Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0116]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to alter a System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to alter a system of records, DMDC 16 DoD, entitled "Interoperability Layer Service (IoLS)" 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.

DATES: Comments will be accepted on or before [**INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the date following the end of

the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, Regulatory and Audit Matters Office, 9010 Defense Pentagon, Washington, DC 20301-9010.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Cindy Allard, Chief, OSD/JS Privacy Office, Freedom of Information Directorate, Washington Headquarters Service, 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0461.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in

the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy and Civil Liberties Division website at http://dpcld.defense.gov/.

The proposed system report, as required by U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on October 29, 2015, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: December 2, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 16 DoD

System name:

Interoperability Layer Service (IoLS) (February 27, 2014, 79 FR 11091)

Changes:

* * * * *

System name:

Delete entry and replace with "Identity Management Engine for Security and Analysis (IMESA)"

* * * * *

Categories of individuals covered by the system:

Delete entry and replace with "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:

Delete entry and replace with "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:
Delete entry and replace with "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 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."

* * * * *

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Delete entry and replace with "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

* * * * *

Safeguards:
Delete entry and replace with "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:

Delete entry and replace with "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."

* * * * *

[FR Doc. 2015-31867 Filed: 12/18/2015 8:45 am; Publication Date: 12/21/2015]