Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0019]

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 10 DoD, entitled "Defense Biometric Identification Data System (DBIDS)" in its inventory of record systems subject to the Privacy Act of 1974, as amended.

The records in the system are used to support DoD physical security 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.

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: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, 2nd Floor, Suite 02G09, Alexandria, VA 22350-3100.

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 February 6, 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: February 10, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 10 DoD

System name:

The Defense Biometric Identification Data System (April 1, 2011, 76 FR 18191).

Changes:

* * * * *

System name:

Delete entry and replace with "Defense Biometric Identification Data System (DBIDS)."

* * * * *

Categories of individuals covered by the system:

Delete entry and replace with "All individuals who request or have been granted physical access to DoD installations and facilities or using facilities interfacing with Defense Manpower Data Center (DMDC) Physical Access Control Systems.

All individuals who have been or will be denied access to a DoD installation or facility using or interfacing with DMDC Physical Access Control System based on the decision of the facility commander in charge of physical access control."

Categories of records in the system:

Delete entry and replace with "Personal data includes name, identification type (e.g. DoD ID number, driver's license number, passport number, state ID number, Social Security Number(SSN), date and place of birth, gender, nationality and country of citizenship, race, tribe, home and work addresses, personal and work email addresses and telephone numbers,

marital status, photographs, weight, height, eye color, hair color, index fingerprints or 10-print rolled and slapped fingerprints, iris scans, hand geometry, grade, dates of issue and expiration of facility and installation access credentials, alert status (e.g. Wants or Warrants, Armed and Dangerous, Be On the Lookout, Red Cross Emergency, Missing) or other similar fields necessary in assisting law enforcement in understanding the current disposition of personnel and property entering and, when required by Status of Forces Agreement, exiting DBIDS controlled facility, and installation name and/or region the record was created.

Privately owned vehicle information includes name of vehicle manufacturer, model year, color and vehicle type, license plate type (e.g., personal, commercial) and number, vehicle identification number (VIN), and current registration, automobile insurance, and driver's license data for those vehicles with established installation access (base/post decals).

Information on personal property stored on a military installation or facility contains data on government-issued (when required by Status of Forces Agreement) and personal weapons, such as type, serial number, manufacturer, caliber,

and firearm registration date; storage location data to include unit, room, building, and phone number; and type(s) of personal property (e.g., bicycles) and description of property, serial number, and color."

Authority for maintenance of the system:
Delete entry and replace with "10 U.S.C. 113, Secretary of Defense; 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 and the DoD Physical Security Review Board (PSRB); DoD 5200.08-R, Physical Security Program; and E.O. 9397 (SSN), as amended."

Purpose(s):
Delete entry and replace with "The records support DoD physical security 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."

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.

Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

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 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:

Delete entry and replace with "Electronic storage media."

Retrievability:

Delete entry and replace with "Retrieved by name, identification type and number, vehicle identifiers, or weapon identification data. Records may also be retrieved by photograph or fingerprints."

Safeguards:

Delete entry and replace with "Computerized records are maintained in a controlled area accessible only to authorized personnel. Entry is restricted by the use of locks, guards, and administrative procedures. Access to personal information is role based and limited to those who require the records in the performance of their official duties.

Access to personal information is further restricted by the use of unique logon and passwords, which are changed periodically, or by two factor authentication including biometric verification."

Retention and disposal:
Delete entry and replace with "Records are deleted three to five (3-5) years after deactivation or confiscation of access credentials."

System manager(s) and address:
Delete entry and replace with "Deputy for Identity, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000."

Notification procedure:
Delete entry and replace with "Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Deputy for Identity, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000.

Signed, written requests should contain the requester's name, identification type and number, date of birth, installation

name and/or region the record was created and current address and telephone number of the individual."

Record access procedures:
Delete entry and replace with "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 Freedom of Information Act Requester Service Center, 4800 Mark Center Drive, Alexandria, VA 22350-3100.

Signed, written requests should contain the requester's name, identification type and number, date of birth, installation name and/or region record was created, current address and telephone number of the requester and the name and number of this system of records notice."

Contesting record procedures:
Delete entry and replace with "The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager."

Record source categories:

Delete entry and replace with "Data is collected from the individual, the Defense Enrollment Eligibility Reporting System (DEERS), the Interoperability Layer Service (IoLS), the Military Services, and the DoD Components."

* * * * *

[FR Doc. 2015-03007 Filed 02/12/2015 at 8:45 am; Publication Date: 02/13/2015]