4334-63-P

DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2019-0005]

[DS65100000, DWSN00000.000000, DP.65106, 20XD4523WS]

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 is issuing a public notice of its intent to modify the Department of the Interior Privacy Act system of records titled, "HSPD-12: Physical Security Files--Interior, DOI-46". This system of records helps the Department of the Interior manage physical security operations and visitor access to Federally-controlled facilities and information systems. The Department of the Interior is updating this system of records notice to add new proposed routine uses, modify existing routine uses to provide clarification, modify the categories of records and categories of individuals covered by the system, and provide updates to remaining sections to accurately reflect management of the system of records. This modified system will be included in the Department of the Interior'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-2019-0005], by any of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov*. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2019-0005] 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-2019-0005]. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://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 Department of the Interior (DOI), Office of Law Enforcement and Security maintains the HSPD-12: Physical Security Files--Interior, DOI-46 system of records. This system helps DOI manage physical security operations and visitor access to DOI-controlled facilities and implement Homeland Security Presidential Directive 12 (HSPD-

12), which requires Federal agencies to use a common identification credential for both logical and physical access to Federally-controlled facilities and information systems. DOI employees, contractors, consultants, volunteers, Federal emergency response officials, Federal employees on detail or temporarily assigned to work in DOI facilities, visitors, and other individuals require access to agency facilities, systems or networks. DOI uses integrated identity management systems to issue credentials to verify individuals' identities, manage access controls, and ensure the security of DOI controlled facilities. This Department-wide system notice covers physical security program records and activities, including all DOI controlled areas where paper-based physical security logs and registers have been established, in addition to or in place of smart-card access control systems.

DOI is publishing this revised notice to describe the purpose of the system, propose new and modified routine uses, and provide updates to the categories of records, categories of individuals covered by the system and the remaining sections to accurately reflect management of the system of records 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*. Additionally, DOI is claiming exemptions for certain records maintained in this system from some provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2), (k)(3), and (k)(5).

DOI is proposing to modify existing routine uses to provide clarity and transparency, and reflect updates consistent with standard DOI routine uses. Routine uses A, B, E, G, and I have been modified to provide additional clarification on external organizations and circumstances where disclosures are proper and necessary to facilitate

physical security operations or to comply with Federal requirements. Modified routine use J and new routine use K allow DOI to share information with appropriate Federal agencies or entities when reasonably necessary to respond to a breach of personally identifiable information and to prevent, minimize, or remedy the risk of harm to individuals or the Federal Government, or assist an agency in locating individuals affected by a breach in accordance with OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.

DOI is proposing to add new routine uses to facilitate sharing of information with agencies and organizations to ensure the efficient and effective management of physical security functions, promote the integrity of the records in the system, or carry out a statutory responsibility of the DOI or Federal Government. New proposed routine use C facilitates sharing of information with the Executive Office of the President to resolve issues concerning an individual's records. Routine use D allows DOI to share information with other agencies when there is an indication of a violation of law. Routine use F facilitates sharing of information related to hiring, issuance of a security clearance, or a license, contract, grant or benefit. Routine use H allows sharing of information with government agencies and organizations in response to court orders or for discovery purposes related to litigation. Routine use L facilitates sharing with the OMB in relation to legislative affairs mandated by OMB Circular A-19. Routine use M allows sharing of information with the Department of the Treasury to recover debts owed to the United States. Routine use N allows sharing with the news media and the public, when it is necessary to preserve the confidence in the integrity of DOI, demonstrate the accountability of its officers, employees, or individuals covered in the system, or where

there exists a legitimate public interest in the disclosure of the information such as circumstances that support a legitimate law enforcement or public safety function, or protects the public from imminent threat of life or property.

Some Personal Identity Verification (PIV) card information in this system may also be covered under government-wide system of records notice, GSA/GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS), which applies to participating Federal agency employees, consultants, and volunteers who require long-term access to Federal facilities, systems and networks, and individuals who are authorized to perform or use services in agency facilities. This system notice covers additional categories of individuals and records to include occasional and short-term visitors and guests, temporary credentials, paper-based security logs, and other information necessary to ensure the safety and security of DOI facilities, systems, occupants, and users.

In a notice of proposed rulemaking, which is published separately in the *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)(2), (k)(3) and (k)(5).

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' personal information. 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 for 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 revised INTERIOR/DOI-46, Physical Security Access Files, 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 personal identifying information, such as your address, phone number, email address, or any other personal identifying information in your comment, may be made publicly available at any time. While you may request to withhold your personal identifying information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER:

INTERIOR/DOI-46, Physical Security Access Files.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records covered by this system are maintained at the following locations:

(1) U.S. Department of the Interior, Office of Law Enforcement and Security, Physical Security Office, 1849 C Street NW, Mail Stop 1324 MIB, Washington, DC 20240; and

(2) U.S. Department of the Interior, Office of the Secretary, Interior Business Center, 7301 W. Mansfield Avenue, MS D-2130, Denver, CO 80235-2300.

(3) Portions of the data covered by this system are also maintained at other Department of the Interior locations, both Federal buildings and Federally-leased space, where staffed guard stations have been established in facilities that have installed a smart-card ID system, and/or paper-based physical security logs and registers, as well as the physical security office(s) of those locations. A list of these locations (as applicable to each bureau) is maintained by each bureau's Physical Security Manager, whose address is provided under item (2) in the System Manager(s) section below.

SYSTEM MANAGER(S):

(1) Security Manager, Physical Security Office, Office of Law Enforcement and Security, Mail Stop 1324 MIB, 1849 C Street NW, Washington, DC 20240.

(2) Bureau Physical Security Managers:

(a) Bureau of Indian Affairs: Indian Affairs Homeland Security Coordinator, 1849 C Street NW, Mail Stop 4160 MIB, Washington, DC 20240.

(b) Bureau of Indian Education: Indian Affairs Homeland Security Coordinator, 1849 C Street NW, Mail Stop 4160 MIB, Washington, DC 20240.

(c) Bureau of Land Management: Chief Security and Intelligence, Bureau of Land

Management, Office of Law Enforcement and Security, 20 M Street SE, Washington, DC 20036.

(d) Bureau of Ocean Energy Management: Bureau of Ocean Energy Management physical security is managed by Security Specialist, Bureau of Safety and Environmental Enforcement, 45600 Woodland Road, Mail Stop VAE-MSD, Sterling, VA 20166.

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

(f) Bureau of Safety and Environmental Enforcement: Security Specialist, Bureau of Safety and Environmental Enforcement, 45600 Woodland Road, Mail Stop VAE-MSD, Sterling, VA 20166.

(g) National Park Service: Law Enforcement, Security and Emergency Service Manager, National Park Service, Security and Intelligence Branch, 1201 I (Eye) Street NW, 10th Floor, Washington, DC 20005.

(h) Office of Surface Mining, Reclamation and Enforcement: Security Officer, Office of Surface Mining, Reclamation and Enforcement, 1951 Constitution Avenue NW, Mail Stop 344 SIB, Washington, DC 20240.

(i) Office of Inspector General: Support Services Supervisor, Office of Inspector General, 12030 Sunrise Valley Drive, Suite 350, Mail Stop 5341, Reston, VA 20191.

(j) Office of the Secretary/Interior Business Center Security Manager, Interior Business Center, Mail Stop 1224 MIB, 1849 C Street NW, 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: Security and Emergency Manager, U.S. Fish and Wildlife Service, 5275 Leesburg Pike, Falls Church, VA 22041.

(m) U.S. Geological Survey: Bureau Security Manager, U.S. Geological Survey, 250 National Center, 12201 Sunrise Valley Drive, Reston, VA 20192.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, section 5113); E-Government Act (Pub. L. 104-347, section 203); Paperwork Reduction Act of 1995 (44 U.S.C. §§ 3501-3521); Government Paperwork Elimination Act (44 U.S.C. § 3504); Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended; Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, Section 3001 (50 U.S.C. 3341); Executive Order 9397; Executive Order 12968; Federal Property Regulations, July 2002; and Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

PURPOSE(S) OF THE SYSTEM:

The primary purposes of the system are to manage physical security and access to DOI-controlled facilities and information systems, verify that all persons entering DOI facilities or other Federal Government facilities are authorized, and ensure the safety and security of DOI facilities and their occupants.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individuals who require regular, ongoing access to Departmental facilities, including DOI employees, contractors, consultants, volunteers, Federal emergency

response officials, Federal employees on detail or assigned to work at DOI facilities, students, interns, affiliates, and individuals formerly in any of these positions. The system also includes individuals authorized to perform or use services provided in DOI facilities (e.g., Credit Union, Fitness Center, Library, Indian Craft Shop, Museum, Child Care Center, etc.). NOTE: These individuals are required to have HSPD-12 compliant credentials issued by a certified USAccess credentialing center if they are employed by DOI for more than 180 days.

(2) Individuals who have been issued HSPD-12 compliant credentials from other Federal agencies who require access to DOI facilities.

(3) Federal government officials, visiting dignitaries, visitors, guests, and other individuals who require infrequent access to DOI facilities, including services provided in DOI facilities (e.g., Credit Union, Fitness Center, Library, Indian Craft Shop, Museum, Child Care Center, etc.).

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Records maintained on individuals requiring regular access to DOI-controlled facilities and information systems, or who are issued HSPD-12 compliant credentials by DOI and by other Federal agencies, include the following data fields: full name; Social Security number (SSN); date of birth; signature; digital image (photograph) and video; fingerprints; hair color; eye color; height; weight; home address; work address; email address; agency affiliation (e.g., employee, contractor, volunteer, etc.); telephone number; vehicle identification, license plate and state of issuance; personal identity verification (PIV) card issue and expiration dates; personal identification number (PIN); results of background investigation; PIV request form; PIV registrar approval signature;

PIV card serial number; emergency responder designation; copies of "I-9" documents (e.g., driver's license, passport, birth certificate, etc.) used to verify identification or 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; digital signature information; and date, time, and location of entry and exit.

(2) Records maintained on visitors, guests, and other individuals who require infrequent access to DOI facilities include the following data fields: full name; signature; image, including photograph and video; SSN or other identification number such as driver's license number, "Green Card" number, Visa number, etc.; images of relevant ID document(s); U.S. Citizenship (yes or no/logical data field); vehicle identification and license plate; date, time, and location of entry and exit; purpose for entry; agency point of contact; company name; security access category; and access status.

(3) Records related to DOI physical security program management and operations include facility access logs; visitor logs; closed circuit television (CCTV) recordings; information pertaining to incidents, offenses, or suspected security violations; statements, affidavits, and correspondence related to potential security violations or incidents; reports of investigations, security violations or remedial actions; referrals to law enforcement organizations; investigations or records related to security details or events involving DOI officials or visiting dignitaries; and information obtained from another system or agency related to providing protective services to the President of the United States or other individuals pursuant to 18 U.S.C. 3056. These records may include: full name;

SSN; driver's license number, "Green Card" number, Visa number, or other documents used to verify identification; date of birth; digital image, including photograph or video; fingerprints; hair color; eye color; height; weight; home or work address; email address; agency affiliation; telephone number; vehicle identification, license plate and state of issuance; PIV card number and dates; information related to background investigation and security clearance; computer system user name; date, time, and location of entry and exit; purpose for entry; any other information identified above for regular or infrequent access to DOI-controlled facilities and information systems; and information related to potential security violations and incidents occurring on DOI-controlled facilities.

RECORD SOURCE CATEGORIES:

Information is obtained from individuals covered by the system, supervisors, and designated approving officials, as well as records supplied by DOI's identity management system, other Federal agencies issuing HSPD-12 compliant cards, and HSPD-12 compliant cards carried by individuals seeking access to Departmental and other Federal facilities occupied by agency employees.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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 maintained in this system may be disclosed to authorized entities outside DOI for purposes determined to be relevant and necessary 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.

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.

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, 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, when a matter has become public knowledge, when it is necessary to preserve the confidence in the integrity of DOI or is necessary to demonstrate the accountability of its officers, employees, or individuals covered in the system, or where there exists a legitimate public

interest in the disclosure of the information, such as circumstances where providing information supports a legitimate law enforcement or public safety function, or protects the public from imminent threat of life or property, 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 another agency with a similar HSPD-12 (PIV/smart-card) system when a person with identification credentials issued by the Department desires access to that agency's facilities.

Q. To another agency with a similar HSPD-12 (PIV/smart-card) system when it controls access to facilities occupied by the agency.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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, email, diskettes, and electronic databases.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by name; SSN; image; organization/office of

assignment; date, time or location of entry or exit; ID security card number or date; or other personal identifier listed in the Category of Records section of this notice.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records covered by this system are retained in accordance with General Records Schedule (GRS) 5.6, Security Records, which cover records about protecting an organization's personnel, assets, and facilities. These records generally have a temporary disposition, and retention schedules vary on the type of record and needs of the agency. Records related to visitor controls files are destroyed two years after final entry or ID security card expiration date. Records related to physical security and protection of facilities, including correspondence relating to administration and operations, and some investigative files are destroyed when two years old. See specific items under GRS 5.6 for retention periods. Retention periods for security violation files relating to investigations referred to administrative or law enforcement organizations may vary depending on the subject matter, legal requirements and Departmental policy. Approved disposition methods for temporary records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1 and 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 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 and individuals at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the systems at the guard stations and badging office are encrypted. Backup tapes are 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, 5 U.S.C. § 552a; Paperwork Reduction Act of 1995, 44 U.S.C. §§3501-3521; Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551-3558; 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 completed on the PACS system to ensure that Privacy Act requirements are met and appropriate privacy controls were implemented to safeguard personally identifiable information.

RECORD ACCESS PROCEDURES:

An individual requesting records on himself or herself should send a signed, written inquiry to the applicable System Manager as identified above. The request must include the requester's bureau and office affiliation and the address of the facility to which the requester needed access 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:

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 requester's bureau and office affiliation and the address of the facility to which the requester needed access to facilitate location of the applicable records. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURE:

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 requester's bureau and office affiliation and the address of the facility to which the requester needed access 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 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)(2), (k)(3), and (k)(5). Pursuant to the Privacy Act, 5 U.S.C. 552a(k)(2), (k)(3), and (k)(5), the Department of the Interior has exempted portions of this system from the following subsections of the Privacy Act: (c)(3), (d), (e)(1), (e)(4)(G) through (e)(4)(I), and (f). In accordance with 5 U.S.C. 553(b), (c) and (e), the Department of the Interior has promulgated rules at 43 CFR Part 2, Subpart K, and is proposing to amend these rules in a Notice of Proposed Rulemaking, which was published separately in today's *Federal Register*.

HISTORY:

72 FR 11043 (March 12, 2007).

Signed: _____

Teri Barnett
Departmental Privacy Officer
Department of the Interior

[FR Doc. 2020-00355 Filed: 1/17/2020 8:45 am; Publication Date: 1/21/2020]