



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 Data Management and Report Generation
System or Project Acronym:	AVSO ADMRG System
Date submitted for review:	March 6, 2026
System Operational Status:	Operational

Point of Contact

Name:	Kenneth Daw
Title:	Valuation Systems Manager
Office:	Appraisal and Valuation Services Office (AVSO)
Phone:	(202) 365-6912
E-mail:	kenneth_daw@ios.doi.gov
Address:	HARTFORD

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

This PIA is being updated to transfer the existing assessment into the current Section 508-compliant DOI PIA template and to clarify how ADMRG handles limited personally identifiable information (PII). There have been no material changes to the system's purpose, functionality, data sources, users, sharing, or operating environment.

The core structured data maintained in ADMRG continues to consist of property, transaction, and comparable-sales information. This update clarifies that authorized AVSO appraisers may enter limited PII in free-text notes when necessary to document valuation research or follow-up communications.

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

The Appraisal Data Management and Report Generation (ADMRG) system supports the Appraisal and Valuation Services Office (AVSO) in providing real-property valuation services for the Department of the Interior (DOI).

ADMRG is a commercial off-the-shelf database and report-generation tool used by authorized AVSO appraisers to enter, organize, analyze, and report property and comparable-sales information. The system's core structured data consists of information about real property and real-estate transactions, including property location, physical characteristics, transaction details, and comparable-sales information obtained from Federal, Tribal, State, county, local, commercial, and other publicly available or authorized sources.

Members of the public do not directly enter information into ADMRG. DOI employees and authorized contractor personnel enter information obtained during appraisal research. When necessary to document the source of valuation information or permit follow-up, an appraiser may enter limited information about a person contacted during the research process in an unstructured comment field. This information may include the person's name, role in the transaction, telephone number, email address, date of contact, and a brief description of the communication.

ADMRG-generated reports are based primarily on property and transaction information. Limited contact information maintained in free-text notes is not included as a standard report field and is not intended for inclusion in valuation reports or public products. Completed reports may be placed in authorized appraisal case files that are maintained separately from ADMRG and subject to the access and retention requirements applicable to those files.

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.

OS-0112-GSS

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

- Federal Land Policy and Management Act of 1976 (FLPMA), as amended [Pub. L. 94-579, 90 Stat. 2743 (1976) (codified as amended at 43 U.S.C. §§ 1701–1787)]
- Federal Land Exchange Facilitation Act of 1988 (FLEFA) [Pub. L. 100-409, 102 Stat. 1086 (1988) (codified at 43 U.S.C. § 1716)]. Section 3
- Financial Institutions Reform, Recovery and Enforcement Act of 1989, Title XI, as amended [Pub. L. 101-73, 103 Stat. 183 (1989) (codified as amended at 12 U.S.C. § 3331)]
- Indian Land Consolidation Act of 1983 (ILCA), as amended [Pub. L. 97-459, 96 Stat. 2517 (1983) (codified as amended at 25 U.S.C. §§ 2201–2221)]
- Indian Self-Determination and Education Assistance Act of 1975 (ISDEAA), as amended [Pub. L. 93-638, 88 Stat. 2203 (1975) (codified as amended at 25 U.S.C. §§ 5301–5368)]
- Indian Trust Asset Reform Act (ITARA) [Pub. L. 114-178, 130 Stat. 432 (2016) (codified at 25 U.S.C. §§ 5601–5636)]. Title III ,
- Uniform Relocation Assistance and Real Property Acquisitions Policies Act of 1970, as amended [Pub. L. 91-646, 84 Stat. 1894 (1971) (codified as amended at 42 U.S.C. §§ 4601– 4655)]
- Land and Water Conservation Fund Act of 1965, as amended [Pub. L. 88-578, 78 Stat. 897) (1965) (codified as amended in scattered sections of title 54 U.S.C.).

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

ADMRG records are organized and routinely retrieved using property- and transaction-related identifiers, such as property address, parcel or land identifier, geographic coordinates, comparable-sale number, transaction number, or other real-property information.

Names and contact information may appear in unstructured comments when an appraiser documents a valuation-related contact. ADMRG is not indexed by those personal identifiers, and authorized users do not routinely retrieve records for the purpose of locating information about an individual by name, telephone number, email address, or another identifier assigned to that individual.

Based on the system's current organization and retrieval practices, ADMRG is not maintained as a Privacy Act system of records and does not require a system-specific SORN. If the system is modified or used to routinely retrieve records by a personal identifier, AVSO will submit the change to the Department Privacy Office for a new SORN applicability determination before implementing that use.

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

☐ Yes

☒ No

ADMRG does not provide a form, portal, survey, or other interface through which members of the public enter information into the system. Information is entered into ADMRG by authorized DOI employees or contractor personnel as part of case-specific appraisal research.

Appraisers may conduct individual valuation interviews to clarify property or transaction information. ADMRG is not used to administer a standardized questionnaire or recurring information collection to ten or more members of the public. If AVSO establishes a standardized collection that seeks the same information from ten or more members of the public within a 12-month period, AVSO will coordinate with the applicable Information Collection Clearance Officer before initiating that collection.

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

ADMRG does not host any minor applications, subsystems, modules, or separately managed applications that require independent identification under this PIA.

Supporting enterprise services used for authentication, hosting, security monitoring, or infrastructure are not hosted applications within ADMRG and are governed through their applicable system boundaries and authorization documentation.

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/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 | |

ADMRG primarily maintains structured information about real property, comparable sales, and real-estate transactions. The system is operated by authorized AVSO appraisers and does not provide a public-facing interface for individuals to enter information.

Limited PII may be entered by an appraiser in an unstructured comment field when necessary to document the source of valuation information or permit follow-up with a person involved in or knowledgeable about a transaction. This information may include:

- Name;
- Mailing address;
- Personal or business telephone number;
- Personal or business email address;
- The individual's role in the transaction, such as owner, buyer, seller, broker, tenant, or other knowledgeable party;
- Date and method of contact; and
- A brief factual summary of information provided during the contact.

ADMRG also maintains business contact information for DOI appraisers and authorized users, including names, position titles, official telephone numbers, official email addresses, usernames, account identifiers, and audit information associated with system activity.

ADMRG is not authorized to maintain Social Security numbers, financial account information, medical information, biometric information, or other Sensitive PII in its free-text fields. Appraisers are instructed to enter only the minimum information necessary to document valuation research and related communications..

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

- | | |
|--|--|
| ☒ Individual | ☒ DOI Records |
| ☒ Federal Agency | ☒ Third Party Records |
| ☒ Tribal Agency | ☒ State Agency |
| ☒ Local Agency | ☒ Other: <i>Describe Below</i> |

PII maintained in ADMRG may originate from Federal, Tribal, State, county, or local government records; commercially available or other authorized property-information sources; existing DOI records; correspondence; and case-specific communications with persons who have knowledge of a property or transaction.

Members of the public do not directly enter information into ADMRG. An authorized AVSO appraiser reviews the source information and determines what information is necessary to enter into the system. When an appraiser documents a valuation-related contact, the individual may be the source of the information, but the appraiser is the person who enters the information into ADMRG.

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

- | | |
|--|--|
| ☒ Paper Format | ☐ Fax |
| ☒ Email | ☒ Telephone Interview |
| ☒ Face-to-Fact Contact | ☐ Shared Between Systems: <i>Describe</i> |
| ☒ Website | ☒ Other: <i>Describe</i> |

Authorized AVSO appraisers collect property and transaction information through review of deeds, leases, surveys, purchase agreements, government records, commercial property-data sources, websites, correspondence, and other authorized appraisal research sources.

Appraisers may also obtain information through telephone, email, virtual, or in-person conversations with property owners, buyers, sellers, brokers, tenants, government officials, or other individuals knowledgeable about a transaction or property.

Members of the public do not directly submit information to ADMRG. The appraiser evaluates the information obtained and enters the property, transaction, and comparable-sales data into the appropriate system fields. When necessary, the appraiser may enter limited names, contact information, and factual contact notes in an unstructured comment field.

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

Limited PII maintained in ADMRG is used to identify and document the source of valuation-related information, maintain an appropriate record of an appraiser's research, and permit follow-up when clarification or additional information is needed.

PII is not used to evaluate, rank, profile, or make determinations about an individual. ADMRG's valuation functions and standard reports are based on property and transaction information rather than personal characteristics.

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

ADMRG limits the collection and use of PII by structuring the system around property and transaction information rather than information about individuals. The standard data fields do not solicit personal information about property owners or other transaction participants.

When an appraiser determines that limited PII is necessary to document a valuation-related contact, the

information is entered only in an authorized free-text field. Appraisers are instructed to:

- Enter only the information necessary to identify the source of valuation information or permit appropriate follow-up;
- Avoid entering Sensitive PII or personal information unrelated to the appraisal;
- Record factual, valuation-related information rather than personal opinions or unnecessary details;
- Use information only for authorized appraisal and valuation activities; and
- Correct or remove information that is inaccurate, unnecessary, or entered in error.

Access to the information is limited to authorized users with a business need to perform appraisal, system administration, maintenance, oversight, or compliance responsibilities.

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.

Limited PII maintained in ADMRG is accessible to authorized AVSO personnel who require the information to conduct, review, supervise, or support DOI appraisal and valuation activities.

A contractor responsible for ADMRG maintenance may have limited system access when necessary to perform authorized technical support. Contractor access is governed by the applicable contract, confidentiality requirements, access controls, training requirements, and DOI Rules of Behavior. Contractor personnel are not authorized to use PII for any independent purpose.

PII from the free-text comment fields is not included in standard ADMRG valuation reports, public reports, or publicly released products. ADMRG does not routinely disclose the PII to individuals or organizations outside DOI. Any disclosure outside DOI must be separately authorized by applicable law, policy, agreement, or records-disclosure authority.

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

ADMRG does not routinely exchange or disclose PII to another Federal, State, local, or Tribal agency under a memorandum of understanding, memorandum of agreement, interconnection security agreement, or similar information-sharing agreement.

Property or transaction information obtained from government records or other authorized sources is entered into ADMRG by authorized appraisers. Receipt of information from a source does not, by itself, constitute an ongoing system-to-system information-sharing arrangement.

If ADMRG establishes an automated connection, recurring data exchange, or formal sharing arrangement with another agency, AVSO will document the arrangement and submit it for appropriate privacy, security, legal, and records-management review.

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 may decline to participate in a valuation interview or decline to provide personal contact information, unless provision of specific information is required by applicable law or as a condition of a transaction or other authorized process outside ADMRG.

If an individual declines to participate, the appraiser may continue the valuation using public records, existing DOI records, other transaction records, or other lawful and appropriate sources. Declining to participate may limit the appraiser's ability to verify or supplement information, but it does not result in an automated or adverse determination by ADMRG.

Participation in an interview does not constitute consent to unrelated collection, use, or disclosure of the individual's information. Information obtained during the interview is used only for authorized appraisal research, documentation, and follow-up.

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

☐ Privacy Act Statement:

☐ Other: *Describe Below*

☒ Privacy Notice:

☐ None: *Example - law enforcement cases.*

ADMRG does not collect information from individuals through a public-facing form, website, or portal. Information is entered into the system by authorized DOI appraisers.

When an appraiser obtains limited personal information directly from an individual during a valuation interview, the individual is informed that the appraiser is collecting the information for official DOI appraisal and valuation purposes and that relevant information may be documented in DOI appraisal records. The individual is also informed whether participation and provision of the information are voluntary and how the information will be used.

Information obtained from public records or other sources is not collected directly from the individual. The DOI system login warning banner provides notice to authorized ADMRG users regarding appropriate system use,

access monitoring, and protection of government information; it is not used as the privacy notice to individuals whose information may be referenced in appraisal notes.

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

ADMRG records are routinely retrieved using property- and transaction-specific information, including property address, parcel or land identifier, geographic coordinates, comparable-sale number, transaction information, or other real-property identifiers.

Names and contact information may appear within unstructured appraisal notes, but those personal identifiers are not used as the system's primary indexing or routine retrieval method. ADMRG is used to locate information about properties and transactions, not to create or retrieve profiles or reports about individuals.

Administrative or technical search functions are used only as necessary for authorized system maintenance, troubleshooting, quality review, or other approved operational purposes. If ADMRG begins routinely retrieving records by a person's name or another personal identifier, AVSO will obtain a new SORN determination from the Department Privacy Office before implementing that use.

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

No reports on individuals are produced. ADMRG reports are generated for property appraisal and valuation purposes and are based on property characteristics, comparable sales, geographic information, transaction information, and other real-property data. Limited PII maintained in unstructured comments is not included as a standard report field and is not used to create profiles, summaries, assessments, or reports about individuals.

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

Property and transaction information obtained from external sources is reviewed by the responsible appraiser and compared, where available, against deeds, leases, surveys, purchase agreements, government records, commercial property records, or other reliable source documentation.

Information obtained during an interview may be compared with available source records or confirmed through another knowledgeable source when appropriate. Interview-derived information is documented as information provided by the identified source and is not represented as independently verified when verification is not available.

The appraiser is responsible for reviewing the information entered into ADMRG for relevance, accuracy, completeness, and consistency with the supporting appraisal research.

Section 4: Data Management and Retention

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

ADMRG property-valuation and comparable-sales data are retained for five years in accordance with the applicable Office of the Secretary records schedule, unless a more specific National Archives and Records Administration-approved schedule applies.

Trust appraisal case and work files are governed by TR-6201-P5, Appraisal Services Case/Work Files (Trust), NARA Job Number N1-075-09-6, as applicable. AVSO creates and maintains records supporting real-property appraisal services but does not use ADMRG to manage Indian trust assets.

Records generated from ADMRG and incorporated into an official appraisal case file are retained under the approved records schedule applicable to that case file. Limited PII maintained in ADMRG comments is retained for the same period as the associated property-valuation record unless it is corrected or removed earlier because it is inaccurate, unnecessary, or entered in error.

System audit logs are retained for 3 years after cutoff under NARA-approved DOI records schedules DRS 1.4A(1) DAA-0048-2013-0001-0013 and DRS 1.4A(2) DAA-0048-2013-0001-0014.

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

The responsible appraiser reviews externally sourced property and transaction information for relevance, accuracy, and completeness before or after entering it into ADMRG. Where available, the appraiser compares the entered information with deeds, leases, surveys, purchase agreements, government records, commercial property records, or other supporting documentation.

Information obtained through an interview is reviewed for consistency with available source records and may be confirmed through another knowledgeable source when appropriate. The appraiser records only information relevant to the valuation and identifies interview-derived information as information provided by the source when independent verification is not available.

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

- ☒ Yes
☐ No

ADMRG records user and administrative activity to support security monitoring, accountability, troubleshooting, and investigation of potential unauthorized activity. Logged information includes, as applicable, username or account identifier, date and time of access, authentication activity, records or functions accessed, searches performed, files created or deleted, account changes, and changes to user privileges.

Access to audit information is limited to authorized personnel with security, system administration, oversight, or investigative responsibilities. Logs are reviewed in accordance with established security procedures and retained under the applicable approved records schedule.

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?

ADMRG's core structured data concerns real property and real-estate transactions. Its principal privacy risk arises from the ability of authorized appraisers to enter limited PII in unstructured comment fields when documenting valuation research.

The primary privacy risks and mitigations are:

Collection: There is a risk that an appraiser could enter more personal information than is necessary or could enter Sensitive PII unrelated to the valuation. This risk is mitigated through field instructions, privacy training, data-minimization requirements, and restrictions prohibiting the entry of unnecessary or Sensitive PII.

Accuracy: Information obtained through interviews may be incomplete, inaccurate, subjective, or inconsistent with public records. Appraisers compare information with available source documentation, identify the source of interview-derived information, and correct information when errors are identified.

Use: There is a risk that PII entered for source documentation or follow-up could be used for an unrelated purpose. Access is limited to authorized AVSO personnel and approved contractor personnel with an official business need. PII may be used only to support authorized appraisal, valuation, oversight, maintenance, or compliance activities.

Access and processing: Unauthorized personnel could access information maintained in ADMRG. The system uses role-based access controls, multifactor authentication, user-account approval, annual training, audit logging, and other inherited and system-specific safeguards to limit and monitor access.

Reporting and disclosure: There is a risk that PII from a comment field could be included in a report or otherwise disclosed unintentionally. Standard valuation reports are based on property and transaction information and do not include free-text contact information as a standard report field. Reports are reviewed by authorized personnel and maintained in restricted case files.

Retention: There is a risk that limited contact information could remain in the system longer than needed. Information is retained under applicable approved records schedules and may be corrected or removed earlier when it is inaccurate, unnecessary, or entered in error.

Disposal: Records are destroyed or transferred in accordance with applicable records schedules and approved DOI media-sanitization and records-disposition procedures.

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

ADMRG does not generate predictions, scores, classifications, profiles, or other inferred information about individuals.

The system organizes property, transaction, and comparable-sales information to support professional real-property appraisal activities. Any calculations, comparisons, or reports generated by ADMRG concern properties and transactions rather than personal characteristics or individual behavior.

Professional appraisal conclusions are developed by authorized appraisers using applicable appraisal standards, source records, and professional judgment. ADMRG does not independently make or recommend decisions about individuals.

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

☐ Yes: *Provide explanation below*

☒ No

ADMRG does not generate new data or inferences about individuals and therefore does not place newly derived information into an individual's record.

Information maintained in ADMRG relates primarily to properties, transactions, comparable sales, and appraisal research. Limited names or contact information may be recorded to identify a source or permit follow-up, but ADMRG does not create an individual profile or add analytical conclusions to a record about that person.

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

☐ Yes: *Provide explanation below*

☒ No

The system supports appraisal and valuation activities involving real property. It does not determine an individual's eligibility, rights, benefits, employment status, legal status, access to services, creditworthiness, risk level, or other personal outcome.

Any appraisal conclusions concern the value or characteristics of real property and are made by qualified appraisers using professional judgment and applicable appraisal standards.

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

Not applicable. ADMRG does not generate new data, predictions, scores, profiles, or inferences about individuals.

Property and transaction information entered into ADMRG is reviewed for relevance and accuracy under the source-verification procedures described elsewhere in this PIA. Because the system does not create new individual-level data through aggregation or analytics, no separate verification process for derived individual data is required.

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.*

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

- ☐ Yes
☐ No

The system does not use an artificial intelligence or machine-learning model and does not produce model-generated outputs.

Because no AI or machine-learning model is used, model validation for fairness, accuracy, explainability, transparency, performance, or reliability is not required for the current system.

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

- ☐ Yes
☐ No

The system does not use AI or machine learning to make, support, recommend, prioritize, or influence decisions or actions concerning individuals.

Because the system does not produce AI-based decisions or recommendations affecting individuals, no AI-specific decision notice is required.

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

- ☐ Yes
☐ No

The system does not use AI, machine learning, automated inference, scoring, ranking, recommendation, prediction, or other model-driven functionality that could introduce AI-specific bias or unintended model outcomes.

The system remains subject to all otherwise applicable privacy, security, data-quality, access-control, records-management, and human-review requirements.

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

- ☐ Yes
☐ No

The system does not use, train, fine-tune, retrain, update, or operate an artificial intelligence or machine-learning model.

Because no model is present within the system boundary, no model lifecycle review, retraining, performance monitoring, drift assessment, or model end-of-life process is required.

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

- ☐ Yes
☐ No

The system does not conduct model training and does not use federated learning or another distributed machine-learning technique.

No information maintained by the system is used to train, fine-tune, or improve an AI or machine-learning model.

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

User access to data is managed through a role-based access control system, ensuring that individuals only see the information they need to perform their duties. Specifically, access is restricted by user permissions defined within Active Directory Security groups. This means that users are limited to data access based on their assigned security group level. In practice, data access is limited to authorized AVSO employees and contractor personnel and further restricted based on their specific roles and responsibilities within the organization. This approach ensures that sensitive information is protected and that users only have access to the data necessary for their job functions.

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

ADMRG stores property-valuation data and limited PII within its authorized DOI hosting environment. The system inherits applicable security and privacy controls from the hosting environment and implements system-specific controls for user access, permissions, logging, data use, and contractor access.

Applicable protections include the authorized security baseline for the hosting environment, NIST Special Publication 800-53 controls, DOI cloud and cybersecurity requirements, encryption, multifactor authentication, role-based access control, audit logging, vulnerability management, incident response, and continuous monitoring.

The presence of limited PII in unstructured comments, user-account information, and audit logs is documented in ADMRG's privacy and security records and must remain consistent with the system's Xacta categorization and authorization boundary.

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

The ADMRG system is managed by authorized DOI employees. To ensure security, only approved individuals can access the system. Before gaining entry to the DOI network or any DOI system, and every year after, all users must agree to the DOI Rules of Behavior and complete training on Cybersecurity, Privacy, and Records Management. They also need to complete specific training related to their job roles in privacy and security.

Before anyone can use ADMRG, they must get approval from the system owner or their representative. To monitor and ensure that user access and actions are authorized and within their job duties, the system uses audit logs. Additionally, a user tracking program is in place to identify and report any attempts to access files that are outside a user's approved permissions.

To prevent unauthorized monitoring, access to data, browsing, and misuse, ADMRG utilizes several security measures. These include audit logs, unique user identification, authentication, multifactor authentication – PIV or login.gov, and the mandatory annual security, privacy, and records management training. These features work together to protect the system and its data.

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

The system has the ability to audit usage of the system, including use by authorized individuals and system administrators as needed. This includes reviewable data concerning actions within the system, including username, date and time of day a user accesses the system, specific uniform resource locators (URLs) of component systems, search terms or parameters used to call data, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges.

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

- ☐ Design
- ☐ Development
- ☒ Maintenance

Contractors are involved in system operations and Privacy Act clauses are included in all contractor agreements.

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

Physical Controls

- | | |
|---|---|
| ☒ Security Guards | ☐ Cipher Locks |
| ☐ Key Guards | ☒ Identification Badges |
| ☐ Locked File Cabinets | ☐ Safes |

- | | |
|--|--|
| ☒ Secured Facility | ☐ Combination Lock |
| ☐ Closed Circuit Television | ☒ Other: <i>Describe Below</i> |

All physical security controls are inherited from the OCIO Enterprise Hosting Environment

Technical Controls

- | | |
|--|--|
| ☐ Password | ☒ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☒ Virtual Private Network (VPN) |
| ☒ Encryption | ☒ Public Key Infrastructure (PKI) Certificates |
| ☐ User Identification | ☐ Biometrics |
| ☒ Other: <i>Describe Below</i> | |

Additional technical controls are inherited from the OCIO Enterprise Hosting Environment, Azure Cloud Hosting environment DOI Bison Shield, and Bison Shield Cloud.

Administrative Controls

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

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

Individuals may submit a privacy-related complaint concerning ADMRG to the AVSO System Owner, the applicable Privacy Officer, or the Department Privacy Office.

The complaint will be reviewed to determine whether it concerns the collection, maintenance, use, access, disclosure, accuracy, or safeguarding of PII. Matters involving rights under the Privacy Act will be processed under applicable DOI Privacy Act regulations and procedures. Security incidents or suspected unauthorized disclosures will be reported and handled through DOI's privacy-incident and breach-response process.

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

Individuals seeking to access information maintained by the Appraisal and Valuation Services Office (AVSO) within ADMRG may submit a Freedom of Information Act (FOIA) request (when appropriate):

- Go to the DOI FOIA Public Access Link (PAL) [DOI Public Access Link for FOIA Request Submission-Home](#) and choose to submit a FOIA Request for AVSO-managed information.
- Clearly describe the records you are seeking, 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 AVSO.
- DOI's FOIA office forwards AVSO-related requests to the Office of the Secretary FOIA (OS-FOIA), which processes them for the Appraisal and Valuation Services Office.
- DOI conducts record searches, applies relevant 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?

An individual who believes that factual information associated with an ADMRG property or transaction record is inaccurate may contact AVSO and provide sufficient information to identify the record, explain the alleged error, and provide supporting documentation.

The responsible appraiser or System Manager will review the request against the source documentation and determine whether the ADMRG information should be corrected. When the challenged information originated from another agency, public record, commercial source, or official case file, AVSO may direct the individual to the organization responsible for maintaining the authoritative source record.

If ADMRG is later determined to be a Privacy Act system of records, requests to amend records about an individual will be processed under the Privacy Act and DOI's applicable amendment and appeal procedures.

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 ADMRG System Owner is responsible for ensuring that information maintained in the system is used only for authorized purposes and that appropriate privacy and security safeguards are implemented.

Authorized users are responsible for entering only information necessary for official appraisal activities, protecting information from unauthorized access or disclosure, complying with DOI Rules of Behavior, and completing required privacy, cybersecurity, and records-management training.

The Information System Security Officer supports implementation and monitoring of system security controls. The applicable Privacy Officer and Privacy Analyst provide privacy-compliance guidance and support review of privacy risks, complaints, and incidents.

Any suspected or confirmed loss, compromise, unauthorized access, use, or disclosure of PII must be reported immediately to DOI-CIRC, the applicable Privacy Officer, and the Department Privacy Office in accordance with DOI incident-response requirements.

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 ADMRG, DOI will follow the procedures outlined in the **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.

These steps ensure a coordinated, timely, and compliant response to mitigate harm to individuals and uphold DOI's legal obligations

The AVSO team is in charge of the day-to-day operation and security of the system. They work to make sure data is handled correctly and that all access is secure and trackable. Specifically, they ensure that security and privacy measures are in place. If any PII is lost, compromised, or accessed without permission, the AVSO team and Information System Security Officers must report it to the DOI-CIRC, DOI's incident reporting system, and other relevant DOI officials, following established DOI rules. They must also follow all privacy and security requirements within their own organization and immediately report any potential data security issues in line with Federal and DOI privacy breach policies.

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

The ADMRG Privacy Impact Assessment will be reviewed and updated at least once every **three years**, in accordance with DOI policy and OMB requirements.

Interim updates will occur sooner if any of the following events take place:

- Significant changes to system functionality, architecture, or hosting environment
- Collection of new categories of PII or expansion of data use beyond what is described in the current PIA
- New data sharing agreements or partnerships
- Implementation of emerging technologies (e.g., AI/ML features, cloud service changes) that could alter privacy risks
- Changes to applicable privacy laws, regulations, or DOI policies

The System Owner is responsible for initiating the review process in coordination with the DOI Privacy Officer. All updated PIAs will undergo the standard review and approval process and be made publicly available on DOI's website unless publication is prohibited for security or law enforcement reasons