# SYSTEM OF RECORD NOTICES (SORNS)

## Office of the Secretary, DoD/Joint Staff

### DMDC 16 DoD

PRINT

**SYSTEM NAME:**

Identity Management Engine for Security and Analysis (IMESA) (December 21, 2015, 80 FR 79310)

**SYSTEM LOCATION:**

Defense Manpower Data Center, DoD Center Monterey Bay, 400 Gigling Road, Seaside, CA 93955-6771.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Any individual seeking access to a DoD facility or installation, and all individuals with felony warrants listed in the Federal Bureau of Investigation's (FBI) National Crime Information Center's (NCIC) Wanted Person File, all individuals maintained in the NCIC National Sex Offender Registry (NSOR) File and all individuals maintained in the FBI's Terrorist Screening Database (TSDB) records.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Information on individuals identified in the IMESA Interoperability Layer Service (IoLS) DoD Population Database: DoD ID number, Social Security Number (SSN), last name, date of birth, credential type, issuance, and expiration information; and security alert information (alert type, alert source, case number).

Information on individuals identified in the IMESA IoLS Local Population Database: Full name; date of birth; SSN; Local Population identifier; foreign national ID; gender; race; citizenship information; contact information (e.g., home or work mailing address, personal phone, work phone); physical features (height, weight, eye color, hair color); biometrics (photograph and fingerprints); credential type, issuance, and expiration information; security alert information (alert type, alert source, case number); and secondary identification such as a driver's license or passport.

The following will be included for individuals about whom records are maintained in the FBI's NCIC Wanted Person File, FBI's NCIC NSOR File, and FBI's TSDB records: Identity information (to include alternate identity information): SSN; full name; gender; race; ethnicity; address; place of birth; date of birth; citizenship; physical features (height, weight, eye color, hair color or other identifying characteristics); vehicle/vessel license information; want/warrant type, time, location, and case number of offense, violation or incident; extradition limitations; incarceration information; employment information; vehicle, vessel, aircraft and/or train information; caution and medical condition indicators.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

10 U.S.C. 113, Secretary of Defense; DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 5200.08, Security of DoD Installations and Resources and the DoD Physical

**SORN Types**
DoD Component Notices
DoD-wide Notices
Government-wide Notices

**SORN Links**
Blanket Routine Uses
DoD Components Preamble
DoD Components Address Directory
DoD Information Management Control Officers

**DOD Components**
Defense Commissary Agency (4)
Defense Contract Audit Agency (9)
Defense Contract Management Agency (1)
Defense Finance and Accounting Service (55)
Defense Health Agency (22)
Defense Information Systems Agency (19)
Defense Intelligence Agency (19)
Defense Logistics Agency (45)
Defense Security Service (11)
Defense Threat Reduction Agency (15)
Department of the Air Force (248)
Department of the Army (211)
Department of the Navy (Navy and Marine Corps) (195)
Missile Defense Agency (0)
National Geospatial-Intelligence Agency (19)
National Guard Bureau (6)
National Reconnaissance Office (25)
National Security Agency/Central Security Service (26)
Office of the Inspector General (18)
Office of the Secretary, DoD/Joint Staff (114)
Unified Commands (COCOMS) (6)

Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Exception to policy memos); Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control; DTM 14-005, DoD Identity Management Capability Enterprise Services Application (IMESA) Access to FBI National Crime Information Center (NCIC) Files; and E.O. 9397 (SSN), as amended.

**PURPOSE(S):**

To evaluate individuals' eligibility for 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.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Law Enforcement Routine Use:
If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use:
Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use:
A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use:
A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use:
A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found online at:

**http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx**

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Electronic storage media.

**RETRIEVABILITY:**

Records may be retrieved by DoD ID Number, Local Population identifier, SSN, or credential information.

**SAFEGUARDS:**

Access to these records is role-based and is limited to those individuals requiring access in the performance of their official duties. Audit logs will be maintained to document access to data. All data transfers and information retrievals using remote communication facilities are encrypted. Access to individual records requires role-based access and use of a Common Access Card (CAC) and PIN. Records are maintained in encrypted databases in a controlled area accessible only to authorized personnel. Entry to these areas is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to this system of records are to receive Information Assurance and Privacy Act training annually.

**RETENTION AND DISPOSAL:**

Records will be destroyed five (5) years after no access by all DoD Physical Access Control Systems (PACS) associated to that individual OR after all PACS have submitted a de-registration request for the individual.

**SYSTEM MANAGER(S) AND ADDRESS:**

Deputy Director for Identity, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000.

**NOTIFICATION PROCEDURE:**

Individuals seeking to determine whether information about themselves is contained in this system should send written inquiries to the Deputy for Identity, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-.

Requests must contain the full name and Social Security Number of the subject, and a return address.

**RECORD ACCESS PROCEDURES:**

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff Privacy Office, 1155 Defense Pentagon, Washington DC 20301-1155.

Signed, written requests must include the full name and Social Security Number of the subject and a return address.

**CONTESTING RECORD PROCEDURES:**

The Office of the Secretary of Defense/Joint Staff rules for accessing records, contesting contents, and appealing initial agency determinations are contained in Office of the Secretary of Defense Administrative Instruction 81; 32 CFR part 311; or may be obtained from the Privacy Act Officer, Office of Freedom of Information, Washington Headquarters Services, 1155 Defense Pentagon, Washington, DC 20301-1155.

Information provided by the NCIC Wanted Person Files is exempt from the amendment and appeal provisions described in 5 U.S.C. 552a (f).

**RECORD SOURCE CATEGORIES:**

Defense Enrollment and Eligibility Reporting System (DEERS), FBI NCIC Wanted Person File, DoD Physical Access Control Systems, DoD Visitor Registration Centers.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

The records contained in this system are used for criminal, civil, and administrative enforcement requirements. To the extent that copies of exempt records may become part of these records through JUSTICE/FBI-001, National Crime Information Center (NCIC), OSD hereby claims the same exemptions for the records as claimed at their source (JUSTICE/FBI-001, National Crime Information Center (NCIC)). This system of records may be exempt from the following provisions of 5 U.S.C. 552a sections (c)(3) and (4), (d), (e)(1) through (3), (e)(4)(G) through (I), (e)(5) and (8), (f), and (g) (as applicable) of the Act.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and published in 32 CFR part 311. For additional information contact the system manager.

**FEDERAL REGISTER HISTORY:**

December 21, 2015, 80 FR 79310; February 27, 2014, 79 FR 11091