U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires Privacy Impact Assessments (PIAs) to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via this form. For further guidance, consult the DOI PIA Guide.

System or Project Name:	Appraisal and Valuation Information System
System or Project Acronym:	AVIS
Date Signed:	August 14, 2026
System Operational Status:	Operational

Point of Contact

Name:	Jamie Huang
Title:	Privacy Officer
Office:	Department Privacy Officer
Phone:	(202)-208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

☐ New System
☐ New Electronic Collection
☐ Significant Modification
☒ Other: Describe below

Renewal of the Privacy Impact Assessment

2. What is the purpose of the system or project?

AVIS is restricted to authorized users with a valid business need and may contain personally identifiable information, including information concerning private property owners, Indian trust or restricted property interests, appraisers, contractors, and other individuals associated with valuation requests.

AVSO, client bureaus and offices, system administrators, contractors, and authorized users share responsibility within their assigned roles for ensuring that PII maintained in or processed through AVIS is collected, accessed, used, disclosed, retained, and safeguarded in accordance with applicable Privacy Act, records management, cybersecurity, contractual, and DOI requirements. The originating program remains responsible for the authority

and accuracy of information it submits, while AVSO is responsible for privacy protections applicable to AVIS and its use of the information.

3. Is the system registered in BisonGRC?

☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

Appraisal Valuation Information System (AVIS) OS-0025-MAJ-2012, UII CODE: 010-000000699

4. What legal authorities authorize the collection and use of data in this system or project?

AVIS supports DOI appraisal, valuation, real-property, and mineral-evaluation functions performed for DOI bureaus and offices.

Applicable authorities include the Economy Act, 31 U.S.C. § 1535, and the Uniform Relocation Assistance and Real Property Acquisition Policies Act and implementing regulations at 49 CFR part 24, as applicable to covered valuation and real-property acquisition activities.

The responsible AVSO program and client bureau identify the mission-specific authority applicable to the underlying valuation request. Authorities governing privacy, information security, financial management, and information resources management establish requirements for how AVIS information is managed but do not independently authorize every category of PII maintained in AVIS.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: If yes, list the applicable citations below.
☐ No

AVIS maintains records about individuals that may be retrieved by personal identifiers, including name and identifiers associated with an AVIS case. These records require coverage under an applicable Privacy Act System of Records Notice.

AVIS is covered under INTERIOR/BIA-04, Trust Asset and Accounting Management System (TAAMS). DOI is currently coordinating an update to INTERIOR/BIA-04 to expressly reflect AVIS and its appraisal and valuation records and activities.

INTERIOR/BIA-04 was most recently published at 79 FR 68292 (November 14, 2014), with subsequent Department-wide modifications. The PIA will be updated with the citation to the revised BIA-04 notice following publication.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

☐ Yes
☒ No

N/A

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

N/A

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

☒ Name (full, first or last)	☒ Home telephone number	☐ Employment or resume info
☐ Aliases/nickname	☒ Personal Email	☐ Full or Truncated SSN
☐ Driver's license	☒ Mailing or home address	☐ Physical characteristics
☐ Citizenship	☐ Religious preference	☐ Biometrics or facial recognition
☐ Legal Status	☐ Mother's maiden name	☐ Vehicle information
☐ Sex	☐ Marital status	☐ Passport information
☐ Race or ethnicity	☐ Spouse Information	☐ Travel information
☐ Date of birth	☐ Child or family information	☐ Parent's name
☐ Place of birth	☐ Emergency contact info	☐ Credit card number
☒ Personal cell phone number	☐ Financial information	☐ Nationality
☐ Tribal or other ID number	☐ Education information	☐ Disability Information
☐ Military records	☒ Other: Describe below	

AVIS maintains PII necessary to identify real or mineral property interests, identify persons associated with a valuation request, locate the property, communicate with appropriate parties, administer the valuation case, and complete the requested appraisal or mineral-evaluation service.

Information may include an individual's name; residential, mailing, business, email, or telephone contact information; property ownership interests; tax map, parcel, tract or lot numbers; legal property descriptions; deed or recording references; encumbrance information; and other information necessary to support the valuation assignment.

Information concerning private property owners may originate from public land, tax, deed, court, or similar property records. Indian Trust records are not publicly available and are handled as protected government records in accordance with applicable requirements.

Business contact information concerning appraisers, sole proprietors, and contractors may also be maintained when necessary for official appraisal and valuation activities.

2. What is the source for the PII collected? Check all that apply.

☒ Individual	☒ DOI Records
☒ Federal Agency	☒ Third Party Records

☒ Tribal Agency
☒ Local Agency
☒ State Agency
☒ Other: *Describe Below*

PII maintained in AVIS is obtained from DOI client bureau records, individuals, public real-property records, contractors and appraisers, Federal agencies, Tribal agencies, State and local agencies, and other authorized sources.

Property-owner information is provided to AVIS by the responsible client bureau. Client bureaus may obtain that information from public property records or other authorized government records.

AVIS also uses a read-only lookup capability for TAAMS to obtain tract and parcel identifiers needed to identify the property associated with a valuation request. The AVIS-TAAMS interaction is limited to the information described in Section 2, Question 3.

Client information enables AVSO staff to meet national professional standards and state licensing laws for valuation services. AVSO will inform clients of any discrepancies found in AVIS requests to maintain accuracy.

3. How will the information be collected? Check all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Fact Contact
☒ Website
☐ Fax
☒ Telephone Interview
☐ Shared Between Systems: *Describe*
☒ Other: *Describe*

Clients submit valuation requests through the AVIS web application by entering required information and uploading supporting documentation. Information may also be received in paper format, by email, telephone, or face-to-face interaction and entered into AVIS by authorized AVSO personnel.

For BIA-initiated requests, AVIS uses a read-only TAAMS lookup capability to retrieve tract and parcel identifiers needed to identify the property associated with the valuation request. AVIS does not modify TAAMS records or write information back to TAAMS.

Follow-up communication may occur when additional information is needed to verify property, ownership, tract, parcel, or other information necessary to process the valuation request.

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

The AVSO staff utilizes the information provided or collected to engage with assigned qualified contractors, locate the property that is the subject of the request, and to coordinate an inspection of the property with the property owner to comply with professional appraisal standards and State licensing laws. Access to the information is limited to only the DOI staff and contractors engaged in the completion of the specific assignment request. PII contained in AVIS supports mission-related business functions and operations.

5. How does this project limit the collection and use of PII to only what is necessary?

AVIS limits collection and use of PII to information necessary to identify the property interest, establish and administer the valuation assignment, communicate with appropriate property owners or representatives, obtain authorized property access when necessary, and complete or review the requested appraisal or mineral evaluation.

Client bureaus and AVSO personnel are expected to submit only information relevant and necessary to the specific valuation assignment and to avoid including unrelated PII.

Access to AVIS case information is restricted to authorized personnel with a business need associated with the applicable valuation request.

Section 3: Data Sharing and Individual Rights

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

☒ **Within the Bureau/Office:** Describe how the data will be used below.
☒ **Tribal, State or Local Agencies:** Describe how the data will be used below.
☒ **Other Bureaus/Offices:** Describe how the data will be used below.
☒ **Contractor:** Describe how the data will be used below.
☐ **Other Federal Agencies:** Describe the federal agency and how the data will be used
☒ **Other Third-Party Sources:** Describe how the data will be used below.

Within DOI: Authorized AVSO personnel and DOI client bureaus and offices may access AVIS case information as necessary to request, administer, complete, review, and manage valuation services. Access is limited by role, case assignment, bureau or office, and business need.

Contractors: Qualified contract appraisers and other authorized contractors may receive the AVIS case information necessary to complete an assigned valuation service. Access and use are limited to the assigned work and applicable contract, privacy, security, and confidentiality requirements.

Tribal, State, or Local Agencies: Information may be shared with authorized Tribal, State, or local government personnel when required to support an authorized appraisal or valuation activity. These entities do not receive general direct access to AVIS.

Other Third Parties: NGOs identified by the program as supporting valuation activities may receive case information necessary to perform the assigned service. Any such disclosure is limited to the information necessary for the authorized work.

AVIS access permissions do not independently establish authority to disclose PII.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

☐ Yes
☒ No

AVIS does not currently rely on an MOU, MOA, or ISA as the basis for routine sharing among DOI bureaus and offices.

External sharing described in Section 3, Question 1 is governed by the applicable mission authority, contract, agreement, or other program instrument associated with the valuation activity. The absence of an MOU/MOA/ISA does not by itself establish disclosure authority.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

☒ Yes: Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.
☐ No: State the reason why individuals cannot object or why individuals cannot give or withhold their consent.

Individuals do not always have the opportunity to decline the collection or use of information maintained in AVIS because valuation case information may be provided by DOI client bureaus or obtained from authorized government or public property records.

Certain private property owners may choose whether to participate in a voluntary property transaction or provide optional contact information. When information is collected directly from an individual and maintained in a Privacy Act system of records, the applicable Privacy Act Statement explains the authority, purpose, routine uses, whether disclosure is mandatory or voluntary, and the consequences of not providing the requested information.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

☒ Privacy Act Statement:
☒ Privacy Notice:
☐ Other: *Describe Below*
☐ None: *Example - law enforcement cases.*

The DOI system-access warning banner provides notice to AVIS users that use of the Federal information system is subject to monitoring. This security-monitoring notice is separate from the Privacy Act notice applicable to collection of information about individuals.

When information is collected directly from an individual for maintenance in a Privacy Act system of records, the collecting office provides an applicable Privacy Act Statement at or before the point of collection. The Privacy Act Statement identifies the authority, principal purpose, routine uses, whether disclosure is mandatory or voluntary, consequences of not providing the information, and the applicable published SORN.

Client bureaus that collect information through their own forms or processes are responsible for ensuring that the applicable collection notice accurately reflects the subsequent maintenance and use of the information in AVIS.

The AVIS Privacy Act Statement must be aligned with the final published AVIS SORN before being represented as the operative notice for AVIS.

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

Keyword search by Name, Case Number, AVIS Project Number, Tract Number, or Case Property will be only available to authorized AVIS users.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

☐ Yes: Describe the use of these reports and who will have access to them.
☒ No

AVIS does not routinely generate reports whose purpose is to profile, evaluate, rank, or report on specific individuals.

AVIS generates operational and management reports concerning valuation assignments, work in progress, completed cases, workload, processing status, and program performance. Because cases may be associated with named property owners, appraisers, requestors, or assigned personnel, operational reports may incidentally include identifying information.

Access to AVIS reports is limited to authorized personnel with a business need.

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

Data received directly from individuals is presumed to be accurate at the time of submission and individuals can update their information to ensure it remains accurate. The data collected through manual intake is required to be verified by the person providing the information. AVSO staff can identify discrepancies and notify the AVIS System Administrator using the AVIS Helpdesk Ticketing system.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

AVIS contains more than one record series, and retention depends on the underlying valuation activity and applicable NARA-approved disposition authority.

Indian Trust valuation records: Records associated with Indian Trust appraisal activities are maintained in accordance with the NARA-approved disposition authority applicable to the BIA Appraisal Services record series.

Federal lands valuation records: Federal lands valuation case and work files are retained and disposed of in accordance with the NARA-approved disposition authority applicable to AVSO valuation-service records.

AVIS and ECS/eERDMS: When a case reaches closeout status, AVIS transfers the required case record to ECS/eERDMS for records management. AVSO and Records Management will identify the official recordkeeping copy after transfer and the disposition authority applicable to any information that remains in AVIS.

AVIS records and attachments are not destroyed solely on the basis of a configured system-retention period. Disposition is carried out under the applicable NARA-approved records schedule and is suspended when a litigation hold, investigation, audit, or other preservation requirement applies.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

When a valuation request (initiation of a new case file) is entered into AVIS, there are automated validation mechanisms to ensure that required information fields are completed. Certain data fields are subject to additional validation to ensure that the proper type of data is entered. Document attachments are reviewed by AVSO staff for completeness whenever a new service request is submitted.

Data may be checked for completeness by authorized users entering the data into AVIS for completeness and they are responsible for ensuring the information is correct by verifying the information at the time it is collected or received; and authorized users that review data in AVIS are responsible for the completeness of the data provided.

3. Does the project include logging capabilities to record and monitor access to PII?

☒ Yes
☐ No

AVIS maintains audit logs that record relevant user and system events, including date and time, event source, event outcome, and the identity of the user or subject associated with the event.

Access to audit information is restricted to authorized personnel with security, administrative, audit, or investigative responsibilities. Audit logs are reviewed in accordance with the documented AVIS security and continuous-monitoring process to identify unauthorized access, suspicious activity, or other security events involving AVIS information.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

AVIS presents privacy risks associated with maintaining information from multiple client bureaus in a centralized case-management system.

Overcollection risk: Valuation requests and supporting documents may contain more PII than is necessary for the assignment. AVSO and client bureaus mitigate this risk by limiting information submitted to that which is

relevant and necessary to the valuation service.

Access and disclosure risk: AVIS case information may be accessed by AVSO personnel, client bureaus, contractors, and other authorized participants. Access is restricted by role, case assignment, bureau or office, and business need.

Indian Trust information: AVIS supports valuation activity involving Indian Trust property. Trust-related records are not treated as publicly available and are restricted to authorized personnel and uses.

Contractor and third-party risk: Contractors and other authorized service providers may receive case information needed to perform an assignment. Access and disclosure are limited to the information necessary to perform the authorized work and are subject to applicable privacy, security, contractual, and confidentiality requirements.

Retention risk: Records may exist in AVIS and ECS/eERDMS during the records lifecycle. AVSO and Records Management identify the official recordkeeping copy and apply the appropriate disposition authority to prevent unauthorized or excessive retention.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*
☒ No

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

☐ Yes: Provide explanation below
☒ No

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

☐ Yes: *Provide explanation below*
☒ No

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

N/A. AVIS does not generate the new or inferred data described in Section 5, Question 2. Accuracy and completeness of source information are addressed in Sections 3.7 and 4.2.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, or have a non-operational AI Component?

☐ Yes
☒ No, *Proceed to Section 7.*

AVIS does not currently use AI, machine learning, generative AI, predictive scoring, automated valuation, or other AI functionality within the authorized AVIS environment.

Valuation determinations are performed by qualified personnel or contractors under applicable professional standards.

Any future proposal to enable AI functionality within AVIS will be reviewed through applicable DOI Privacy, Cybersecurity, and AI governance processes before operational use.

2. How are models validated for fairness, accuracy, and transparency?

☐ Yes
☐ No

N/A. AVIS does not use AI or machine learning models.

3. Are individuals notified of AI-based decisions that affect them?

☐ Yes
☐ No

N/A. AVIS does not make or support AI-based decisions affecting individuals.

4. Are safeguards in place to prevent bias or unintended consequences?

☐ Yes
☐ No

N/A. AVIS does not use AI or machine learning models that could introduce AI-related bias or unintended consequences.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

☐ Yes
☐ No

N/A. AVIS does not use AI or machine learning models that require review, retraining, or ongoing model validation.

6. Is federated learning used for privacy-preserving model training?

☐ Yes
☐ No

N/A. AVIS does not use federated learning or conduct AI or machine learning model training.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

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

Contractors, developers, and system administrators may be engaged in AVIS O&M. User records including roles, profiles, and permissions are assigned by the system administrator. Specific users with Case Manager responsibilities may add other users to the case team when they are assigned responsibility in the workflow. Case team membership allows access limited to only that particular case and access removed after the completion of that case. All federal users authenticate via PIV-enabled SSO through Active Directory / Azure AD.

2. What data protection policies apply to cloud-based PII storage?

AVIS protects personally identifiable information (PII) through end-to-end encryption, including encryption of data at rest and in transit, along with other security controls. AVIS is a Federal Information Security Modernization Act (FISMA) Moderate system and is provided to the Department of the Interior (DOI) as a Software as a Service (SaaS) solution hosted by Salesforce, a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud service provider. The system is assessed in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5 security controls and operates in compliance with DOI cloud computing policies and security requirements.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

AVIS uses role-based access controls, named user accounts, case-level permissions, audit logging, and security monitoring to detect and investigate unauthorized access or suspicious activity involving PII.

Audit logs record relevant user and system activity and are reviewed in accordance with the documented AVIS continuous-monitoring process. Access to audit information is restricted to authorized personnel with an assigned role and need-to-know.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.

☐ No

AVIS performs user-linked audit and security monitoring.

Audit information may identify the user or subject associated with an event and may record the date and time, source, affected record or object, event type, and outcome.

Monitoring is conducted for authorized cybersecurity, system-administration, troubleshooting, compliance, audit, and incident-response purposes. Access to monitoring capabilities and audit records is restricted by role and need-to-know.

5. Will contractors be involved in the following project activities? Check all that apply.

☒ Design
☒ Development
☒ Maintenance

The appropriate privacy clauses and provisions were included in the contract with Salesforce.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Lock
☒ Other: *Describe Below*

Technical Controls

☐ Password
☒ Firewall
☒ Encryption
☒ User Identification
☒ Other: *Describe Below*
☒ Intrusion Detection Systems (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☐ Biometrics

Administrative Controls

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

☒ Other: *Describe Below*

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals with concerns regarding AVIS's collection, maintenance, use, disclosure, access, or amendment of personal information may contact the Department Privacy Office or use the Privacy Act procedures established by DOI regulations and the applicable AVIS SORN.

The Department Privacy Office coordinates with the AVIS System Manager, System Owner, client bureau, and other appropriate officials to review and respond to privacy complaints..

8. What processes are in place for individuals to access their information?

Individuals seeking access to records about themselves maintained in AVIS and covered by a Privacy Act system of records may submit a Privacy Act request in accordance with DOI Privacy Act regulations and the records-access procedures identified in the applicable AVIS SORN. DOI verifies identity as required before releasing protected records.

Individuals may separately submit a FOIA request for agency records under the Freedom of Information Act. FOIA and Privacy Act requests are processed under their respective statutory and regulatory requirements.

The public does not receive direct system access to AVIS for purposes of exercising Privacy Act or FOIA rights.

- Go to the DOI FOIA Public Access Link (PAL) DOI Public Access Link for FOIA Request Submission-Home and choose to submit a FOIA/PA Request for AVIS-managed information.
- Clearly describe the records you are seeking, including system name and relevant date ranges.
- If unable to use PAL, submit a written request by mail or fax to the DOI FOIA office (Office of the Secretary FOIA office), specifying it's for records held by AVIS.
- DOI's FOIA office forwards AVIS-related requests to the Office of the Secretary FOIA (OS-FOIA), which processes them for the Appraisal and Valuation Services Office.
- DOI verifies your identity as needed, conducts record searches, applies relevant PA or FOIA exemptions, and produces a formal response.
- You can monitor your request's status, communicate with FOIA staff, and retrieve documents—all via PAL.
- Review the released records. If any are improperly withheld, you may file an administrative appeal or request mediation through NARA's Office of Government Information Services (OGIS).

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Routine factual or administrative corrections identified during valuation processing may be addressed by authorized AVSO or client-bureau personnel.

Individuals seeking amendment or correction of records maintained about them in a Privacy Act system of records may also use the amendment procedures established by DOI Privacy Act regulations and the applicable AVIS SORN.

Administrative correction through AVIS personnel or the Help Desk does not replace an individual's Privacy Act amendment rights.

10. 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 AVIS System Owner is responsible for operational oversight of the system and for ensuring that AVIS access and information are managed in accordance with applicable security and privacy requirements.

The System Owner, ISSO, administrators, contractors, client personnel, and other authorized users must promptly report suspected or confirmed loss, compromise, unauthorized access, use, or disclosure of PII through DOI's established incident-response process.

Suspected privacy incidents are reported to DOI-CIRC and the Department Privacy Office in accordance with the current DOI Privacy Incident and Breach Response Plan. Authorized DOI officials make breach, notification, and external-reporting determinations.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving AVIS, DOI will follow the procedures outlined in the **DOI Privacy Breach Response Plan.** A risk scoring matrix will be detailed in the updated DOI Privacy Breach Response Plan:

1. **Immediate Reporting** – Any suspected or confirmed breach must be reported within **one hour** of discovery to the DOI Computer Incident Response Center (DOI-CIRC) and the DOI Privacy Officer.
2. **Containment and Mitigation** – The ISSO and DOI-CIRC work to secure affected systems, revoke compromised credentials, and prevent further data loss.
3. **Risk Assessment** – The Privacy Officer and breach response team assess the nature and scope of the breach, the sensitivity of the compromised PII, and the potential risk to affected individuals.
4. **Notification** – If required, affected individuals will be notified without unreasonable delay, consistent with OMB M-17-12 and DOI policy, providing:
    - A description of the incident
    - The type of information involved
    - Steps individuals can take to protect themselves
    - DOI contact information for questions and assistance
5. **Oversight Reporting** – DOI will report to OMB, Congress, DHS, and other required oversight bodies when thresholds for major incidents are met.
6. **Remediation and Prevention** – The system team will implement additional controls, update procedures,

and retrain personnel to prevent recurrence. ISSO will consult Departmental Privacy Officers before external notifications to impact individuals should a breach occur.

These steps ensure a coordinated, timely, and compliant response to mitigate harm to individuals and uphold DOI's legal obligations. The system owner with guidance from the ISSO will follow the DOI Enterprise Computer Security Incident Response Plan to work with the OCIO Privacy Office when responding to a breach.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

This PIA will be reviewed periodically to ensure that it continues to accurately describe AVIS operations, categories of individuals and PII, sources, TAAMS interaction, retrieval, sharing, contractor and third-party access, cloud services, retention, safeguards, and privacy risks.

AVIS will also be evaluated through the applicable DOI annual PTA review and reaffirmation process.

The PIA will be updated when a material privacy change occurs, including changes to system functionality or architecture, categories of PII or individuals, TAAMS or other interfaces, retrieval practices, SORN coverage, sharing or recipients, contractor or provider access, retention practices, or AI capabilities.

When review confirms that no material privacy change has occurred and the existing PIA remains accurate, it may be reaffirmed in accordance with DOI privacy procedures.