



DEPARTMENT OF THE INTERIOR

Geological Survey

[DOI-2023-0006; 234G0804MD GGH DFA3540 GF0200000 GX23FA35SA40000]

Privacy Act of 1974; System of Records

AGENCY: United States Geological Survey, Interior.

ACTION: Notice of a new 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 create the United States Geological Survey (USGS) Privacy Act system of records, INTERIOR/USGS-28, USGS Store Customer Records. This system of records is being established to manage customer records for earth science and information products available through the USGS Store. This newly established system will be included in DOI's inventory of record systems.

DATES: This new system will be effective upon publication. New 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-2023-0006] by any of the following methods:

- Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2023-0006] in the subject line of the message.
- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC

20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2023-0006]. All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

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

FOR FURTHER INFORMATION CONTACT: Cozenja Berry, Associate Privacy Officer, Office of the Associate Chief Information Officer, U.S. Geological Survey, 12201 Sunrise Valley Drive, Mail Stop 159, Reston, VA 20192, privacy@usgs.gov or (571) 455-2415.

SUPPLEMENTARY INFORMATION:

I. Background

The USGS maintains the INTERIOR/USGS-28, USGS Store Customer Records, system of records. Through partnerships with the National Parks Service, Bureau of Land Management, United States Fish and Wildlife Service, United States Forest Service, and other federal agencies, the USGS provides a centralized point of sales for recreational land passes, earth science products, and forestry products via the USGS Store. The USGS Store (referred to as store throughout this notice) is a component of the USGS Science Information Delivery Branch, Office of the Associate Chief Information Officer. Products available for purchase or issuance to the general public through the store include: America the Beautiful - the National Parks and Federal Recreational lands passes; government produced maps; satellite imagery prints; science publications; and a variety of educational materials.

The USGS Store utilizes the Integrated Business Solutions (IBiS) system to process transactions and administer customer records. The records in IBiS are currently covered by two system of records notices (SORNs): INTERIOR/USGS-15, Earth Science

Information Customer Records, 63 FR 60375 (November 9, 1998); modification published at 74 FR 23430 (May 19, 2009), and INTERIOR/DOI-06, America the Beautiful—The National Parks and Federal Recreational Lands Pass System, 80 FR 63246 (October 19, 2015); modification published at 86 FR 50156 (September 7, 2021). Records pertaining to the sale of earth science and forestry products (government produced maps, satellite imagery prints, science publications, and educational materials) were previously managed by the USGS Earth Science Information Office (ESIO), National Mapping Division, and maintained under INTERIOR/USGS-15. With the establishment of the USGS Store, the program responsibility and associated records transferred from ESIO to the store to provide a single point of sales within the bureau, thereby prompting the creation of this new system of records. The USGS intends to rescind the SORN for INTERIOR/USGS-15 after the public comment period for this notice has expired and comments received have been adjudicated. All records pertaining to the sale of passes through the America the Beautiful—The National Parks and Federal Recreational Lands Pass System, which are sold on behalf of the National Parks Service, will continue to be maintained in accordance with the INTERIOR/DOI-06 notice as published in the *Federal Register*.

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/USGS-28, USGS Store Customer Records, SORN is published in its entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Participation

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

SYSTEM NAME AND NUMBER:

INTERIOR/USGS-28, USGS Store Customer Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained by the Science Information Delivery Branch, Office of the Associate Chief Information Officer, U.S. Geological Survey, Denver Federal Center, Denver, CO 80225.

SYSTEM MANAGER(S):

Chief, Science Information Delivery Branch, Office of the Associate Chief

Information Officer, U.S. Geological Survey, Mail Stop 306, Denver Federal Center,
P.O. Box 25286, Denver, CO 80225.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301, Departmental Regulations; 7 U.S.C 1387, Photographic reproductions and maps; 16 U.S.C. 6804, Recreation passes; 31 U.S.C. 9701, Fees and charges for Government services and things of value; 43 U.S.C. 1457, Duties of Secretary; 43 U.S.C. 31, Director of United States Geological Survey; 43 U.S.C 31c, Geologic mapping program; 43 U.S.C. 41, Publications and reports; preparation and sale; 43 U.S.C. 42, Distribution of maps and atlases, etc.; 43 U.S.C. 44, Sale of transfers or copies of data; 43 U.S.C. 45, Production and sale of copies of photographs and records; disposition of receipts; and 7 CFR 2.60, Chief, Forest Service.

PURPOSE(S) OF THE SYSTEM:

The purpose of this records system is to process orders and respond to customer inquiries from individuals who have requested earth science and forestry products (government produced maps, satellite imagery prints, science publications, and other educational materials) through the USGS Store. In addition, feedback provided by individuals may be used by the USGS to propose process improvements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system includes individuals who have ordered products from, or sent an inquiry or comment to, the USGS Store by telephone, mail, email, or the online storefront.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system maintains records related to individual inquiries, customer order history, and payment information, and customer feedback. Individuals may use their personally identifiable information or business information for transactions and communications with the USGS Store. Information collected on individuals includes:

first and last name, email address, telephone number, mailing address, billing address, debit or credit card information (card number, expiration date and security code), and purchase order number. Although not required, some customers may provide their company name or other organizational affiliation.

RECORD SOURCE CATEGORIES:

The individual provides the personal information collected to process orders and respond to inquiries they initiate through the USGS Store. USGS personnel and contractors may contribute information to customer records as it pertains to order status and fulfilment, purchase issues, product shipping, and responding to general inquiries.

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 contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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

- (1) DOI or any component of DOI;
- (2) Any other Federal agency appearing before the Office of Hearings and Appeals;
- (3) Any DOI employee or former employee acting in his or her official capacity;
- (4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or

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

B. To a congressional office when requesting information on behalf of, and at the request of, the individual who is the subject of the record.

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, 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 process credit card payments and

recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Customer records are maintained with appropriate administrative, physical and technical controls to protect individual privacy. Electronic records are stored in secure facilities. Paper records are contained in file folders stored in file cabinets in secure office locations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by the system generated customer number, last name/first name, email address, or phone number. Records may also be retrieved by a search of the individual's address, purchase order number, and by company or organizational affiliation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained under the USGS General Records Disposition Schedule (GRDS), Item 305-06 – IBiS System. GRDS Item 305-06 is a USGS-wide records schedule that supports the Natural Science Network program in the distribution of all USGS published materials such as maps, books, and scientific reports. Files consist of the scanned original customer correspondence for orders, copies of checks, and deposit slips. Records are destroyed six years and three months after the end of the fiscal year in which they were collected.

Approved destruction methods for temporary records that have met their retention

period include shredding or pulping paper records and erasing or degaussing electronic records in accordance with NARA guidelines and Departmental policy.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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. Electronic records are stored on encrypted servers located in secured Federal agency and contractor facilities with physical, technical and administrative levels of security to prevent unauthorized access to information. Access is only granted to authorized personnel 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 in accordance with DOI security policy. Backup tapes are encrypted and stored in a locked and controlled room in a secure, off-site location.

Electronic records are maintained in information systems that are regulated by 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. A Privacy Impact Assessment was conducted on IBiS, the host information 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. Security controls include user identification, multi-factor authentication, database permissions, encryption, firewalls, audit logs, network system

security monitoring, and software controls. Customer data is stored separately from order data. All credit card data is encrypted when entered and only the accounting team has access to unencrypt this data. This database is on an internal server behind numerous firewalls and other security measures.

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.

RECORD ACCESS PROCEDURES:

An individual requesting access to their records should send a written inquiry to the System Manager identified in this notice. 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:

An individual requesting amendment of their records should send a written request to the System Manager as identified in this notice. 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:

An individual requesting notification of the existence of records about them should send a written inquiry to the System Manager as identified in this notice. 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:

None.

HISTORY:

None.

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

[FR Doc. 2023-17577 Filed: 8/15/2023 8:45 am; Publication Date: 8/16/2023]