



DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2023-0005; 234D0104IG, DG10100000, DIG000000.000000]

Privacy Act of 1974; System of Records

AGENCY: Office of Inspector General, 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 Office of Inspector General (OIG) Privacy Act system of records, INTERIOR/OIG-02, Investigative Records. DOI is publishing this revised notice to update the system location, record source categories, storage and records retention, expand and clarify categories of individuals and records, propose a new routine use and modify existing routines uses, and provide general administrative updates to remaining sections to accurately reflect management of the system of records in accordance with the Office of Management and Budget (OMB) policy. Additionally, DOI is publishing a notice of proposed rulemaking (NPRM) elsewhere in the Federal Register to claim exemptions in 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-2023-0005] 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-2023-0005] 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-2023-0005]. 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: Eric Trader, Associate Privacy Officer, Office of Inspector General, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 4428-MIB, Washington, DC 20240, oig_privacy@doioig.gov or (202) 208-1644.

SUPPLEMENTARY INFORMATION:

I. Background

The OIG maintains the INTERIOR/OIG-02, Investigative Records, system of records. The purpose of this system is to maintain certain investigative case files and other materials created or gathered during the course of an official investigation. DOI last published the INTERIOR/OIG-02, Investigative Files, system of records notice in the *Federal Register* at 76 FR 60519 (September 29, 2011); modification published at 86 FR 50156 (September 7, 2021). DOI is publishing this revised notice to update the system location; record source categories; policies and practices for storage and records retention; expand the categories of individuals; update categories of records to clarify that

the system may contain additional personally identifiable information obtained from any source relevant to an OIG investigation; update the record access, contesting record, and notification procedures; and provide general and administrative updates to the remaining sections of the notice in accordance with the OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*.

Additionally, OIG is changing the routine uses from a numeric to an alphabetic list, and is proposing to modify existing routine uses and add a new routine use to provide clarity and transparency, and to reflect updates consistent with standard DOI routine uses.

Routine uses A, B, F, H, J, N, and P have been modified to provide additional clarification on external organizations and circumstances where disclosures are proper and necessary to facilitate investigations or comply with Federal requirements. Routine use A was slightly modified to further clarify disclosures to the Department of Justice (DOJ) or other Federal agencies, or other individuals or entities when necessary, in relation to litigation or judicial hearings. Routine use B was modified to clarify disclosures to a congressional office to respond to or resolve an individual's request made to that office. Routine use F was modified to clarify sharing of information with government agencies, individuals, or entities when relevant for hiring and retention, or issuance of security clearance, license, contract, grant or benefit. Routine use H was modified to clarify sharing of information with government agencies and organizations in response to court orders or for discovery purposes related to litigation. Modified routine use J allows OIG 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 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 include review by designated OIG officials and clarify circumstances where there is a legitimate

public interest in the disclosure of information that would not constitute an unwarranted invasion of privacy. Routine use P was modified to share information with the DOJ regarding their obligations under an international treaty, convention, or executive agreement.

Proposed routine use C facilitates sharing of information with the Executive Office of the President to resolve issues concerning an individual's records. DOI is also removing three routine uses that are no longer needed. The notice of disclosure to consumer reporting agencies in former routine use 13 was moved to the end of this section. Former routine uses 21 and 28 were removed as they are no longer needed since OIG no longer shares information with the Federal Labor Relations Authority and the Recovery Accountability and Transparency Board.

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, 5 U.S.C. 552a(k)(1), (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' 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/OIG-02, Investigative Records, 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/OIG-02, Investigative Records.

SECURITY CLASSIFICATION:

Classified and Unclassified.

SYSTEM LOCATION:

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

(1) U.S. Department of the Interior, Office of Inspector General, 1849 C Street NW, Washington DC 20240;

(2) Office of Inspector General, 381 Elden Street, Suite 3000, Herndon, VA 20170;

(3) Office of Inspector General Regional Offices and Regional sub-offices. A current listing of these offices may be obtained by writing to the System Manager; and

(4) Investigative site during the course of an investigation.

SYSTEM MANAGER(S):

Assistant Inspector General for Investigations, Office of Inspector General, U.S. Department of the Interior, 1849 C Street NW, Mail Stop 4428-MIB, Washington, DC 20240.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Inspector General Act of 1978, as amended, 5 U.S.C. §§ 401–424.

PURPOSE(S) OF THE SYSTEM:

The primary purpose of this system is to help facilitate the OIG’s various responsibilities under the Inspector General Act of 1978, as amended. The OIG is statutorily directed to conduct and supervise investigations relating to programs and operations of the DOI, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, records in this system are used within the DOI and OIG during the course of investigating individuals and entities suspected of misconduct, fraud, waste, and abuse, other illegal or unethical acts, and in conducting related criminal prosecutions, civil proceedings, and administrative actions. These records are also used to fulfill reporting requirements, to maintain records related to the OIG’s activities, and to prepare and issue reports to Congress, the DOI and its components, the DOJ, the public, and other entities as appropriate within the mission of the OIG.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by the system include current and former DOI employees, potential employees, contractors, and subcontractors; complainants, witnesses, confidential and non-confidential informants, union officials; recipients of federal assistance or funds and their contractor or subcontractors and employees; alleged violators of DOI rules and regulations; individuals investigated and interviewed; persons suspected of violations of administrative, civil and criminal provisions; and grantees, sub-grantees, lessees, licensees, and other persons engaged in business with the DOI or having contact with the DOI or geographical areas under its jurisdiction.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records related to investigations conducted by the OIG, include:

- (1) Complaints, requests to investigate, and administrative referrals;
- (2) Records of case initiation including the following data fields: case number, title of case, dates, offices/personnel assigned, summary;
- (3) Documents, statements, and information of any kind gathered through investigation;
- (4) Reports, correspondence, notes and memoranda generated by OIG regarding investigations; and
- (5) Records on complainants, subjects, victims, witnesses that may contain the following: name, status as government employee, Social Security number, birth date, birth place, aliases, gender, citizenship, race/ethnicity, driver's license or other identification number(s), education, financial or credit card information, spouse and family information, group affiliation(s), government and nongovernment employment information, home and mailing address(s), personal and official phone number(s), personal and official e-mail address(s), photo, and any other personal information obtained from any source relevant to the DOI OIG investigations.

RECORD SOURCE CATEGORIES:

As an investigative agency focusing on the activities of the DOI, the OIG collects records in this system from any relevant investigative source, including the DOI; other federal, state, and local governments, businesses, and other entities; and private parties or individual members of the public who communicate, interact with, or request assistance or services from the OIG, or who have information that is relevant to OIG investigations.

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 OIG 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, or to other individuals or entities who are parties to such litigation or proceedings, 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, when 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 OIG suspects or has confirmed that there has been a breach of the system of records;

(2) DOI OIG 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 the 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 OIG 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 designated OIG officials, where there is a legitimate public interest in the disclosure of the information, which may include but is not limited to, a matter under investigation or audit becomes public knowledge; or the disclosure is deemed appropriate to preserve confidence in the integrity of the OIG audit or investigative process; or to demonstrate the accountability of DOI officers, employees, or individuals covered by this system; 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 an individual or entity, to the extent necessary in order to seek information relevant to a decision by DOI concerning the hiring, assignment or retention of an individual or other personnel action, the issuance, renewal, or retention or revocation of a security clearance, the execution of a security or suitability investigation, the letting of a contract, or the issuance, retention or revocation of a license, grant, or other benefit.

P. To an individual or entity, to the extent necessary in order to seek information or assistance relevant to an OIG investigation, audit, or evaluation.

Q. To a foreign government or to DOJ regarding obligations under an international treaty, convention, or executive agreement entered into by the United States.

R. To an authorized appeal grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator or other person properly engaged in an investigation or settlement of an administrative grievance, complaint, claim, or appeal filed by an employee, special studies of the civil service and other merit systems, review of Human Resources or component rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of an OIG or DOI investigation, and such other functions promulgated in 5 U.S.C. 1205-06.

S. To a grand jury agent pursuant to a federal or state grand jury subpoena or in response to a prosecution request that such record or information is released for the purpose of its introduction to a grand jury.

T. To the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deductions, or other information necessary as a result of an investigation for OPM to carry out its personnel management functions and studies.

U. To Treasury and to the DOJ, when the information is subject to an ex parte court order permitting the disclosure of return or return information (26 U.S.C. 6103(b)) by the Internal Revenue Service, or when disclosure is necessary to facilitate obtaining such an order.

V. To the Office of Government Ethics for any purpose consistent with that office's mission including the compilation of statistical data.

W. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

X. To an individual who has been interviewed or contacted by OIG pursuant to an audit, investigation or evaluation, OIG may provide copies of that individual's statements, testimony, or records produced.

Y. To appropriate agencies, entities, and persons when OIG determines that disclosure may prevent or minimize a risk of harm to DOI programs, personnel or property, including but not limited to a risk of loss or misuse of funds granted or paid by the DOI to any other agency, entity or person.

Z. To the Council of the Inspectors General on Integrity and Efficiency, any successor entity, and other Federal agencies and their Offices of Inspectors General, as necessary to respond to an authorized audit, investigation or review.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper records and all other media including but not limited to photographs, audio recordings, diskettes, and CDs are stored in file cabinets in a secured area. Electronic records are maintained on file and email servers that are protected with user account access controls and other appropriate electronic security measures, such as multi-factor authentication and data encryption at rest and during transit, and are physically located in locked facilities that are secured at all times by alarm systems and video surveillance cameras.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrievable by individual's name, case number, or document title.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained in accordance with Office of the Secretary Records Disposal Schedule, 2802 - Investigative Records, which was approved by NARA (N1-048-10-03) Records relating to investigative reports and material pertaining allegations of violation of regulations, Departmental policy, and law are covered under 2802.2 with a temporary disposition and destroyed ten years after the completion of the investigation or action and transferred to NARA. Records selected to have historical value are covered under 2802.1 and are held permanently and transferred to NARA after twenty-five years. Records are disposed of in accordance with NARA guidelines and Departmental policy.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to paper records is restricted to authorized personnel on a need-to-know basis. During duty hours, paper records are located in file cabinets in OIG space occupied by authorized personnel. During non-duty hours, paper records and other physical media are maintained in locked cabinets located in appropriately secured OIG space.

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, network system security monitoring, and software controls.

Access to electronic records is restricted to authorized personnel who use them for official purposes. Each person granted access to the system must be individually authorized to use the system. Security of the system and records therein is maintained through the use of passwords and other electronic security measures. Passwords are changed on a cyclical basis. These computer servers are located in locked facilities that are secured at all times by alarm systems and video surveillance cameras. During non-duty hours the alarm system provides immediate notification of any attempted intrusion to OIG Information Technology personnel. All data exchanged between the servers and individual personal computers is encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location. Measures have been taken to ensure that the handling of this information meets the requirements of the DOI Privacy Act regulations, 43 CFR 2.226.

A Privacy Impact Assessment was conducted and recently updated regarding the electronic records within the system to ensure that Privacy Act requirements are met, and appropriate privacy controls were implemented to safeguard the personally identifiable information contained in the system. The assessment verified that appropriate controls and safeguards are in place. Safeguards include, but are not limited to, a requirement restricting access to the system to authorized OIG personnel as granted by the System

Manager. All personnel within OIG, including all personnel with access to records in this system, are required to complete all privacy, records management, and security training on an annual basis and sign the DOI Rules of Behavior.

RECORD ACCESS PROCEDURES:

DOI has exempted portions of this system from the access provisions of the Privacy Act pursuant to sections 5 U.S.C. 552a(j) and (k). OIG 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 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. 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 pursuant to sections (j) and (k). OIG 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 pursuant to 5 U.S.C. 552a(j) and (k). OIG 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 investigatory records that are exempt from certain provisions of the Privacy Act, 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), and (k)(5).

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), and (k)(5). 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: 76 FR 60519 (September 29, 2011); modification published at 86 FR 50156 (September 7, 2021).

Signed:

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

[FR Doc. 2023-14882 Filed: 7/12/2023 8:45 am; Publication Date: 7/13/2023]