DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2021-0006; 223D0102DM, DLSN00000.000000, DS65100000, DX.65101]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, Interior.

ACTION: Notice of a modified system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) is issuing a public notice of its intent to modify the Privacy Act system of records, INTERIOR/DOI-45, HSPD-12: Identity Management System and Personnel Security Files. DOI is revising this notice to update the title of the system, update all sections of the system notice, propose new and modified routine uses, and provide general administrative updates to the remaining sections of the notice. Additionally, DOI is publishing a notice of proposed rulemaking (NPRM) elsewhere in the *Federal Register* to exempt this system of records from certain provisions of the Privacy Act. This modified system will be included in DOI's inventory of record systems.

DATES: This modified system will be effective upon publication. New or modified routine uses will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]. Submit comments on or before [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments identified by docket number [DOI-2021-0006] by any of the following methods:

- Federal eRulemaking Portal: *https://www.regulations.gov*. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2021-0006] in

the subject line of the message.

- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2021-0006]. All comments received will be posted without change to *https://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *https://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240, DOI_Privacy@ios.doi.gov or (202) 208-1605.

SUPPLEMENTARY INFORMATION:

I. Background

The DOI Office of Law Enforcement and Security (OLES) maintains the INTERIOR/DOI-45, HSPD-12: Identity Management System and Personnel Security Files, system of records. This system supports the DOI Personnel Security Program functions to determine suitability, eligibility, and fitness for service of applicants for Federal employment and contract positions or individuals appointed to commissions and boards, including Bureau of Indian Education agency or local school boards, who require access to Departmental facilities, information systems and networks. The system also helps OLES manage a National Security Program to document and support decisions regarding clearance access to classified information and implement provisions that apply to Federal employees and contractors who access classified information or materials and participate in classified activities that impact national security, and ensure the safety, storage of classified information and security of Departmental facilities, information

systems and networks, occupants, and users.

DOI last published the INTERIOR/DOI-45, HSPD-12: Identity Management System and Personnel Security Files, system notice in the *Federal Register* on March 12, 2007 (72 FR 11036), modification published at 86 FR 50156 (September 7, 2021). DOI is publishing this revised notice to reflect the expanded scope of the modified system of records to meet personnel security and national security requirements outlined in Federal law, Executive Orders, and Intelligence Community (IC) policy for security clearance and access determinations, access to Sensitive Compartmented Information (SCI) reciprocity, exceptions to personnel security standards, and safeguarding classified information and secure facilities. DOI is proposing to change the title to INTERIOR/DOI-45, Personnel Security Program Files, to accurately reflect the purpose and scope of the system of records; update the system manager and system location; expand on categories of individuals covered by the system, the categories of records and records source categories sections; update authorities for maintenance of the system; update storage, safeguards, and records retention schedule; update the notification, records access and contesting procedures; and provide general updates in accordance with the Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

DOI personnel security records are maintained in DOI Bureau and Office Personnel Security Offices and in the National Background Investigation Services (NBIS) system managed by the Department of the Defense (DoD), Defense Counterintelligence and Security Agency (DCSA). The DCSA conducts background investigations, end-to-end personnel security, suitability, fitness, and credentialing processes, investigations, adjudications, and continuous vetting activities on behalf of Federal agencies. The records created and managed by DCSA belong to the DCSA and are covered by the DoD system of records notice (SORN), DUSDI 02-DoD, Personnel

Vetting Records System (October 17, 2018; 83 FR 52420). Copies of these decentralized records may be in the custody of DOI, but are owned by DoD and are subject to the DoD SORN. To the extent that individuals are seeking access to their background investigation records owned and managed by the DoD, individuals must follow the instructions in the DUSDI 02-DoD SORN and must submit a Privacy Act request for access, notification or amendment to the DoD system manager.

This notice covers the records created and managed by DOI to support personnel security activities and document evaluations and decisions regarding suitability, eligibility, and fitness for service of applicants for Federal employment and contract positions to the extent necessary to manage secure access to Departmental facilities, information systems and networks, and to manage access to classified information and reciprocity.

DOI is also changing the routine uses from a numeric to alphabetic list and is proposing to modify existing routine uses to provide clarity and transparency and reflect updates consistent with standard DOI routine uses. Routine use A has been modified to further clarify disclosures to the Department of Justice or other Federal agencies when necessary in relation to litigation or judicial proceedings. Routine use B has been modified to clarify disclosures to a congressional office to respond to or resolve an individual's request made to that office. Modified routine use E allows DOI to share information with other Federal agencies to assist in the performance of their responsibility to ensure records are accurate and complete, and to respond to requests from individuals who are the subject of the records. Routine use F facilitates sharing of information related to hiring, issuance of a security clearance, or a license, contract, grant or benefit. Routine use G has been modified to update the legal authority for the National Archives and Administration to conduct records management inspections. Routine use H has been modified to expand the sharing of information with territorial

organizations in response to court orders or for discovery purposes related to litigation. Routine use I has been modified to include the sharing of information with grantees of DOI that perform services requiring access to these records on DOI's behalf to carry out the purposes of the system. Routine use J was slightly modified to allow DOI to share information with appropriate Federal agencies or entities when reasonably necessary to prevent, minimize, or remedy the risk of harm to individuals or the Federal Government resulting from a breach in accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. Routine use L was modified to clarify sharing with OMB in relation to legislative affairs mandated by OMB Circular A-19. Routine use P was modified to expand the sharing of information with DoD and DCSA in support of personnel security programs, suitability, and/or credentialing. Routine use Q was modified to clarify that information is shared with the Federal Bureau of Investigation during background investigation activities.

Proposed new routine use C permits sharing of information with the Executive Office of the President to respond to an inquiry by the individual to whom that record pertains. Proposed routine use D allows DOI to refer matters to the appropriate Federal, state, local, or foreign agencies, or other public authority agencies responsible for investigating or prosecuting violations of, or for enforcing, or implementing, a statute, rule, regulation, order, or license. Proposed routine use M allows sharing with the Department of the Treasury to recover debts owed to the United States. Proposed routine use N allows sharing of information with the news media and the public, with approval by the Public Affairs Officer and Senior Agency Official for Privacy in consultation with counsel, where there is a legitimate public interest or in support of a legitimate law enforcement or public safety function. Proposed routine use R allows sharing with Federal agencies and organizations in the IC to manage accounts and access to systems, verify personnel security information, implement visitor control, and facilitate

information sharing and clearance reciprocity. Proposed routine use S allows sharing with other Federal agencies and organizations to report, investigate, and respond to a classified spillage or major security violation. Proposed routine use T allows sharing with Congressional committees that have oversight of personnel security programs, background investigations, and continuous vetting activities. Proposed routine use U allows the Merit Systems Protection Board or the Office of the Special Counsel to respond to requests related to appeals and civil service and other merit systems, review of applicable agency rules and regulations, investigations of personnel practices, and other functions. Proposed routine use V allows sharing with another Federal agency or organization for national security purposes to fulfill responsibilities under Federal law or Executive Order. Proposed routine use W allows sharing with other agencies under a shared service agreement with DOI for the processing or maintenance of records in this system.

In an NPRM published separately in today's *Federal Register*, DOI is proposing to exempt records maintained in this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6).

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under

the control of DOI by complying with DOI Privacy Act regulations at 43 CFR Part 2, Subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the *Federal Register* a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. The INTERIOR/DOI-45, Personnel Security Program Files, SORN is published in its entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Participation

You should be aware your entire comment including your personally identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER:

INTERIOR/DOI-45, Personnel Security Program Files.

SECURITY CLASSIFICATION:

Classified and Unclassified.

SYSTEM LOCATION:

The system is centrally managed by the Office of Law Enforcement and Security, Office of the Secretary, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 3428 MIB, Washington, DC 20240. Records are maintained in the NBIS system located at the Defense Information Systems Agency (DISA), Defense Enterprise Computing Center (DECC), 3990 E Broad St, Columbus, OH 43213. Records in this system are also maintained by DOI bureaus and offices that manage personnel security programs at the

following locations:

(1) Bureau of Indian Affairs, Office of Human Capital Management, Personnel Security Office, 1011 Indian School Road NW, Suite 273, Albuquerque, NM 87104.

(2) Bureau of Indian Education, Human Resources, Personnel Security Office, 1011 Indian School Road NW, Suite 150, Albuquerque, NM 87104.

(3) Bureau of Land Management, National Operations Center, Office of Security Operations, Denver Federal Center, Building 50, Denver, Colorado, 80225.

(4) Bureau of Ocean Energy Management, 45600 Woodland Road, Mail Stop VAE/PSB, Sterling VA 20166.

(5) Bureau of Reclamation, Policy and Programs Directorate, Security Division, Personnel Security and Suitability Program, P.O. Box 25007, Denver, CO 80225.

(6) Bureau of Safety and Environmental Enforcement, 45600 Woodland Road, Mail Stop VAE/PSB, Sterling VA 20166.

(7) National Park Service, Workforce & Inclusion Directorate, Personnel Security & Identity Management Group, 1849 C Street NW, Washington, DC 20240.

(8) Office of Surface Mining, Reclamation and Enforcement, Office of Human Resources, 1849 C Street NW, Mail Stop 1543 MIB, Washington, DC 20240.

(9) Office of Inspector General, 381 Elden Street, Suite 3000, Herndon, VA 20170.

(10) Office of the Solicitor, Division of Administration, 1849 C Street NW, Mail Stop 6556 MIB, Washington, DC 20240.

(11) U.S. Fish and Wildlife Service, 5275 Leesburg Pike, Mail Stop: JAO, Falls Church, VA 22041.

(12) U.S. Geological Survey, Office of Management Services, Security Management Branch, 12201 Sunrise Valley Drive, Mail Stop 250 National Center, Reston, VA 20192.

(13) Assistant Secretary-Indian Affairs, Office of Human Capital Management, Personnel Security, 12220 Sunrise Valley Drive, Reston, VA 20191.

SYSTEM MANAGER(S):

(1) Personnel Security Manager, Office of Law Enforcement and Security, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 3428 MIB, Washington, DC 20240.

(2) National Security Program Office Manager, Office of Law Enforcement and Security, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 3428 MIB, Washington, DC 20240. This official is responsible for the Classified National Security Information, the Sensitive Compartmented Information, and the Industrial Security Programs.

(3) Bureau Personnel Security System Managers:

(a) Bureau of Indian Affairs: Personnel Security Officer, Bureau of Indian Affairs, Office of Human Capital Management, Personnel Security Office, 1011 Indian School Road, NW, Suite 273, Albuquerque, NM 87104.

(b) Bureau of Indian Education: Personnel Security Specialist, Bureau of Indian Education, Human Resources, Personnel Security Office, 1011 Indian School Road NW, Suite 150, Albuquerque, NM 87104.

(c) Bureau of Land Management: Chief Security and Intelligence, Bureau of Land Management, Office of Law Enforcement and Security, 1620 L Street NW, Washington, DC 20036.

(d) Bureau of Ocean Energy Management, Personnel Security Officer, 45600 Woodland Road, Mail Stop VAE/PSB, Sterling VA 20166.

(e) Bureau of Reclamation: Lead Personnel Security Specialist, Bureau of Reclamation, P.O. Box 25007, Denver, CO 80225.

(f) Bureau of Safety and Environmental Enforcement: Personnel Security

Officer, 45600 Woodland Road, Mail Stop VAE/PSB, Sterling VA 20166.

(g) National Park Service: Security Officer, National Park Service, Workforce & Inclusion Directorate, Personnel Security & Identity Management Group, 1849 C Street, N.W., Washington, DC 20240.

(h) Office of Surface Mining, Reclamation and Enforcement: Personnel Security Officer, Office of Surface Mining, Reclamation and Enforcement, 1951 Constitution Avenue, NW, South Interior Building, Washington, DC 20240.

(i) Office of Inspector General: Security Specialist, Office of Inspector General, 381 Elden Street, Suite 3000, Herndon, VA 20170.

(j) Office of the Secretary/Interior Business Center: Security Manager, Interior Business Center, 1849 C Street NW, Mail Stop 1224 MIB, Washington, DC 20240.

(k) Office of the Solicitor: Director of Administrative Services, Division of Administration, Office of the Solicitor, 1849 C Street NW, Mail Stop 6556 MIB, Washington, DC 20240.

(l) U.S. Fish and Wildlife Service: Personnel Security Manager, U.S. Fish and Wildlife Service, 5275 Leesburg Pike, Mail Stop: JAO, Falls Church, VA 22041.

(m) U.S. Geological Survey: U.S. Geological Survey, Office of Management Services, Security Management Branch, 12201 Sunrise Valley Drive, Mail Stop 250 National Center, Reston, VA 20192.

(n) Assistant Secretary-Indian Affairs, Office of Human Capital Management, Personnel Security Specialist, 12220 Sunrise Valley Drive, Reston VA 20191.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

50 U.S.C. Ch. 23, Internal Security Act of 1950, as amended; National Security Act of 1947, as amended, Pub. L. 80-253; 40 U.S.C. 11331, Responsibilities for Federal information systems standards; Federal Property and Administrative Services Act of 1949, as amended, Pub. L. 81-152; E-Government Act of 2002, Pub. L. 107-347, section

203; 44 U.S.C. 3501-3520, Paperwork Reduction Act of 1995; 5 U.S.C. 301, Departmental regulations; 5 U.S.C. 3301, Civil service; generally; 5 U.S.C. 9101, Access to criminal history records for national security and other purposes; 42 U.S.C. 2165, Security restrictions; 42 U.S.C. 2201, General duties of Commission; 5 CFR Part 5, Regulations, Investigation, and Enforcement (Rule V); 5 CFR Part 732, National Security Positions; 5 CFR Part 736, Personnel Investigations; Executive Order (E.O.) 9397, as amended, Numbering System for Federal Accounts Relating to Individual Persons; E.O. 10450, as amended, Security Requirements for Government Employment; E.O. 10865, Safeguarding Classified Information within Industry; E.O. 12829, as amended, National Industrial Security Program; Executive Order 12333, as amended, United States Intelligence Activities; Executive Order 12968, as amended, Access to Classified Information; E.O. 13470, Further Amendments to Executive Order 12333, United States Intelligence Activities; 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; Security Executive Agent Directives; Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; 32 CFR Parts 2001 and 2003; and Federal Information Processing Standard (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors.

PURPOSE(S) OF THE SYSTEM:

The primary purposes of the system are:

(1) To document and support decisions regarding suitability, eligibility, and fitness for service of applicants for Federal employment, contractors and subcontractors,

students, interns, affiliates, or volunteers, or individuals appointed to commissions and boards, including Bureau of Indian Education agency or local school boards, to the extent their duties require regular, ongoing access to Departmental facilities and information systems and networks including clearance for access to classified information and Sensitive Compartmented Information (SCI) access;

(2) To prescribe a uniform system for classification management, safeguarding, and declassifying national security information;

(3) To ensure the safety and security of Departmental facilities, information systems and networks, occupants, and users; and

(4) To verify personnel security clearances, access to SCI, reciprocity, and documented exceptions to personnel security standards.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individuals who require regular, ongoing access to Departmental facilities, information systems and networks, that will grant them access to either classified and unclassified information in the interest of national security, including applicants for employment or contracts with DOI, Departmental employees, contractors, subcontractors, students, interns, volunteers, affiliates, or individuals appointed to commissions and boards, including Bureau of Indian Education agency or local school boards, and individuals formerly in any of these positions. In addition, it will cover individuals needing access to a uniform system of classification management.

(2) Employees of independent agencies, councils and commissions, which are provided administrative support by DOI.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Copies of forms submitted by individuals covered by this system including but not limited to: SF 85, Questionnaire for Non-Sensitive Positions; SF 85P, Questionnaire for Public Trust Positions; SF 85P-S, Supplemental Questionnaire for

Selected Positions; SF-86, Questionnaire for National Security Positions; SF 86C, Certification; SF 87 Fingerprint Chart; the FD 258 Applicant Fingerprint Card; and other forms and information provided by individuals.

(2) Personnel security records including but not limited to favorable or unfavorable adjudications related to suitability, fitness for service, credentialing, and continuous vetting, and approvals, denials, revocations, suspensions, waivers, deviations or eligibility-for-access determinations related to national security.

(3) Records of all collateral clearances, SCI access, and personnel security background investigations and adjudications granted or conducted by an IC element, to include pending and cancelled investigations or adjudications.

(4) Copies of letters of transmittal between DOI and the Department of Defense regarding the covered individual's background investigation.

(5) Copies of certification of clearance status and briefings and/or copies of debriefing certificates signed by the individual, as appropriate. Card files contain case file summaries, case numbers, and dispositions of case files following review.

(6) Copies of the annual Self-Inspection Report that is due to the Information Security Oversight Office (ISOO); loss, possible compromise, or unauthorized disclosure of classified information; mandatory review of declassified information report; and any report as stipulated by ISOO under the authority 32 CFR Parts 2001 and 2003.

(7) Records maintained on individuals issued credentials by the Department including personal identity verification (PIV) request form, PIV registrar approval signature, PIV card serial number, PIV card issue and expiration dates, personal identification number, emergency responder designation, copies of "I-9" documents including driver's license, birth certificate or other government issued identification used to verify identification. These records include information derived from those documents such as document title, document issuing authority, document number, or document

expiration date; level of national security clearance and expiration date; computer system user name; user access and permission rights, authentication certificates; and digital signature information.

These records may contain a combination of personally identifiable information on individuals including but not limited to: full name, former names, date of birth, place of birth, Social Security number (SSN), signature, home and work address, personal and official e-mail address, personal and official phone numbers, driver's license number, passport number, foreign passport, employment or travel visa, employment history, agency affiliation (i.e., employee, contractor or volunteer); military record including status, branch of service, entry and separation date, and type of discharge; residential history, education and degrees earned, names of associates and references and their contact information, citizenship, names of relatives, birthdates and places of relatives, citizenship of relatives, names of relatives who work for the Federal government, criminal history, mental health history, drug use, financial information, image (photograph), fingerprints, gender, hair color, eye color, height, weight; and background investigation, summary report of investigation, results of suitability decisions, level of security clearance, date of issuance of security clearance, and requests for appeal.

RECORD SOURCE CATEGORIES:

Information is obtained from a variety of sources including applicants for employment with DOI, employees, contractors, subcontractors, students, interns, volunteers, affiliates, or individuals appointed to commissions and boards, including Bureau of Indian Education agency or local school boards, individuals formerly in any of these positions, and individuals who are the subject of a background investigation through forms such as the SF-85, Questionnaire for Non-Sensitive Positions, SF-85P, Questionnaire for Public Trust Positions, SF-86, Questionnaire for the National Security Positions, and self-reported information provided in other forms; personal interviews;

employers' and former employers' records; other Federal agencies supplying data on covered individuals; Federal Bureau of Investigation criminal history records and other law enforcement databases; financial institutions and credit reports; medical records and health care providers; educational institutions; and individuals or Federal, state, local, territory, tribal entities or an individual as protected by the Freedom of Information Act.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(1) DOI or any component of DOI;

(2) Any other Federal agency appearing before the Office of Hearings and Appeals;

(3) Any DOI employee or former employee acting in his or her official capacity;

(4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

(5) The United States Government or any agency thereof when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office when requesting information on behalf of, and at the request of, the individual who is the subject of the record, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(k).

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf, or for a purpose compatible with the reason for which the records are collected or maintained, to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(k).

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, or contractor (including employees of the

contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records;

(2) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (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 DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI 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.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the

extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

O. To the Federal Protective Service and appropriate Federal, state, local or foreign agencies responsible for investigating emergency response situations or investigating or prosecuting the violation of or for enforcing or implementing a statute, rule, regulation, order or license, when DOI becomes aware of a violation or potential violation of a statute, rule, regulation, order or license.

P. To the Department of Defense, Defense Counterintelligence and Security Agency, 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 oversight or any functions authorized by law or executive order in support of personnel security programs, suitability, and/or credentialing.

Q. To the Federal Bureau of Investigation for the purpose of conducting background investigations and performing authorized audit and oversight functions.

R. To Federal agencies and organizations in the Intelligence Community to manage individual accounts and logical access to systems, verify personnel security information, and facilitate information sharing, visitor control, and clearance reciprocity.

S. To other Federal agencies and organizations as appropriate to report, investigate, and respond to a classified spillage and/or any major security violation.

T. To a Congressional committee with jurisdiction for oversight of matters pertaining to personnel security programs, background investigations, and continuous vetting activities.

U. To the Merit Systems Protection Board or the Office of the Special Counsel to disclose information 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.

V. To another Federal agency or organization when authorized and necessary for the purpose of national security, to include but not limited to, insider threat, counterintelligence, counterterrorism, and homeland defense activities to fulfill responsibilities under Federal law or Executive Order.

W. To another Federal agency or organization operating under a shared service agreement with DOI for the processing and maintenance of records and support related to the provision of personnel security and suitability services, to reconstitute the system in case of system failure or helpdesk request, and to ensure the integrity of the system and effective management of personnel security program functions.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper records are contained in file folders stored within filing cabinets in secured rooms. Electronic records are contained in computers, compact discs, computer tapes, removable drives, e-mail, diskettes, and electronic databases.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by name, SSN, and date of birth.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The Departmental Records Schedule (DRS), Administrative Records Bucket Schedule has superseded many of the General Records Schedule (GRS) items for security records. Personnel security records include questionnaires, summaries of reports prepared by the investigating agency, documentation of agency adjudication process and final determination, as well as case files of applicants not hired. The records disposition is temporary. Records are cut off one year after consideration of the candidate ends and

destroyed when no longer needed after cutoff (DRS 1.1.0003, DAA-0048-2013-0001-0003). For records maintained on individuals issued credentials by the Department including PIV request form, PIV registrar approval signature, PIV card serial number, PIV card issue and expiration dates, personal identification number, emergency responder designation, copies of "I-9" documents including driver's license, birth certificate or other government issued identification used to verify identification, the records disposition is temporary. The records are cut off at the end of the fiscal year in which files are closed and destroyed 7 years after cut off (DRS 1.1.0002, DAA-0048-2013-0001–0002). The Standard Form 312, Classified Information Nondisclosure Agreement (NDA), is covered under GRS 4.2 item 121 (DAA-GRS-2015-0002-0003) and requires longer retention. The disposition is temporary. SF 312 forms are destroyed 50 years after final signature.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The records contained in this system are safeguarded in accordance with 43 CFR 2.226 and other applicable security and privacy rules and policies. Paper records are maintained in locked file cabinets and/or safes under the control of authorized personnel during normal hours of operation. Computer servers on which electronic records are stored are located in secured DOI and DoD facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI or DoD network and information assets. Authorized DOI and DoD personnel must complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information before they are granted access to the system of records.

Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974, as amended, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C.

3501 et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq.; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Security controls include user identification, passwords, database permissions, encryption, firewalls, audit logs, and network system security monitoring and software controls which establish access levels according to the type of user. Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. Audit trails are maintained and reviewed periodically to identify unauthorized access or use. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior.

RECORD ACCESS PROCEDURES:

DOI is proposing to exempt portions of this system from the notification, access, and amendment procedures of the Privacy Act pursuant to sections (k)(1), (k)(2), (k)(3), (k)(5), and (k)(6). DOI will make access determinations on a case-by-case basis.

An individual requesting records on himself or herself should send a signed, written inquiry to the applicable System Manager identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked "PRIVACY ACT REQUEST FOR ACCESS." A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

DOI is proposing to exempt portions of this system from the notification, access, and amendment procedures of the Privacy Act pursuant to sections (k)(1), (k)(2), (k)(3),

(k)(5), and (k)(6). DOI will make amendment determinations on a case by case basis.

An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the applicable System Manager as identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

DOI is proposing to exempt portions of this system from the notification, access, and amendment procedures of the Privacy Act pursuant to sections (k)(1), (k)(2), (k)(3), (k)(5), and (k)(6). DOI will make notification determinations on a case by case basis.

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the applicable System Manager as identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked "PRIVACY ACT INQUIRY." A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system contains background investigation records and investigatory records related to law enforcement and counterintelligence activities that are exempt from certain provisions of the Privacy Act, 5 U.S.C. 552a(k). Pursuant to the Privacy Act, 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6), DOI has exempted portions of this system from the following subsections of the Privacy Act: (c)(3), (c)(4), (d), (e)(1) through (e)(3), (e)(4)(G) through (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), and (g). In accordance with 5 U.S.C. 553(b), (c) and (e), DOI is publishing a NPRM separately in the *Federal Register* to claim exemptions under 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), and (k)(6). Additionally, when this system receives a record from another system exempted

in that source system under 5 U.S.C. 552a(j) or (k), DOI claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

72 FR 11036 (March 12, 2007); modification published at 86 FR 50156 (September 7, 2021).

Signed:

Teri Barnett,
Departmental Privacy Officer,
Department of the Interior.

[FR Doc. 2022-19077 Filed: 9/1/2022 8:45 am; Publication Date: 9/2/2022]