BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2018-OS-0076]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, DoD.

ACTION: Notice of a new System of Records.

SUMMARY: The Office of the Secretary of Defense (OSD) proposes to establish a new system of records, "Personnel Vetting Records System," DUSDI 02-DoD. The system supports the Department of Defense (DoD) in conducting end-to-end personnel security, fitness, suitability, and credentialing processes, including application and questionnaire submission, investigations, adjudications, and continuous vetting activities. The Personnel Vetting Records System integrates DoD information technology capabilities developed to support the execution of federal background investigation activities, including: investigations and determinations of eligibility for access to classified national security information, eligibility to occupy a sensitive position, and for access to special access programs; suitability for federal employment; fitness of contractor personnel to perform work for or on behalf of the U.S. Government, and Homeland Security Presidential Directive (HSPD)-12 determinations for Personal Identity Verification (PIV) credentials to gain logical or physical access to government facilities and systems. The Personnel Vetting Records System also supports: submissions of adverse personnel information; verification of investigation and adjudicative history and status; support of continuous evaluation (CE); and insider threat detection, prevention, and mitigation activities. The system may also be used as a management tool for statistical analyses; tracking, reporting, and evaluating program effectiveness; and conducting research related to personnel vetting.

DATES: This SORN, with the exception of routine uses, is effective on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Routine Uses will be effective [INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Comments will be accepted on or before [INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

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 Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, 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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mr. Mark Nehmer, Technical Director, Defense Security Enterprise / Federal Vetting Enterprise Program Executive Office, Building 600, 10th Street, Ft. George G. Meade, MD, 20755; by email at Mark.A.Nehmer.civ@mail.mil or by phone at (301) 833-3488.

SUPPLEMENTARY INFORMATION: The OSD is proposing to establish a system of records that will be integral to the Federal Government's need to conduct background

investigations and make vetting decisions for persons who are proposed for new or continuing access to classified national security information, eligibility to positions with sensitive duties, enlistment or appointment into a military service, federal employment, assignment to contractual duties in support of federal requirements, or physical or logical access to U.S. Government systems or facilities.

As background, in January 2016 the Federal Government announced a series of changes to modernize and strengthen how the Federal Government performs and safeguards background investigations for federal employees, military personnel, and contractor personnel. The changes resulted from a review conducted by the interagency Performance Accountability Council (PAC) to re-examine reforms to the federal background investigations process, assess additional enhancements to further secure information networks and systems, and determine improvements that could be made to the way the Federal Government conducts background investigations for suitability, security, and credentialing (SSC).

One of the actions resulting from the PAC review was a direction to leverage expertise at the DoD for processing background investigations and protecting against threats. DoD was therefore assigned the responsibility to design, build, test, operate, and secure the National Background Investigation System (NBIS), a federal government-wide information technology system for conducting federal SSC investigations and adjudications. Specific direction for the Secretary of Defense to design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, vetting information technology systems is stated in subsection 2.6(b) of Executive Order 13467, as amended by Executive Order 13764, issued on January 23, 2017. Requirements for NBIS elements and enhancements were also passed into law

by the National Defense Authorization Acts for fiscal years 2017 and 2018 (PL 114-328, paragraph 951(f)(1), and PL 115-91, paragraph 925(f)(1), respectively)).

This Privacy Act system of records consists of background investigation information collected, created, and compiled in connection with authorized personnel security background investigations, adjudications, and continuous vetting activities conducted by the DoD.

The OSD notices for systems of records subject to the Privacy Act of 1974, as amended, are published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at https://defense.gov/privacy.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on September 5, 2018, to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated: October 11, 2018.

Shelly E. Finke,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Personnel Vetting Records System, DUSDI 02-DoD.

SECURITY CLASSIFICATION: Unclassified and Classified. This system of records consists of linked information systems and records that support DoD's personnel security, suitability, fitness, and credentialing processes. Some of these systems may contain classified information.

SYSTEM LOCATION: Defense Information Systems Agency (DISA), DISA Defense Enterprise Computing Center (DECC), 3990 E Broad St, Columbus, OH 43213-1152.

SYSTEM MANAGER(S): Mr. Mark Nehmer, Technical Director, Defense Security Enterprise / Federal Vetting Enterprise Program Executive Office, Building 600, 10th Street, Ft. George G. Meade, MD, 20755; by email at Mark.A.Nehmer.civ@mail.mil or by phone at (301) 833-3488.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 137, Under Secretary of Defense for Intelligence; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: Qualifications, term, grade; Atomic Energy Act of 1954, 60 Stat. 755; Public Law 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 401 note); Public Law 114-92, Section 1086, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Reform and Improvement of Personnel Security, Insider Threat Detection and Prevention, and Physical Security (10 U.S.C. 1564 note); Public Law 114-328, Section 951 (NDAA for FY2017), Enhanced Security Programs for Department Defense Personnel and Innovation Initiatives (10 U.S.C. 1564 note); Public Law 115-91, Section 925, (NDAA for FY2018) Background and Security Investigations for Department of Defense Personnel (10 U.S.C. 1564 note); 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; Executive Order (E.O.) 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities; E.O. 12333, as

amended, United States Intelligence Activities; E.O. 12829, as amended, National Industrial Security Program; E.O. 10865, as amended, Safeguarding Classified Information Within Industry; E.O. 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 12968, as amended, Access to Classified Information; E.O. 13470, Further Amendments to Executive Order 12333; E.O. 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13526, Classified National Security Information; E.O. 13741, Amending Executive Order 13467, To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; E.O. 13764, Amending the Civil Service Rules; DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP); DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: This system of records allows DoD to conduct end-to-end personnel security, suitability, fitness, and credentialing processes, including application and questionnaire submission, investigations, adjudications, and continuous vetting (including continuous evaluation) activities.

DoD developed the information technology capabilities that contribute to the Personnel Vetting Records System to support federal background investigation processes pursuant to Executive Order 13467, as amended, and Section 925 of the National Defense Authorization Act (NDAA) for FY2018. The Personnel Vetting Records System integrates information technology capabilities to conduct background investigations activities including: investigations and determinations of eligibility for access to classified national security information, and for access to special access programs; suitability for federal employment; fitness of contractor personnel to perform work for or on behalf of the U.S. Government; and Homeland Security Presidential Directive (HSPD)-12 determinations for Personal Identity Verification (PIV) credentials to gain logical or physical access to government facilities and systems. The Personnel Vetting Records System also supports: submissions of adverse personnel information; verification of investigation and adjudicative history and status; continuous evaluation; and insider threat detection, prevention, and mitigation activities.

Records in the information systems covered by this system notice may also be used as a management tool for statistical analyses; tracking, reporting, and evaluating program effectiveness; and conducting research related to personnel vetting. This system notice does not cover personnel vetting records (including investigation and adjudication records) collected or retained separately by those DoD Components with specific personnel vetting authorities and that conduct their own investigations and vetting, or by non-DoD agencies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Personnel for whom DoD conducts or adjudicates background investigations for security, suitability, fitness, and credentialing. This includes Armed Forces personnel; DoD and U.S. Coast Guard civilian personnel, DoD contractor personnel and consultants, and applicants for those positions; civilian

employees, contractor personnel and consultants, and applicants for those positions, working for or on behalf of other federal agencies and offices, for whom DoD conducts background investigations; other government personnel who have authorized access to the system for reciprocity purposes; "affiliated" personnel (e.g., Non-Appropriated Fund employees, Red Cross volunteers and staff, USO personnel, and congressional staff members); and other individuals (including contractor personnel of other government entities and foreign nationals) requiring a DoD determination for fitness, HSPD-12 access, access to classified national security information, Sensitive Compartmented Information, and/or assignment to a position with sensitive duties; and officials or employees of State, local, tribal and private sector entities sponsored for access to classified information by a federal agency.

CATEGORIES OF RECORDS IN THE SYSTEM: Name (current, former and alternate names); Social Security Number (SSN); DoD Identification Number (DoD ID Number); date of birth; place of birth; height; weight; hair and eye color; gender; sex; mother's maiden name; residential history, phone numbers, and e-mail addresses; employment history; military records and discharge information; selective service registration record; educational data, including conduct records and degrees earned; names of relatives, associates and references with their contact information; country(ies) of citizenship; travel, immigration, and passport information; mental health history; records related to drug and/or alcohol use; financial record information; information from the Internal Revenue Service pertaining to income tax returns; bureau of vital statistics records (e.g., birth certificate, death certificate, marriage application and license); credit reports; prior security clearance and investigative information; type of DoD affiliation; employing activity; current employment status; position sensitivity; personnel security investigative basis; status of current adjudicative action; security clearance eligibility status and

access status; self-reported information; eligibility recommendations or decisions made by an appellate authority; inadvertent disclosure briefing and agreement; non-disclosure execution dates; indoctrination date(s); level(s) of access granted; briefing/debriefing date(s) and reasons for briefing/debriefing; and other biographical information as required during the course of a background investigation.

Records documenting the outcomes of investigations and adjudications conducted by other Federal investigative organizations (e.g., U.S. Office of Personnel Management (OPM), Federal Bureau of Investigation (FBI), National Aeronautics and Space Administration (NASA), etc.) and locator references to such investigations. Entries documenting fitness determinations, HSPD-12 access, continuous vetting adverse information flags, or counter insider threat reports of the subject.

Name, date and place of birth, social security number, country of citizenship, criminal history and prior security clearance and investigative information for spouse or cohabitant(s); the name and marriage information for current and/or former spouse(s); the country(ies) of citizenship, name, date and place of birth, contact information (e.g., phone numbers, email addresses), and address for relatives.

Reports from pre-employment screening, such as counterintelligence screening or military accessions vetting; results of subject and reference interviews conducted during the course of background investigations, continuous evaluation, counter insider threat, counterintelligence screening, security incident resolution, or program access requests.

Information detailing agency investigation requests including type of investigation requested, tracking codes, and requesting officials' contact information.

Polygraph reports, polygraph charts, polygraph tapes and recordings in other forms, and notes from polygraph interviews or activities related to polygraph interviews.

Biometric information including but not limited to images and fingerprints; criminal and civil fingerprint history information.

Foreign contact, affections, associates (e.g., family members, friends or social contacts), travel, and activities information, including names of individuals known, dates, country(ies) of citizenship, country(ies) of residence, type and nature or contact, financial interests, assets, benefits from foreign governments, countries and dates of arrival and departure for U.S. border crossings; association records; information on loyalty to the United States.

Criminal history information, including information contained in local, state, military, Federal, and foreign criminal justice agency records and local, state, military, and Federal civil and criminal court records. Information about affiliation with known criminal and/or terrorist organizations.

Records concerning civil or administrative proceedings, (for example, bankruptcy records, civil lawsuits, Merit System Protection Board), including information contained in local, state, military, Federal, and foreign courts and agency records.

Information about and evidence of unauthorized use or misuse of information technology systems.

Information aggregated in counter-insider threat inquiries or investigations, including payroll information, travel vouchers, benefits information, equal employment opportunity complaints, performance evaluations, disciplinary files, training records, substance abuse and mental health records of individuals undergoing law enforcement action or presenting an identifiable imminent threat, counseling statements, outside work and activities requests, and personal contact records;

particularly sensitive or protected information, including information held by special access programs, law enforcement, inspector general, or other investigative sources or programs. Access to such information may require additional approval by the senior official who is responsible for managing and overseeing the program; information related to reports regarding harassment or discrimination.

Information collected through user activity monitoring, which is the technical capability to observe and record the actions and activities of all users, at any time, on a computer network controlled by a government agency in order to deter, detect, and/or mitigate insider threats as well as to support authorized investigations. Such information may include key strokes, screen captures, and content transmitted via email, chat, or data import or export.

Agency or Component summaries of reports, and full reports, about potential insider threats from records of usage of government telephone systems, including the telephone number initiating the call, the telephone number receiving the call, and the date and time of the call.

U.S. and foreign finance and real estate information that consists of names of financial institutions, number of accounts held, monthly and year-end account balances for bank and investment accounts, address, year of purchase and price, capital investment costs, lease or rental information, year of lease or rental, monthly payments, deeds, lender/loan information and foreclosure history; information on owned and leased vehicles, boats, airplanes and other U.S. and foreign assets that include type, make, model, year, plate or identification number, year leased, monthly rental payment; year of purchase and price, and fair market value; information pertaining to large or suspicious currency transactions; U.S. and foreign mortgages, loans, and liabilities information that consist of type of loan, names and addresses of creditors, original balance, monthly and year-end balance, monthly payments, and payment history.

Publicly available electronic information about or generated by a covered individual (e.g., public records, civil court records, social media content, news articles, and web blog information). Results of record checks and data analyses for purposes of improving all types of investigations, reinvestigations, or continuous evaluation with respect to efficiency or cost-effectiveness.

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 provided in other forms, such as interviews); DoD personnel and other record systems (e.g. Defense Enrollment Eligibility Reporting System; Defense Civilian Personnel Data System; Electronic Military Personnel Record System, Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System, etc.); continuous evaluation records; DoD and Federal investigative and adjudicative facilities/organizations; other Federal agency records and/or systems of records (as authorized by their routine use clauses in system of records notices) that provide security-relevant information; and security managers, security officers, or other officials requesting or sponsoring an individual for security eligibility, suitability, fitness or credentialing determination, or determinations concerning access to facilities. Additional information may be obtained from Federal, State, local, or tribal government entities, including information from criminal or civil investigations, courts, law enforcement agencies, agencies authorized to collect information concerning citizenship, probation officials, prison officials, information technology officials, and security representatives. Information also may be obtained from other publicly available information sources, commercial data providers (e.g., credit reporting companies and online news sources), past and present employers, personal references and associates, relatives,

neighbors, education institutions, subject's personal financial records, military service records, travel records, medical records, and unsolicited sources.

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, may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To Federal, State, and local government agencies, if necessary, to obtain information from them which will assist DoD in conducting studies and analyses in support of evaluating and improving the effectiveness of personnel security, suitability, and credentialing programs and methodologies.

b. To the Federal Bureau of Investigation and U.S. Office of Personnel Management personnel to help ensure the accuracy and completeness of FBI, OPM, and DoD records.

c. To the Office of Personnel Management, the Office of the Director of National Intelligence, and other federal government agencies responsible for conducting background investigations, continuous evaluation, and continuous vetting in order to provide them with information relevant to their inquiries and investigations.

d. To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies, or other public authorities, or to other offices or establishments in the executive, legislative, or judicial branches of the Federal Government, in connection with the hiring or retention of an employee, the conduct of a suitability, credentialing, or security investigation, the classifying of jobs, 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 and the Department deems appropriate.

e. To designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government or the Government of the District of Columbia having a need to investigate, evaluate, or make a determination regarding loyalty to the United States; qualification, suitability, or fitness for Government employment or military service; eligibility for logical or physical access to federally-controlled facilities or information systems; eligibility for access to classified information or to hold a sensitive position; qualification or fitness to perform work for or on behalf of the Government under contract, grant, or other agreement; or access to restricted areas.

f. To an element of the U.S. Intelligence Community as identified in E.O. 12333, as amended, for use in intelligence activities for the purpose of protecting the United States national security interests.

g. To an agency, office, or other establishment in the executive, legislative, or judicial branches of the Federal Government in response to its request, in connection with its current employee's, contractor employee's, or military member's retention; loyalty; qualifications, suitability, or fitness for employment; eligibility for logical or physical access to federally-controlled facilities or information systems; eligibility for access to classified information or to hold a sensitive position; qualifications or fitness to perform work for or on behalf of the Government under contract, grant, or other agreement; or access to restricted areas.

h. To contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or assignment for the Federal Government, when necessary to

accomplish an agency function related to this system of records. Such recipients shall be required to comply with the Privacy Act of 1974, as amended.

i. To the appropriate Federal, State, local, tribal, foreign, or other public authority in the event of a natural or manmade disaster. The record will be used to provide leads to assist in locating missing subjects or assist in determining the health and safety of the subject. The record will also be used to assist in identifying victims and locating any surviving next of kin.

j. For agencies that use adjudicative support services of another agency, at the request of the original agency, the information may be furnished to the agency providing the adjudicative support.

k. 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 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.

l. To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual under investigation, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

m. To contractors whose employees require fitness determinations, or eligibility for access to classified national security information, for the purpose of ensuring that the employer is appropriately informed about the status of the employee's application for a fitness or eligibility determination.

n. To provide information 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. However, the

investigative file, or parts thereof, will only be released to a congressional office if DoD receives a notarized authorization or signed statement under 28 U.S.C. 1746 from the subject of the investigation.

o. To the Director of National Intelligence, as Security Executive Agent, the Director of the Office of Personnel Management, as Suitability Executive Agent or Credentialing Executive Agent, or their assignee, to perform any functions authorized by law or executive order in support of personnel security programs, suitability, and/or credentialing. Examples include the Intelligence Reform and Terrorism Prevention Act and E.O. 13741—Amending Executive Order 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters.

p. To the White House to obtain approval of the President of the United States regarding certain military personnel officer actions as provided for in DoD Instruction 1320.04, Military Officer Actions Requiring Approval of the President, Secretary of Defense or the Under Secretary of Defense for Personnel and Readiness Approval, or Confirmation by the Senate.

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

r. For the Merit Systems Protection Board —To disclose information to officials of the Merit Systems Protection Board or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of applicable agency rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, e.g., as promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

s. To disclose information to an agency Equal Employment Opportunity (EEO) office or to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discriminatory practices in the Federal sector, or in the processing of a Federal sector EEO complaint.

t. To disclose information to the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

u. To another Federal agency's Office of Inspector General when DoD becomes aware of an indication of misconduct or fraud during the applicant's submission of the standard forms.

v. To another Federal agency's Office of Inspector General in connection with its inspection or audit activity of the investigative or adjudicative processes and procedures of its agency as authorized by the Inspector General Act of 1978, as amended, exclusive of requests for civil or criminal law enforcement activities.

w. To a Federal agency or state unemployment compensation office upon its request in order to adjudicate a claim for unemployment compensation benefits when the claim for benefits is made as the result of a qualifications, suitability, fitness, security, identity credential, or access determination.

x. To appropriately cleared individuals in Federal agencies, to determine whether information obtained in the course of processing the background investigation is or should be classified.

y. To the Office of the Director of National Intelligence for inclusion in its Scattered Castles system in order to facilitate reciprocity of background investigations and security clearances within the intelligence community or assist agencies in obtaining information required by the Federal Investigative Standards.

z. To the Office of Personnel Management (OPM) for the purpose of addressing civilian 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.

aa. A record from this system may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence, counterterrorism, and homeland defense 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; this includes disclosure to Executive Branch Agency insider threat, counterintelligence, and counterterrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, 13587 and the National Insider Threat Policy and Minimum Standards.

bb. 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, 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 and 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.

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

dd. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official (including to another Federal agency or party in litigation in such a proceeding,

as well as to the 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.

ee. 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.

ff. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that 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.

gg. 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in paper and electronic storage media, in accordance with the safeguards below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Information is retrieved by SSN, case number, DoD ID number, name, date of birth, state and/or country of birth, or some combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Draft Records Retention/Disposition Schedule is currently in development, pending submission to and approval from the Archivist of the United States, National Archives and Records Administration (NARA). Unscheduled NBIS records will be treated as permanent until receipt of retention/disposition instruction approval from the Archivist of the United States, NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The system is protected against compromise of Personally Identifiable Information (PII) and cyberattack by the full suite of defenses and sensors of the DoD cybersecurity perimeter. Electronic data is encrypted where it is stored, and network traffic is encrypted based on the type of user traffic and risk to PII data. User access to data is protected using Identity and Access Management with multifactor authentication that will only allow an authenticated and authorized user to access or manipulate the specific records based on user role and permissions. The system audits access to information. Paper records are contained and stored in safes and locked filing cabinets that are located in a secure area with access only by authorized personnel. Physical entry is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to the system must complete Information Assurance and Privacy Act training before initially accessing the system and annually thereafter, and these users must have also been adjudicated as being eligible for system access through the information technology credentialing and/or security clearance eligibility process.

RECORD ACCESS PROCEDURES: Individuals seeking information about themselves contained in this system should address written inquiries to the Defense Security Service, Office of FOIA and PA, 27130 Telegraph Road, Quantico, VA 22134-2253. Requests for vetting records not covered by this system notice, including vetting records maintained by other DoD Components and other federal agencies, should be addressed to those DoD Components and federal agencies.

Signed, written requests should contain the requester's full name (and any alias and/or alternate names used), SSN, DoD ID Number (if available), and date and place of birth.

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 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 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 other agency will be provided to the requester.

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

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Defense Security Service, Office of FOIA and PA, 27130 Telegraph Road, Quantico, VA 22134-2253. Requests for vetting records not covered by this systems notice, including vetting records maintained by other DoD Components and other federal agencies, should be addressed to those DoD Components and federal agencies.

Signed, written requests should contain the requester's full name, telephone number, street address, email address, and name and number of this system of records notice.

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 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)."

EXEMPTIONS CLAIMED FOR THE SYSTEM: The DoD is exempting records maintained in DUSDI 02-DoD "Personnel Vetting Records System," from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (2), (3), (5), (6), and (7). In addition, in the course of carrying out personnel vetting, including records checks for

continuous vetting, exempt records from other systems of records may in turn become part of the records maintained in this system. To the extent that copies of exempt records from those other systems of records are maintained in this system, the Department also claims the same exemptions for the records from those other systems that are maintained in this system, as claimed for the original primary system of which they are a part.

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 310. For additional information contact the system manager.

HISTORY: None

[FR Doc. 2018-22508 Filed: 10/16/2018 8:45 am; Publication Date: 10/17/2018]