Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD-2016-OS-0064]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to add a system of records, DMDC 24 DoD, entitled "Defense Information System for Security (DISS)." The Office of the Secretary of Defense proposes to establish a new system of records to serve as the Department of Defense enterprise-wide information system for personnel security, providing a common, comprehensive medium to request, record, document, and identify personnel security actions within the Department including: determinations of eligibility and access to classified information, national security, suitability and/or fitness for employment, and HSPD-12 determination for Personal Identity Verification (PIV) to access government facilities and systems, submitting adverse information, verification of investigation and/or adjudicative status, support of continuous evaluation and insider threat, prevention, and mitigation activities.

DISS consists of two applications, the Case Adjudication Tracking system (CATS) and the Joint Verification System (JVS). CATS is used by the DoD Adjudicative Community for the purpose of recording eligibility determinations. JVS is used by DoD Security Managers and Industry Facility Security Officers for the purpose of verifying eligibility, recording access determinations, submitting incidents for subsequent adjudication, and visit requests from the field (worldwide). These records may also be used as a management tool for statistical analyses, tracking, reporting, evaluating program effectiveness, and conducting research.

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 for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, 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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPD2), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

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 May 19, 2016, 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: May 24, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DMDC 24 DoD

System name:

Defense Information System for Security (DISS)

System location:

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

Categories of individuals covered by the system:

All Armed Forces personnel; DoD and U.S. Coast Guard civilian personnel, contractor employees, and applicants; other federal personnel with authorized access to DISS or for reciprocity purposes; "affiliated" personnel (e.g., Non-Appropriated Fund employees, Red Cross volunteers and staff, USO personnel, and congressional staff members); industry personnel requiring DISS access for personnel security

purposes; and individuals with access to National Security Information (NSI), Sensitive Compartmented Information and/or assignment to a sensitive position.

Categories of records in the system:
Name (current, former and alternate names); Social Security Number (SSN); DoD Identification Number (DoD ID); date of birth; place of birth; gender; marital status; personal cell and home telephone number; personal e-mail address; country of citizenship; type of DoD affiliation; employing activity; current employment status; photo; position sensitivity; personnel security investigative basis; status of current adjudicative action; security clearance eligibility status and access status; suitability and/or fitness determination for employment eligibility status, HSPD-12 determination for Personnel Identity Verification (PIV) eligibility status; whether eligibility determination was based on a condition (personal, medical, or financial), deviation or waiver of prescribed investigative standards or adjudication guidelines; security-related incident reports, to include issue files and information identified through continuous evaluation which may require additional investigation or adjudication; foreign travel and foreign contacts; self-reported information; eligibility recommendations or

decisions made by an appellate authority, Department of Hearings and Appeals (DOHA), and/or Component Personnel Security Appeals Boards for due process; non-disclosure execution dates; indoctrination date(s); level(s) of access granted; and debriefing date(s) and reasons for debriefing. Records documenting investigation status, adjudications, and outcomes conducted by Federal investigative organizations (e.g., U.S. Office of Personnel Management (OPM), Central Intelligence Agency, etc.) or DoD agencies; Continuous Evaluation flags and/or locator references to such investigations. Investigative file is available to adjudicators only.

Authority for maintenance of the system:
5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; E.O. 12333, United States Intelligence Activities; E.O. 12829, National Industrial Security Program; E.O. 10450, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information Within Industry; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security

Information; E.O. 12968, Access to Classified Information; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoD Directive (DoDD) 5205.16, The DoD Insider Threat Program; DoDD 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2-R, Department of Defense Personnel Security Program; DoD Manual 5105.21, Volume 1, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security; DoDI 1304.26, Qualification Standards for Enlistment, Appointment, and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12, Policy for Common

Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

Purpose(s):

DISS is a DoD enterprise information system for personnel security, providing a common, comprehensive medium to request, record, document, and identify personnel security actions within the Department including: determinations of eligibility and access to classified or national security information, suitability, and/or fitness for employment, and HSPD-12 determination for Personal Identity Verification (PIV) to access government facilities and systems, submitting adverse information, verification of investigation and/or adjudicative status, support of continuous evaluation and insider threat detection, prevention, and mitigation activities.

DISS consists of two applications, the Case Adjudication Tracking system (CATS) and the Joint Verification System (JVS). CATS is used by the DoD Adjudicative Community for the purpose of recording eligibility determinations. JVS is used by DoD Security Managers and Industry Facility Security Officers for the purpose of verifying eligibility, recording

access determinations, submitting incidents for subsequent adjudication, and visit requests from the field (worldwide).

These records may also be used as a management tool for statistical analyses, tracking, reporting, evaluating program effectiveness, and conducting research.

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, the records contained herein, with the exception of U.S. Office of Personnel Management (OPM) Federal Investigative Services (FIS) records which must be requested directly from OPM FIS, may specifically be disclosed outside the DoD as follows:

To the White House to obtain approval of the President of the United States regarding certain military personnel office actions as provided for in DoD Instruction 1320.4, Military Officer Actions Requiring Approval of the Secretary of Defense or the President, or Confirmation by the Senate.

To the U.S. Citizenship and Immigration Services for use in alien admission and naturalization inquiries.

To a Federal agency and its employees who are eligible to have a security clearance and/or have access to classified national security information in order to ensure that the agency is informed about information that relates to and/or impacts its employees eligibility to have a security clearance and/or access to classified national security information.

To a Federal agency with contractor personnel who are eligible to have a security clearance and/or have access to classified national security information in order to ensure that the agency is informed about information that relates to and/or may impact the contractor's eligibility to have a security clearance and/or access to classified national security information.

To a contractor with an active Facility Clearance and employees who are eligible to have a security clearance and/or have access to classified national security information in order to ensure that the employer is informed about information that relates to and/or may impact its

employees eligibility to have a security clearance and/or access to classified national security information.

To disclose information to contractors, grantees, experts, consultants, or volunteers performing or working on a contract, service, or job for the Federal Government. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.

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.

Disclosure When Requesting Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local

agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

Disclosure of Requested Information Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the

United States Government, is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

To a Federal, State, local, foreign, tribal, or other public authority the fact that this system of records contains information relevant to the retention of an employee, or the

retention of a security clearance, contract, license, grant, or other benefit. The other agency or licensing organization may then make a request supported by written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative personnel, or regulatory action.

Private Relief Legislation Routine Use: Relevant information contained in all systems of records of the Department of Defense published on or before August 22, 1975, will be disclosed to the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular A-19, at any stage of the legislative coordination and clearance process as set forth in that Circular.

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 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 Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.

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.

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 or the U.S. Government 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 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.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Electronic storage media and paper records.

Retrievability:

Information is retrieved by SSN, DoD ID number, name, date of birth, state and/or country of birth, or some combination thereof.

Safeguards:

Access to personal information is restricted to those who require the records in the performance of their official duties, who are appropriately screened, investigated, and determined eligible for access. Access to personal information is further restricted by the use of Personal Identity Verification (PIV) cards for JVS and CATS. Access to self-report information by the subject is available by the use of a PIV. Physical entry is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to DISS must complete initial Information Assurance and Privacy Act training and annually

thereafter; and all have been through the information technology and/or security clearance eligibility process.

Retention and disposal:
Records are destroyed no later than 16 years after termination of affiliation with the DoD, from the date of closing or the date of the most recent investigative activity, whichever is later except for investigations involving potentially actionable issue(s) which will be maintained for 25 years from the date of closing or the date of the most recent investigative activity.

For OPM FIS investigative reports within CATS, those records will be maintained in accordance with General Records Schedule 18 part 22 (a), and destroyed upon notice of death or not later than 5 years after the subject has separated/transferred.

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

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) Boyers, ATTN: Privacy Act Office, P.O. Box 168, Boyers, PA 16020-0168.

Signed, written requests must contain the full name (and any alias and/or alternate names used), SSN, DoD ID Number, 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 Defense Manpower Data Center (DMDC) Boyers, ATTN: Privacy Act Office, P.O. Box 168, Boyers, PA 16020-0168.

Signed, written request must contain their full name (and any alias and/or alternate names used), SSN, DoD ID Number, 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.

Note: Information generated, authored, or compiled by Another Government Agency (AGA) that is relevant to the purpose of the record may be incorporated into the record. In such instances that information will be referred to the originating entity for direct response to the requester, or contact information and record access procedures for the AGA will be provided to the requester.

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:
Information contained in this system is obtained from the individual (e.g. SF-85, Questionnaire for Non-Sensitive Positions, SF-85P, Questionnaire for Public Trust Positions, SF-86, Questionnaire for the National Security Positions, or self-reported information); DoD personnel systems (e.g. Defense Enrollment Eligibility Reporting System; Defense Civilian Personnel Data System; Electronic Military Personnel Record System, etc.); continuous evaluation records; DoD and federal adjudicative facilities/organizations; investigative agencies (e.g. Office of Personnel Management (OPM) Federal Investigative Services (FIS); and security managers, security officers, or other officials requesting and/or sponsoring the security eligibility or suitability determination or visitation of facility. Additional information may be obtained from other sources such as personnel security investigations, criminal or civil investigations, security representatives, subject's personal financial records,

military service records, travel records, medical records, and unsolicited sources.

Exemptions claimed for the system:
Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

An exemption rule for this system has been promulgated in accordance with 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. 2016-14182 Filed: 6/14/2016 8:45 am; Publication Date: 6/15/2016]