U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Bison File and Serve
Bureau/Office: Office of the Secretary (OS)
Date: January 7, 2026
Point of Contact
Name: Adrienne Brooks-Hill
Title: OS Departmental Offices, Associate Privacy Officer
Email: OS_Privacy@ios.doi.gov
Phone: 202-208-3368
Address: 1849 C Street, NW, Room 7112, Washington DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Bison File and Serve (BFS) is an e-filing and case management system that streamlines the adjudication process for the Office of Hearings and Appeals. The primary purpose of the

BFS system is to support administrative determinations and adjudications delegated to the Office of Hearings and Appeals (OHA). BFS modernizes OHA's case management and adjudication processes and workflows, incorporates electronic filing (e-filing), improves on current indexing and search capabilities, and consolidates and automates OHA dockets. Bison File and Serve replaced the Docket Management System, as the office's current internal case management module, residing in OHA-Internal for OHA employee use. Data migration from the Docket Management System was completed in the second quarter Fiscal Year-24. The launch of the new cloud-based system that replaced the Docket Management System triggered this PIA.

BFS includes an e-filing service that allows electronic submission of documents relating to a case by relevant parties, including members of the public, other government organizations and Tribes, DOI bureaus and offices, and/or corporations and non-profit organizations. BFS also permits parties to pending OHA matters to electronically access docket information and documents submitted by other parties and issued by OHA. BFS will also be used by OHA to produce reports on case-related data including case status and docket processing metrics.

Moreover, probate records will not be found in BFS. To access probate records, the public will continue to rely on OHA-External, a web-based interface on the OHA website, and OHA staff on OHA-Internal.

C. What is the legal authority?

Departmental Regulations, 5 U.S.C. 301, 551 et seq.; Federal Power Act, 16 U.S.C. 791 et seq.; Appeals from Administrative Decisions, 25 U.S.C. 2, 9, 372, 373, 373a, 373b, 374, 2201 et seq.; Mineral Land and Mining, 30 U.S.C. chap. 2, 3, 3A, 5, 7, 16, 23, 25 and 29; Contract Disputes - Definitions, 41 U.S.C. 7101 et seq.; Grazing Lands - Protection, Administration; Regulation and Improvement of Districts; Rules and Regulations; Study of Erosion and Flood Control; Offenses, 43 U.S.C. 315a, 1201, 1331 et seq., 1601 et seq., 1701 et seq.; Department Hearings and Appeals Procedures, 43 CFR parts 4, 30, and 45.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in the Governance, Risk, and Compliance platform?

☒ Yes: UII: 010-000000702, BISON File and Serve
☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: INTERIOR/OS-09, Hearings and Appeals Files, 80 FR 26291 (May 7, 2015); modification published 86 FR 50156 (September 7, 2021).

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*

☒ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Sex
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service

☒ Mailing/Home Address

☒ Other: *Specify the PII collected.*

A specific tracking number and docket number are assigned to each case in the system and are used to organize filings and retrieve case materials. PII elements submitted into BFS are provided voluntarily by filers and vary by case and document type.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☒ Third party source
☒ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☐ Information Shared Between Systems: *Describe*
☒ Other: Document upload into the system for storage and processing.

D. What is the intended use of the PII collected?

In cases involving individuals, it may be necessary to obtain and hold personal information to process the hearing or appeal. Moreover, individuals who are parties to a hearing or appeal must be given the opportunity to provide information that they deem relevant, including personal information.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

Parties before OHA may include DOI bureaus and offices; the DOI Solicitor's office; other Federal agencies; Tribal, State or Local agencies; corporations and other legal entities; non-profit entities and non-government organizations; and individual members of the public.

In accordance with OHA's SORN, information contained in the BFS system may be disclosed to any and all parties before OHA, as well as authorized party representatives, upon request or in the course of case adjudication, including service lists (list of persons designated by a clerk in a proceeding upon whom parties must serve motions) but excluding documents protected from disclosure by 43 C.F.R. 4.31. Disclosure of the information to these individuals may be necessary for adequate due process to be provided in OHA's administrative adjudications. Further, in accordance with OHA's SORN, OHA may disclose to the public case docket lists that provide limited information on pending cases, such as the docket number, case title, and docketed date. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

Further, final opinions rendered in the adjudication of cases will be disclosed outside DOI as required by 5 U.S.C. 552(a)(2) and 32 C.F.R. 2.1(g); 2.67(b). OHA may also disclose to the public decisions and orders that are not required to be disclosed under 5 U.S.C. 552(a)(2), if such disclosure would not cause a clearly unwarranted invasion of personal privacy; and such documents would not otherwise be exempt from disclosure under 5 U.S.C. 552(b).

BFS does not provide the general public access to case files; access is restricted to OHA personnel and to parties and authorized representatives for the specific case(s) to which they are associated, consistent with due process requirements and 43 CFR Part 4 procedures.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The data will only be shared between OHA Judges, Attorneys, Paralegals, and/or Legal Assistants who process and adjudicate the hearing or appeal in question.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

Data is provided to OHA by the Bureau or Office that rendered the decision subject to hearing, appeal or referred the file to OHA for a hearing. Records are also returned to the originating Bureau or Office at the conclusion of a hearing or appeal. These records include any PII initially received by OHA, and other PII received during the hearing or appeal pertinent to its resolution. Bureaus/offices that are parties to a case may have access to documents containing PII during the adjudication of the case through BFS as authorized and outlined in the routine uses found in INTERIOR/OS-09. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
Other Federal Agencies that are parties to a case may have access to documents containing PII during the adjudication of the case through BFS as authorized and outlined in the routine uses found in INTERIOR/OS-09. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. Information from BFS is not shared on a system-to-system basis.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Other Tribal, State or Local Agencies that are parties to a case may have access to documents containing PII during the adjudication of the case through BFS as authorized and outlined in the routine uses found in INTERIOR/OS-09. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn. Information from BFS is not shared on a system-to-system basis.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors will only access information needed in performance of official duties as authorized under routine uses found in INTERIOR/OS-09. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☒ Other Third-Party Sources: *Describe the third-party source and how the data will be used.*

Information may be shared with parties and their authorized representatives as authorized and outlined in the routine uses found in INTERIOR/OS-09. The SORN may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals voluntarily choose to provide information when participating in an OHA matter. The Privacy Act Statement appears upon account registration. An individual may decline to provide information by omitting it from entry, but failure to provide such information may result in OHA's inability to adequately adjudicate that individual's hearing or appeal or may result in the individual not being able to meet the requirements necessary for success in their hearing or appeal (e.g., standing to appeal).

Parties can also request a protective order to limit the disclosure of documents or information pursuant to 43 C.F.R. § 4.31. Paragraph (a) of § 4.31 provides a basis for submitting to OHA information that is not to be disclosed to the public, but that may be disclosed under paragraphs (b) and (c) to a party to the appeal who agrees under oath in writing not to disclose the information except in the context of the proceeding and to return all copies at the conclusion of the proceeding. Paragraph (d) of § 4.31 applies when a person submitting a document claim that disclosure of information in the document to another party to the proceedings is "prohibited by law, notwithstanding the protection provided under paragraph c of this section." Under § 4.31(d), the person submitting the document will request that OHA review such evidence as a basis for its decision "without disclosing it to the other party or parties" to the proceeding.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: The following notice is provided on screen during user registration, and the user is required to acknowledge consent prior to registering for a system account.

Privacy Act Statement

This is a Privacy Act System of Records

Access to this information is limited to only those who have a need for the information in the performance of their official duties. Disclosure without the consent of the subject of the information is restricted unless required by the Freedom of Information Act, or as permitted under the Privacy Act and outlined in 43 C.F.R. 2.231 or as a routine use in the Hearing & Appeals Records - Interior, OS-09 system of records notice.

These records may not be altered or destroyed except as authorized by 43 C.F.R. § 2.227.

The Privacy Act contains provisions for criminal penalties for knowingly and/or willfully disclosing information from this system unless properly authorized.

Figure 1: Privacy Act Statement

☒ Privacy Notice: Notice is provided through the publication of this PIA and published systems of records notices including INTERIOR/OS-09, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

A specific tracking number and docket number are assigned to each case in the system and used to retrieve associated information.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

OHA will not use BFS to produce reports based on data collected from individuals. Reports are routinely run from BFS to show the status of individual cases. These reports are for OHA internal docket management purposes and are not shared with the parties or the public.

OHA does publish orders and decisions in the adjudication of their cases that may contain information pertaining to individual parties to the case. In those orders and decisions, the judge summarizes the facts, the issues in dispute, the applicable law, and makes a legal determination on the issues. These orders and decisions are provided to the parties, and many of them are made available on the OHA website to assist other parties in making legal

decisions or arguing their cases. When posted to the OHA website, PII such as phone numbers, addresses, and email addresses are removed or redacted. While these orders and decisions are produced by judges, and not by BFS itself, they are routinely uploaded to the system.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

In adjudicatory proceedings, procedural safeguards are used to evaluate the credibility of witnesses and determine the validity or accuracy of information presented. For example, parties to appeals can file pleadings, briefs, and other documents to challenge the accuracy of any information in the record compiled by the bureau. Parties to hearings can present testimony and cross-examine witnesses to challenge the accuracy of any information presented in the case.

B. How will data be checked for completeness?

In adjudicatory proceedings, using the procedural safeguards described above, the judge and the parties are responsible for ensuring that the record is complete and contains information necessary for resolution of the case.

User registration data is verified and validated by comparison with the registrant's login.gov registration data for completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

In adjudicatory proceedings, using the procedural safeguards described above, the judge and the parties are responsible for ensuring that the information in the administrative record is current and not out-of-date.

User registration data is verified through GSA's login.gov user registration to ensure matching credentials when users apply for access to the system. Access is then managed through Multi-factor Authentication (MFA) provided by login.gov.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Case and docket data will be retained for the life of the system plus 3 years in accordance with the OHA records disposition schedule (OHA Record Management Schedule – 6301thru 6307). Documents in the system may be retained for up to 8 years in accordance with the OHA records disposition schedule (OHA Record Management Schedule – 6301thru 6307); however, many documents will only be retained for up to six months after conclusion of the

OHA proceeding and then will be purged from the BFS system and returned to the Bureau or Office that originated the matter.

User accounts will be deactivated after 45 days of inactivity and require a request to reactivate if access is required. User accounts will not be deleted. User account records are retained to support system security, auditability, and accountability and are managed in accordance with applicable records schedules and Department policy.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Records are disposed of in accordance with the OHA records disposition schedule (OHA Record Management Schedule – 6301thru 6307), Departmental policy, and National Archives and Records Administration guidelines.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Privacy risks exist at each stage of the information lifecycle because BFS processes case filings that may include sensitive PII (for example, contact information, identifiers, and information submitted as evidence). The primary risk across collection, use, processing, and retention is unauthorized access, misuse, or accidental exposure of case information. This risk is mitigated through role-based access controls and least-privilege permissions so users can only access the cases and documents necessary for their role and, for non-OHA users, only the case(s) in which they are a party or authorized representative. Data is protected using the security controls described in Section 4, including strong authentication, encryption, and audit logging to detect and investigate inappropriate access.

During collection and processing, parties submit documents through the e-filing function, creating a risk that individuals may include more personal information than necessary. OHA mitigates this risk through procedural safeguards (including the ability to request protective treatment of sensitive filings under 43 CFR § 4.31) and by limiting access to filings to authorized case participants. During disclosure, the primary privacy risk is inappropriate sharing of case documents or public release of PII. BFS disclosures are limited to authorized parties and representatives as required for due process and case adjudication, and any disclosures outside the case process occur only as permitted by the Privacy Act and consistent with the published routine uses in INTERIOR/OS-09, Hearings and Appeals Files.

During retention and destruction, privacy risks include retaining information longer than necessary or improper disposal. BFS records are retained and disposed of in accordance with the approved OHA records schedule and Department policy, and records are disposed of using approved methods to prevent recovery. Collectively, these lifecycle controls reduce the likelihood and impact of unauthorized access or disclosure and support fair adjudication while protecting individual privacy.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: In cases involving individuals, it may be necessary to obtain and hold personal information to process the hearing or appeal. Moreover, individuals who are parties to a hearing or appeal must be given the opportunity to provide information that they deem relevant, including personal information.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No (n/a)

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No (n/a)

E. How will the new data be verified for relevance and accuracy?

Not Applicable. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Non-OHA users are only given access to records in the system that are associated with the case(s) to which they are a party or authorized representative. Non-OHA users must register in the system using login.gov and will gain access to specific case records by OHA user approval, or by initiating the case in the system.

OHA user access to non-public information is restricted to OHA employees who need the information to do their jobs. There is a documented process for requesting, establishing, issuing, and closing OHA user accounts. Access to the system must be requested by the user's supervisor in writing via a memo or an e-mail to the IT Manager. This request must identify the specific level of access the user requires to do his or her job. Access is limited to the lowest possible need for access to the PII data in the case.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes: Contractor developers will perform their tasks in separate development and testing environments using simulated data and will never have access to live system data. The contract contains FAR Clause 52.239-1 is titled "Privacy or Security Safeguards" to address Privacy and security concerns

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes: *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes: The system maintains audit logs that record username and time for each action taken in the system. The ability to identify, track, and monitor is from a technical security audit logging perspective only. Audit logging is implemented solely for information security, compliance, and operational integrity and is not used for behavioral surveillance.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system collects time and type of action taken in the system in relation to a specific username.

M. What controls will be used to prevent unauthorized monitoring?

BFS is designed to protect data fields once the filer data has been entered and completed. Access and permission levels have been established by the System Owner and authorized only to those individuals who must have the information contained in the system to carry out their roles and responsibilities. Pursuant to OMB Circulars A-123, and A-130, BFS has controls in place to prevent unauthorized access to the data in the system. Users are greeted with system use notification which outlines the consequences for unauthorized use and monitoring of US government information system that users must acknowledge before access is granted. The ISSO will perform audit logs review pursuant to OCIO policy and procedures to identify any malicious use of the system and report to system owner for further investigation. No user within DOI can access the system without prior approval from the System Owner. Data at rest and in transit are encrypted using FIPS 140-2 approved encryption keys. BSF follows the DOI and other Federal Government IT Security Standards for this system. Further, access to the system is through multi-factor authentication method for both end users and privilege users.

The system is hosted by the vendor in a FedRAMP-authorized cloud environment and is operated in accordance with documented security controls and continuous monitoring requirements. Security measures are implemented to reduce the likelihood and impact of unauthorized access, disclosure, or alteration of system information. BFS follows the official rules for how users get access, how permissions are managed, and how the system is regularly checked. These rules come from FedRAMP—a government program that ensures cloud services are secure. BFS has received FedRAMP approval (Package ID: FR2108649352).

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☐ Secured Facility
☐ Closed Circuit Television
☐ Cipher Locks

☐ Identification Badges
☐ Safes
☐ Combination Locks
☐ Locked Offices
☒ Other:

The solution is hosted and secured in a vendor hosted data center. The vendor does not publicly share physical security protocols for its on-premises hosting located in Ashburn, VA

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☐ Intrusion Detection System (IDS)
☐ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other: *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☐ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☐ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other: *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The System Owner, the OHA IT Manager, and the OHA IT Privacy Liaison are responsible for implementing and maintaining system-specific privacy and security protections for BFS. The Department Privacy Office provides Department-wide privacy governance oversight, including review of Privacy Act compliance alignment, privacy risk management, and PIA maintenance. Privacy Act complaints and requests for redress are addressed pursuant to DOI policy and applicable DOI Privacy Act regulations, in coordination with OHA and the Department Privacy Office as appropriate.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The System Owner, the OHA IT Manager, the OHA IT Privacy Liaison, the DOI Associate Privacy Officer are responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information reported to DOI-CIRC within one hour of discovery, consistent with Department procedures. Breach response coordination and privacy risk assessment activities are conducted in coordination with the Department Privacy Office to ensure timely intake, prioritization, notification decision-making, and remediation, as appropriate.

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the DOI Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Information System Owner

Name: Amy Sosin
Title: Administrative Law Judge / Acting Director
Bureau/Office: Office of Hearings and Appeals
Phone: 7103.235.0176 Email: Amy_Sosin@oha.doi.gov

Signature: AMY SOSIN Digitally signed by AMY SOSIN Date: 2026.01.08 09:28:47 -05'00'

Information System Security Officer

Name: Jason W. Sanders
Title: DOI-OCIO Information System Security Officer
Bureau/Office: Interior Business Center/Office of the Secretary
Phone: 385-214-6950 Email: Jason_Sanders@ios.doi.gov

Signature: JASON SANDERS Digitally signed by JASON SANDERS Date: 2026.01.08 07:10:20 -07'00'

Privacy Officer

Name: Adrienne Brooks-Hill
Title: Departmental Offices Associate Privacy Officer
Bureau/Office: Office of the Secretary
Phone: 202.208.3368 Email: Adrienne_Brooks-Hill@ios.doi.gov

Signature: ADRIENNE BROOKS-HILL Digitally signed by ADRIENNE BROOKS-HILL Date: 2026.01.07 15:40:23 -05'00'

Reviewing Official

Name: Walter Clay
Title: Acting Departmental Privacy Officer
Bureau/Office: Office of the Chief Information Officer
Phone: 202.279.1712 Email: Walter_Clay@ios.doi.gov

Signature: Walter Clay Digitally signed by WALTER CLAY Date: 2026.01.08 10:18:20 -05'00'