

Billing Code:

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2024-DMDC-XXXX]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, Department of Defense (DoD)

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Office of the Secretary of Defense is modifying and reissuing a current system of records titled, “Defense Biometric Identification Data System (DBIDS), DMDC 10 DoD.” This system of records was originally established to support DoD physical security programs, to issue individual facility/installation access credentials, and for identity verification purposes. The records may be accessed by other physical access control systems for further verification at other sites. 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. This system of records is being updated to incorporate the DoD standard routine uses (routine uses A through J). The DoD is also modifying various other sections within the SORN to improve clarity or update information that has changed.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT 30 DAYS AFTER DATE OF**

PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

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

* Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

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 <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: DHRA Component Privacy Officer, 400 Gigling Rd, Rm DODC-MB 7028, Seaside, CA 93955, dodhra.mc-alex.dhra-hq.mbx.privacy@mail.mil or 831-220-7330.

SUPPLEMENTARY INFORMATION:

I. Background

The Office of the Secretary of Defense proposes to modify a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. 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. Subject to public comment, the OSD proposes to update this SORN to add the standard DoD routine uses (routine uses A through J). In addition to changes made to the routine use section, other modifications are as follows: (1) to the System Location section to update the address; (2) to the Retrieval of Records section by removing the SSN and replacing with the DoD ID number; (3) to the Administrative, Technical, and Physical Safeguards to update the individual safeguards protecting the personal information; (4) Record Access, Notification, and Contesting Record Procedures, to reflect the need for individuals to identify the appropriate DoD office or component to which their request should be directed and to update the appropriate citation for contesting records. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Office of the Assistant to the Secretary for Defense for Privacy, Civil Liberties, and Transparency (OATSD(PCLT)) website at <https://dpclld.defense.gov/privacy>.

II Privacy Act

Under the Privacy Act, “a system of records” is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated:

Aaron T. Siegel,
Alternate OSD Federal Register
Liaison Officer, Department of Defense

SYSTEM NAME AND NUMBER: Defense Biometric Identification Data System (DBIDS), DMDC 10

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Manpower Data Center, 400 Gigling Road, Seaside, CA 93955-6771. For a list of installations using this system, contact the system manager.

SYSTEM MANAGER: The system manager is Program Manager, Defense Manpower Data Center, 4800 Mark Center Drive, Alexandria, VA 22350-6000. E-mail: dodhra.dodc-mb.dmdc.mbx.webmaster@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 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.

PURPOSE(S) OF THE SYSTEM: The records support DoD physical security programs, issuing 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.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: 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:

A. Personal data includes name, identification type (e.g. DoD ID number, Social Security Number (SSN), driver's license number, passport number, state ID number, tax ID number), 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, physical attributes, biometric information, , , **familial relation, stored identity proofing documents, 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.

B. 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, and current registration, automobile insurance, and driver's license data for those vehicles with established installation access (base/post decals).

C. 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.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individual, the Defense Enrollment Eligibility Reporting System (DEERS), the Identity Management Engine for Security and Analysis (IMESA), the National Law Enforcement Telecommunications System (NLETS), the Military Services, the DoD Components, and other Federal Criminal Justice Information Services Division (CJIS) systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND 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, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction

with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1987, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, DoD ID number, or SSN,

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: 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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: 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.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records 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 name and number of this system of records notice along with full name, identification type and number (DoD ID number, Social Security number , date of birth, installation name and/or region record was created, current address and telephone number. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)”.

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURE: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: February 13, 2015, 80 FR 8072; April 1, 2011, 76 FR 18191.