Information (CJI) and terrorist screening biographic information as appropriate and authorized for the populations delineated in DoD physical security policy.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ 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.

Information in IMESA is derived from existing federal systems.

f. 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.

Information in IMESA is derived from existing federal systems.

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.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

For data provided from the PACS: 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.
DD FORM 2930 NOV 2008 Page 6 of 15
For identity data provided from DEERS: Privacy Act Statements are printed on DD Forms 1172, 1172-2 and 2842 and provided at the collection point. The statement provides collection purpose, authorities, external uses, nature of the program, the name and number of the PAS notice governing the collection, and an electronic link to the system notice. The statement is included on paper and electronic collection forms. A PAS is also available for those updating their information via telephone. For data provided from the NCIC: None.

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)*

☒ Within the DoD Component	Specify.	DoD Visitor Registration facilities
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	USA, USAF, USMC, USN
☒ 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://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.htm
☒ State and Local Agencies	Specify.	Data may be provided to state and local agencies under the DoD "Blanket Routine Uses" published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html
☐ 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)*

☐ Individuals ☒ Databases
☒ Existing DoD Information Systems ☐ Commercial Systems
☒ Other Federal Information Systems

Data is coDefense Enrollment and Eligibility Reporting System (DEERS), Various Dept of Justice source files, DoD Physical Access Control Systems, DoD Visitor Registration Centers.

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)*
☐ In-Person Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☒ Information Sharing - System to System ☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

Defense Enrollment and Eligibility Reporting System (DEERS), various Dept of Justice source files, DoD Physical Access Control Systems, DoD Visitor Registration Centers.

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DMDC 16

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. DAA-0330-2013-0009

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

(3) Retention Instructions.

Destroy 5 years after no access by all PACS associated to that individual OR after all PACS have submitted a de-registration request for the individual.

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; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08 and all volumes, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; Federal Information Processing Standards (FIPS) 201-2; National Institute of Standards and Technology (NIST) 800-63, Digital Identity Guidelines; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoDI 5525.19 DoD Identity Matching Engine for Security and Analysis (IMESA); DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; 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.

☐ 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.

IMESA does not collect data directly from individuals. The Privacy Office has determined, due to the functionality of IMESA, that an OMB number is not required. Evidence of the aforementioned determination can be provided upon request.