



DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2023-0023; DS65100000 DWSN00000.000000 24XD4523WS DP.65102]

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, Department) is issuing a public notice of its intent to modify the Privacy Act system of records, INTERIOR/DOI-10, Incident Management, Analysis and Reporting System. DOI is revising this notice to change the title of the system, propose new and modified routine uses, and update all sections of the system notice to accurately reflect the scope of the system. This modified system will be included in DOI's inventory of systems of records.

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

ADDRESSES: You may send comments identified by docket number [DOI-2023-0023] 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-2023-0023] 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-2023-0023]. 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-10, Incident Management, Analysis and Reporting System, as a unified Department-wide law enforcement records management system. This system of records helps DOI protect life and resources, manage law enforcement incidents and investigations, measure performance, meet reporting requirements, and foster public trust through transparent and accountable law enforcement programs. The system also provides the capability to prevent, detect, and investigate known and suspected criminal activity and violations of fish and wildlife laws; transmit information to Federal law enforcement databases and repositories; analyze and prioritize protection efforts; provide information to justify law enforcement funding requests and expenditures; assist in managing visitor use and protection programs; investigate, detain and apprehend those committing crimes on DOI properties, including National Wildlife Refuges, National Parks, and Tribal reservations (for the purpose of this system of records notice, Tribal reservations include contiguous areas policed by Tribal or Bureau of Indian Affairs (BIA) law enforcement officers) managed by Native American Tribes under BIA; and

investigate and prevent visitor accidents and injuries on DOI properties or Tribal reservations. Incident and non-incident data related to criminal activity will be collected in support of law enforcement, homeland security, and security (physical, personnel, suitability, and industrial) activities. This may include data documenting criminal and administrative investigations and other law enforcement activities, use of force and critical incidents, traffic safety, property damage claims, motor vehicle crashes, domestic violence incidents, and information sharing and analysis activities. This notice covers all DOI law enforcement records, investigations, and case files in any medium that are created, collected, maintained, or managed by DOI bureaus and offices, excluding the Office of Inspector General, which maintains its own investigations system of records. DOI law enforcement bureaus and offices include OLES, Office of the Secretary, BIA, Bureau of Land Management, Bureau of Reclamation, the U.S. Fish and Wildlife Service, and the National Park Service. The OLES has Department-wide coordination and oversight responsibilities of law enforcement activities; however, each bureau and office is responsible for managing their records in this system for the administration of their law enforcement programs.

DOI is proposing to change the title of the system of records to INTERIOR/DOI-10, DOI Law Enforcement Records Management System (LE RMS) to reflect the modified scope of the system; update the system manager and system location sections; 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 the storage, safeguards, and records retention schedule; update the notification, records access and contesting procedures; and provide general updates in accordance with the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

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. The notice of disclosure to consumer reporting agencies in former routine use 13 was moved to the end of this section.

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. 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 and shared service providers 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 N was modified to clarify the sharing of information with the news media and the public to assure public safety related to potential or imminent threats to life, health, or property. Routine use P was modified to add the sharing of information when permitted by Federal law, statute, regulation, executive order, and DOI policy. Routine use Q was modified to add shared service providers who may need to access records in order to perform authorized activities on DOI's behalf.

Proposed routine use O allows DOI to share information with the news media and the public where there exists a legitimate public interest in the disclosure of information

and it is necessary to preserve the confidence in the integrity of the DOI, demonstrate DOI's commitment to serving the public and the accountability of its officers and employees. Proposed routine use T allows DOI to share information with adjudicative or regulatory agencies when necessary and appropriate to adjudicate decisions affecting individuals who are subjects of investigations or covered by this system notice. Proposed routine use U allows DOI to share information with complainants, victims, family members, and representatives to the extent necessary to provide information on results of investigations or cases or matters they may be involved in. Proposed routine use V allows DOI to share information with an official or employee regarding a matter within that individual's area of responsibility or when relevant and necessary to respond to official inquiries by the Department or other authority. Proposed routine use W allows DOI to share information with Tribal organizations when necessary and relevant under the Indian Self-Determination and Education Assistance Act.

Pursuant to the Privacy Act, 5 U.S.C. 552a(b)(12), DOI may disclose information from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)) to aid in the collection of outstanding debts owed to the Federal Government.

In a Notice of Proposed Rulemaking published separately in the *Federal Register*, DOI is proposing to claim additional exemptions for records maintained in this system pursuant to the Privacy Act of 1974, 5 U.S.C. 552a(k)(1), (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-10, DOI Law Enforcement Records Management System (LE RMS), system of records notice 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-10, DOI Law Enforcement Records Management System (LE RMS).

SECURITY CLASSIFICATION:

Classified and Unclassified.

SYSTEM LOCATION:

Office of Law Enforcement and Security, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240; Albuquerque Data Center, 1011 Indian School Road, Northwest, Albuquerque, NM 87104; DOI facilities and data centers; DOI-approved cloud service providers; and DOI bureaus and offices that manage law enforcement programs as identified in the System Manager section below.

SYSTEM MANAGER(S):

(1) Director, Office of Law Enforcement and Security, U.S. Department of the Interior, 1849 C Street NW, Mail Stop Room 3411, Washington, DC 20240.

(2) Bureau of Indian Affairs, Office of Justice Services, 1849 C Street NW, Mail Stop MS-3662-MIB, Washington, DC 20240.

(3) Director, Office of Law Enforcement and Security, Bureau of Land Management, 1849 C Street NW, Mail Stop: Fifth Floor, Room #5618, Washington, DC 20240.

(4) Bureau of Reclamation, Policy and Programs Directorate, Denver Security Division, Supervisory Security Specialist, PO Box 25007, Denver, CO 80225.

(5) Director, Office of Law Enforcement, U.S. Fish and Wildlife Service, MS: OLE, 5275 Leesburg Pike, Falls Church, Virginia 22041.

(6) National Park Service, Program Manager, National Park Service Law Enforcement, Security, and Emergency Services, U.S. Department of the Interior, 1849 C Street NW, Mailstop 2560, Washington, DC 20240.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Uniform Federal Crime Reporting Act, 28 U.S.C. 534; Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458); Homeland Security Act of 2002 (Pub. L. 107-296); USA PATRIOT ACT of 2001 (Pub. L. 107-56); USA PATRIOT Improvement Act of 2005 (Pub. L. 109-177); Tribal Law and Order Act of 2010 (Pub. L.

111-211); Fish and Wildlife Act of 1956, 16 U.S.C. 742a-742j-1; Refuge Recreation Act, 16 U.S.C. 460k-460k-4; Endangered Species Act of 1973, 16 U.S.C. 1531-1544; Lacey Act, 18 U.S.C. 42; Executive Order 14074: Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, May 25, 2022; Homeland Security Presidential Directive 7--Critical Infrastructure Identification, Prioritization, and Protection; Homeland Security Presidential Directive 12--Policy for a Common Identification Standard for Federal Employees and Contractors; Criminal Intelligence Systems Operating Policies, 28 CFR part 23; Law and Order, 25 CFR Part 10, Indian Country Detention Facilities and Programs; Courts of Indian Offenses and Law and Order Code, 25 CFR Part 11; and Indian Country Law Enforcement, 25 CFR Part 12.

PURPOSE(S) OF THE SYSTEM:

The LE RMS system of records is an incident management and reporting system used to prevent, detect, and investigate known and suspected criminal activity; protect natural and cultural resources; capture, integrate and share law enforcement and related information and observations from other sources; measure performance of law enforcement programs and management of emergency incidents; meet reporting requirements; foster public trust through transparent and accountable law enforcement programs; transmit information to Federal law enforcement databases and repositories; analyze and prioritize protection efforts; assist in managing visitor use and protection programs; enable the ability to investigate, detain and apprehend those committing crimes on DOI properties or Tribal reservations; and to investigate and prevent visitor accident incidents and injuries on DOI properties or Tribal reservations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered in the system include current and former Federal employees, consultants, contractors, subcontractors, and grantees; Federal,

Tribal, State, local and foreign law enforcement officers and officials; witnesses, complainants, informants, and parties who have been identified as potential subjects or parties to an investigation; and individuals or entities who are or have been the subject of investigations and other individuals associated with alleged violation(s) of Federal law, regulations, or rules of conduct.

Additionally, this system contains information regarding members of the general public, including individuals and/or groups of individuals involved with law enforcement incidents involving Federal assets or occurring on public lands and Tribal reservations, such as witnesses, individuals making complaints, individuals involved in reports of traffic accidents on DOI managed properties and Tribal reservations, and individuals being investigated or arrested for criminal or traffic offenses or involved in certain types of non-criminal incidents.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system includes law enforcement incident reports, law enforcement personnel records, and law enforcement training records, which contain the following information: names, home addresses, work addresses, telephone numbers, email addresses and other contact information, emergency contact information; dates of birth, place of birth; gender, ethnicity and race; biometric information such as physical or distinguishing attributes of an individual; Social Security numbers, driver's license numbers, passport numbers, identification numbers for non-citizens, Federal Bureau of Investigation (FBI) Universal Control Numbers, State identification numbers; Tribal identification numbers or other Tribal enrollment data; vehicle identification numbers, license plate numbers, boat registration or hull number; work history, educational history, affiliations, and other related data; criminal history, arrest and incarceration records, prior contacts with law enforcement, and records related to the transport of individuals.

Incident and investigation records related to or documenting criminal and

administrative investigations and other law enforcement activities, use of force, critical incidents, traffic safety, property damage claims, motor vehicle crashes, domestic violence incidents, information sharing and analysis, and other law enforcement activities may include, but are not limited to: incident reports, case files and notes; attachments such as photos or digital images, video recordings from body worn cameras, vehicle mounted cameras, hand-held cameras or devices, closed circuit television or other surveillance including sketches; medical reports; correspondence, email and text messages; letters, memoranda, and other documents citing complaints of alleged criminal, civil, or administrative misconduct; reports of investigations with related statements, affidavits or records obtained during investigations; prior criminal or noncriminal records of individuals related to investigations; reports from or to other law enforcement bodies; information obtained from informants; identifying information on suspects and allegations made against suspects; and public source materials; and information concerning response to and outcome of incidents and investigations.

Records in this system also include information concerning Federal civilian employees and contractors, Federal, Tribal, State, and local law enforcement officers and may contain information regarding an officer's name, contact information, station and career history, firearms qualifications, medical history, background investigation and status, date of birth, and Social Security number. Information regarding officers' equipment, such as firearms, electronic control devices, body armor, vehicles, computers and special equipment related skills is also included in this system.

RECORD SOURCE CATEGORIES:

Sources of information in the system include current and former DOI officials and employees; officials of Federal, State, Tribal, local, and foreign law enforcement and non-law enforcement agencies and organizations including the FBI and Department of Justice; subjects of investigations, complainants, informants, suspects, victims, witnesses,

private citizens, and visitors to Federal properties; photos and recordings captured from law enforcement body worn cameras, vehicle mounted cameras, hand-held cameras or other devices, closed circuit television, or other surveillance methods; and public source materials. Records may also be obtained from other internal and external sources such as personnel, training or other systems of records, DOI personnel, contractors, and other parties for matters related to the maintenance of this system, and information sharing partners.

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 their official capacity;
- (4) Any DOI employee or former employee acting in their 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(j) and (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(j) and (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, shared service provider, 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 in support of the law enforcement activities,

including obtaining public assistance with identifying and locating criminal suspects and lost or missing individuals, providing the public with alerts about dangerous individuals, and assuring public safety related to potential or imminent threats to life, health, or property.

O. To the news media and the public (including select members of the public, such as victims' family members) when:

(1) Release of the specific information would not constitute an unwarranted invasion of personal privacy, and

(2) There exists a legitimate public interest in the disclosure of the information and its release would:

(a) Preserve public confidence and trust in the integrity of DOI;

(b) Demonstrate DOI's commitment to serving the public and achieving its mission; or

(c) Reveal the accountability of DOI's officers, employees, or individuals covered by the system.

P. To the Department of Justice, the Department of Homeland Security, or other Federal, State, Tribal, and local law enforcement agencies for the purpose of information exchange on law enforcement activity or as required by Federal law, statute, regulation, executive order, and DOI policy.

Q. To agency contractors, grantees, shared service providers, or volunteers for DOI or other Federal Departments who have been engaged to assist the Government in the performance of a contract, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform the activity.

R. To any of the following entities or individuals, for the purpose of providing information on traffic accidents, personal injuries, or the loss or damage of property:

- (1) Individuals involved in such incidents;
- (2) Persons injured in such incidents;
- (3) Owners of property damaged, lost or stolen in such incidents; and/or
- (4) These individuals' duly verified insurance companies, personal representatives, administrators of estates, and/or attorneys.

The release of information under these circumstances should only occur when it will not interfere with ongoing law enforcement proceedings; risk the health or safety of an individual; reveal the identity of an informant or witness that has received an explicit assurance of confidentiality; or reveal protected or confidential law enforcement techniques and practices. Social Security numbers and Tribal identification numbers should not be released under these circumstances unless the Social Security number or Tribal identification number belongs to the individual requester.

S. To any criminal, civil, or regulatory authority (whether Federal, State, territorial, local, Tribal or foreign) for the purpose of providing background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks.

T. To an administrative forum, including ad hoc forums, which may include an Administrative Law Judge, public hearings/proceedings, or other established adjudicatory or regulatory agencies (e.g., the Merit Systems Protection Board, the National Labor Relations Board), or other agencies with similar or related statutory responsibilities, where necessary to adjudicate decisions affecting individuals who are the subject of investigations and/or who are covered by this system, to affect any necessary remedial actions, disciplinary or other appropriate personnel action, or other law enforcement related actions, where appropriate.

U. To complainants, victims, decedent's estate representative, or family members

of victims, and their attorney or legal representative, to the extent necessary to provide such persons with information concerning the results of an investigation or case arising from the matters of which they complained and/or of which they were the subject of law enforcement activity.

V. To a former official or employee of the Department when relevant and necessary to respond to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or to facilitate communications with a former official or employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance regarding a matter within that person's former area of responsibility.

W. To Tribal organizations when necessary and relevant to the assumption of a program under Public Law 93-638, the Indian Self-Determination and Education Assistance Act, 25 U.S.C. 450 et seq.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic records are maintained in information systems or stored on magnetic disc, tape or digital media. Paper records are maintained in file cabinets in secure facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by multiple identifiers including Social Security number, first or last name, badge number, address, phone number, vehicle information and physical attributes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are retained and disposed of in accordance with Office of the Secretary Records Schedule 8151, Incident, Management, Analysis and Reporting

System, which was approved by the National Archives and Records Administration (NARA) (N1-048-09-5), and other NARA approved bureau or office records schedules. The specific record schedule for each type of record or form is dependent on the subject matter and records series. After the retention period has passed, temporary records are disposed of in accordance with the applicable records schedule and DOI policy. Disposition methods include burning, pulping, shredding, erasing, and degaussing in accordance with Departmental records policy. Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA guidelines.

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. During normal hours of operation, paper records are maintained in locked file cabinets under the control of authorized personnel. Computer servers on which electronic records are stored are located in secured DOI controlled facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Access granted to authorized personnel is password-protected, and each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice appears on computer monitor screens when records containing information on individuals are first displayed. Data exchanged between the servers and the system is encrypted. Backup tapes are encrypted and stored in a locked and controlled room in a secure, off-site location.

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.

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. 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. A Privacy Impact Assessment was conducted to ensure that Privacy Act requirements are met and appropriate privacy controls were implemented to safeguard the personally identifiable information contained in the system.

RECORD ACCESS PROCEDURES:

DOI has exempted portions of this system from the access provisions of the Privacy Act of 1974 pursuant to 5 U.S.C. 552a(j) and (k). DOI will make access determinations on a case-by-case basis.

To the extent that portions of this system are not exempt, an individual requesting access to their records should send a written inquiry to the applicable System Manager identified above. DOI forms and instructions for submitting a Privacy Act request may be obtained from the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records sought and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746.

The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. Requests submitted by mail must be clearly marked “PRIVACY ACT REQUEST FOR ACCESS” on both the envelope and letter. A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

DOI has exempted portions of this system from the amendment provisions of the Privacy Act of 1974 pursuant to 5 U.S.C. 552a(j) and (k). DOI will make amendment determinations on a case-by-case basis.

To the extent that portions of this system are not exempt, an individual requesting amendment of their records should send a written request to the applicable System Manager as identified above. DOI instructions for submitting a request for amendment of records are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must clearly identify the records for which amendment is being sought, the reasons for requesting the amendment, and the proposed amendment to the record. The request must include the requester’s full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester’s identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked “PRIVACY ACT REQUEST FOR AMENDMENT” on both the envelope and letter. A request for amendment must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

DOI has exempted portions of this system from the notification procedures of the Privacy Act of 1974 pursuant to 5 U.S.C. 552a(j) and(k). DOI will make notification determinations on a case-by-case basis.

To the extent that portions of this system are not exempt, an individual requesting

notification of the existence of records about them should send a written inquiry to the applicable System Manager as identified above. DOI instructions for submitting a request for notification are available on the DOI Privacy Act Requests website at <https://www.doi.gov/privacy/privacy-act-requests>. The request must include a general description of the records and the requester's full name, current address, and sufficient identifying information such as date of birth or other information required for verification of the requester's identity. The request must be signed and dated and be either notarized or submitted under penalty of perjury in accordance with 28 U.S.C. 1746. Requests submitted by mail must be clearly marked "PRIVACY ACT INQUIRY" on both the envelope and letter. A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system contains law enforcement and investigatory records that are exempt from certain provisions of the Privacy Act of 1974, 5 U.S.C. 552a(j) and (k). In accordance with 5 U.S.C. 553(b), (c) and (e), DOI has promulgated rules separately in the *Federal Register* to claim exemptions for this system pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), (k)(3), (k)(5), and (k)(6).

Pursuant to 5 U.S.C. 552a(j)(2), DOI has exempted this system from the provisions of the Privacy Act except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i). DOI has also exempted portions of this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act pursuant to 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 that is 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 in the primary systems of records from which they originated and any additional exemptions set forth here.

HISTORY:

79 FR 31974 (June 3, 2014); modification published at 86 FR 50156 (September 7, 2021).

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

[FR Doc. 2024-00325 Filed: 1/9/2024 8:45 am; Publication Date: 1/10/2024]