This document is scheduled to be published in the Federal Register on 10/30/2015 and available online at **http://federalregister.gov/a/2015-27745**, and on **FDsys.gov**

Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2015-OS-0115]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a new System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to add a new system of records, DMDC 20, entitled "Personnel Security Breach Notification and Mitigation Services Records". The Department of Defense is providing notification and facilitating the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases the Department must establish this system in order to provide notification to and facilitate the provision of breach mitigation services. Due to the number and proportion of affected individuals belonging to the DoD, DoD entered into agreements with OPM to handle the breach notification and mitigation services. DoD will also use these records to respond to breach verification inquiries. Individuals may go to OPM's website and click on a link that will redirect them to a DoD website where they can enter their information to find out if they have been affected by this breach. These

records may also be used for tracking, reporting, measuring, and improving The Department's effectiveness in implementing this data breach notification.

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 day 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, 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 http://dpcld.defense.gov/. The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on October 27, 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: October 27, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 20

System name:

Personnel Security Breach Notification and Mitigation Services Records.

System location:

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

Categories of individuals covered by the system:

Federal civilian and military personnel and applicants, and employees of government contractors, experts, instructors, and consultants to Federal programs who underwent a personnel background investigation after January 1, 1990. Other individuals whose Social Security Numbers (SSNs) were provided on an SF85, SF85-P and SF86 after January 1, 1990. Individuals who submit a breach verification inquiry. Minor children, who were minors as of July 1, 2015, of individuals described in this paragraph.

Categories of records in the system:

Last, first, and middle name; Social Security Number (SSN); date of birth, place of birth; citizenship status; country of citizenship; home and/or business addresses, phone numbers, and e-mail addresses.

Authority for maintenance of the system:

The E-Government Act of 2002 (Pub. L. No. 107-347); the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) (44 U.S.C. 3551-3559); 10 U.S.C. 113, Secretary of Defense; 50 U.S.C. 3038, Responsibilities of Secretary of Defense Pertaining to National Intelligence Program; E.O. 12333, United States Intelligence Activities, as amended; E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft, as amended; E.O. 13526, Classified National Security Information; White House Memorandum dated September 20, 2006, Subject: Recommendations for Identity Theft Related Data Breach Notification; and E.O. 9397 (SSN), as amended.

Purpose(s):

To provide breach notification and facilitate the provision of breach mitigation services to individuals affected by the breach of information in the Office of Personnel Management (OPM) background investigation databases. DoD will also use the data to respond to breach verification inquiries received from individuals using the link on OPM's website that redirects individuals to a DoD website where they can enter their information to find out if they have been affected by

this breach. These records may also be used for tracking, reporting, measuring, and improving the Department's effectiveness in implementing this data breach notification.

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

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

To commercial entities, under contract with DoD, for the sole purpose of verifying addresses of affected individuals in order to provide notification to such individuals.

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 Federal agency concerned, 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.

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.

Disclosure to the Office of Personnel Management Routine Use: A record from a system of records subject to the Privacy Act and maintained by a DoD Component may be disclosed to the OPM concerning information necessary for the OPM to carry out its legally authorized functions.

Counterintelligence Purpose Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use outside the DoD for the purpose of counterintelligence activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States.

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 Component's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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 an individual's name, SSN, date and place of birth.

Safeguards:

Access to personally identifiable information is restricted to those who require access to the records in the performance of their official duties in connection with the breach notification process. Access to personally identifiable information is further restricted by the use of Personal Identity Verification (PIV) cards and PIN. Physical entry is restricted by the use of locks, key cards, security guards, and identification badges. All individuals granted access to this system of records will have completed annual Information Assurance and Privacy Act training and be appropriately vetted. Audit logs will be maintained to document access to data. All electronic records transfers into this system of records will be encrypted. Records will be maintained in a secure database with an intrusion detection system in a physically controlled area accessible only to authorized personnel.

Retention and disposal:

The National Archives and Records Administration has authorized the destruction of these records 3 (three) year(s)

after credit monitoring and identity management services have concluded.

System manager(s) and address:
Deputy Director for Identity, Defense Manpower Data Center, 4800 Mark Center, Alexandria, VA 22350-4000.

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

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Defense Manpower Data Center (DMDC), DoD Center Monterey Bay, ATTN: Privacy Act Office, 400 Gigling Road, Seaside, CA 93955-6771.

Signed, written requests must contain the full name (and any alias and/or alternate names used), SSN, and date and place of birth.

Record access procedures:
Individuals seeking 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, 1155 Defense Pentagon, Washington, DC 20301-1155.

Individuals should provide their full name (and any alias and/or alternate names used), SSN, and date and place of birth.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following 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).'

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for their representative to act on their behalf.

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

Record source categories:
Individuals requesting verification via OPM's website who click on a link that will redirect them to a DoD website where they can enter their information to find out if they have been affected by this breach. The OPM (Personnel Investigations Records). Employees address records from Federal employers (e.g., OPM, Defense Finance and Accounting Service, Defense Manpower Data Center, Department of State, United States Postal Service, Library of Congress, the General Accountability Office, Death master files, the Executive Office of the President, Former Presidents Office, etc.) and address verification from cleared contractors and commercial vendors.

Exemptions claimed for the system:

Parts of this record system may be exempt under 5 U.S.C. 552a(k)(1), as applicable.

An exemption rule for this record system has been promulgated according to the 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.

[FR Doc. 2015-27745 Filed: 10/29/2015 8:45 am; Publication Date: 10/30/2015]