DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on a Modified System of Records
Under the Privacy Act of 1974

1. System identifier and name: DMDC 10 DoD, Defense Biometric Identification Data System (DBIDS).

2. Nature of changes proposed for the system: The DBIDS system tracks a visitor's familial relationship to their sponsor. This must be tracked in order to ensure compliance with host nation agreements, which provide that only family members may stay on base with a sponsor or member.

3. Authority for the 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.

4. Provide the agency's evaluation of the probable or potential effects on the privacy of individuals: In reviewing this SORN, the Defense Manpower Data Center (DMDC) carefully reviewed the safeguards established for the system to ensure they are compliant with DoD's requirements and are appropriate to the sensitivity of the information stored within this system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information is provided, and if applicable, a data use agreement has been established.

5. Routine Use compatibility: The first four routine uses are consistent with the purpose for which the information was collected. The remaining routine uses have been determined to be necessary and proper.

6. OMB Information collection requirements:
   OMB collection required: Yes
   OMB Control Number: 0704-0455
   Date Approved or Submitted: Submitted 04/10/17
   Expiration Date: TBD

   If no, then state reason:

7. FORMS:
   DBIDS Registration Application

Information requested by DPCLTD, not submitted to OMB:

8. Is the system, in whole or in part, being maintained by a contractor? Yes

9. Name of IT System (State NONE if paper records only): DBIDS

DMDC 10 DoD

System name:
Defense Biometric Identification Data System (DBIDS)

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.

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:
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, familial relation, pet information, 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:
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):
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 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.

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.

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**

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:
Electronic storage media.

Retrievability:
Retrieved by name, identification type and number, vehicle identifiers, or weapon identification data. Records may also be retrieved by photograph or fingerprints.

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.

Retention and Disposal:
Records are deleted three to five (3-5) years after deactivation or confiscation of access credentials.

System Manager(s) and Address:

Principal Deputy Director for Enterprise Benefits Operations, 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 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:
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:
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:
Data is collected from the individual, the Defense Enrollment Eligibility Reporting System (DEERS), the Identity Management Engine for Security and Analysis (IMESA), the Military Services, and the DoD Components.

Exemptions Claimed for the System:
None.