



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: Minerals Information

Bureau/Office: U.S. Geological Survey/Office of Enterprise Information

Date: April 12, 2019

Point of Contact:

Name: Steven T. Stoller

Title: IT Specialist

Email: [sstoller@usgs.gov](mailto:ssoller@usgs.gov)

Phone: (703) 648-4960

Address: 12201 Sunrise Valley Drive, Mail Stop 988, Reston, VA 20192

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?

The purpose of the system is to collect, store, evaluate, and analyze data from 142 monthly, quarterly, semiannual, and annual canvasses concerning domestic mineral occurrence, production, stocks, value, and use. A number of these minerals and materials have traditionally



been considered as strategic and critical. The data obtained from this collection are used by Government agencies, Congressional offices, educational institutions, research organizations, financial institutions, consulting firms, industry, and the public.

Personally identification information (PII) is collected within the following components for this system:

1. Minerals Information Data System (MIDS) - Collects raw and edited data; produces tables for publication. PII includes name of the person to be contacted, phone number, address, signature, and title.
2. Minerals Archival and Retrieval System (MARS) - Internal imaging system that indexes and stores images of canvass forms according to National Archives and Records Administration (NARA) guidance. PII includes name of the person to be contacted, phone number, address, signature, and title.

C. What is the legal authority?

The Secretary of the Department of the Interior (DOI) is mandated [30 U.S.C. 1601 et seq.] by Congress to collect, evaluate, and analyze information concerning mineral occurrence, production, and use from industry, academia, and Federal and State agencies. The Director of the U.S. Geological Survey (USGS), under Interior Order No. 3193, is delegated, through the Assistant Secretary–Water and Science (DOI), all the program authority necessary to carry out this minerals information function. The mission of the USGS National Minerals Information Center (NMIC) is to collect, analyze, and disseminate information on the domestic and international supply of and demand for minerals and mineral materials essential to the U.S. economy and national security.

- National Materials and Minerals Policy, Research and Development Act of 1980 (30 U.S.C. 1601 et seq.)
- National Mining and Minerals Policy Act of 1970 (30 U.S.C. 21(a))
- Strategic and Critical Materials Stock Piling Act (50 U.S.C. 98 et seq.)
- Defense Production Act
- Comprehensive Test Ban Treaty Part III
- Comprehensive Test Ban Treaty USGS-DoD Memorandum of Agreement

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 CSAM?

- Yes: *Enter the UII Code and the System Security Plan (SSP)*

010-000001013; System Security Plan (SSP) for Science and Support Systems (S&SS) - Moderate

- 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 <i>If Yes, provide a description.</i>
None	None	No	N/A

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

- Yes: *List Privacy Act SORN Identifier(s)*

No: We retrieve information by Respondent ID, which is assigned to an establishment, or company name—no information is retrieved about individuals by name or other unique identifier.

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

- Yes: *Describe* See below

1028-0053 – Nonferrous Metals Surveys – 07/31/2021
 1028-0059 – Comprehensive Test Ban Treaty – 01/31/2020
 1028-0060 – Mine, Development, and Mineral Exploration Supplement – 08/31/2019
 1028-0062 – Industrial Minerals Surveys – 02/28/2022
 1028-0065 – Production Estimate – 01/31/2020
 1028-0068 – Ferrous Metals Surveys – 12/31/2020
 1028-0070 – Consolidated Consumers’ Report – 07/31/2020

- No



Section 2. Summary of System Data

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

- | | |
|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Credit Card Number |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Law Enforcement |
| <input type="checkbox"/> Gender | <input type="checkbox"/> Education Information |
| <input type="checkbox"/> Birth Date | <input type="checkbox"/> Emergency Contact |
| <input type="checkbox"/> Group Affiliation | <input type="checkbox"/> Driver's License |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Race/Ethnicity |
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Social Security Number (SSN) |
| <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Personal Cell Telephone Number |
| <input type="checkbox"/> Truncated SSN | <input type="checkbox"/> Tribal or Other ID Number |
| <input type="checkbox"/> Legal Status | <input checked="" type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Home Telephone Number |
| <input type="checkbox"/> Security Clearance | <input type="checkbox"/> Child or Dependent Information |
| <input type="checkbox"/> Spouse Information | <input type="checkbox"/> Employment Information |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Military Status/Service |
| <input type="checkbox"/> Medical Information | <input type="checkbox"/> Mailing/Home Address |
| <input type="checkbox"/> Disability Information | |
| <input checked="" type="checkbox"/> Other: <i>Specify the PII collected. See below</i> | |

Name of person to be contacted regarding the completed form, phone number, address, signature, date of signature, title.

To comply with the Paperwork Elimination Act, email addresses are collected for those respondents who elect to respond online.

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
- Other: *Describe*

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

Names, addresses, phone numbers, signatures, dates of signatures, and titles are collected to communicate with respondents to canvasses. The PII is not released outside of the USGS NMIC.

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

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

Names, addresses, phone numbers, signatures, dates of signatures, and titles are collected to communicate with respondents to canvasses. The PII is not released outside of the USGS NMIC.

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

- Other Federal Agencies: *Describe the federal agency and how the data will be used.*

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

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

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

Unless authorization is granted (i.e., “May tabulations be published which could indirectly reveal the data reported?”), the data furnished in the completed form will be treated in confidence by



the DOI, except that they may be disclosed to Federal defense agencies, or to the Congress upon official request for appropriate purposes.

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.*

As stated on each collection instrument, responding to these canvasses is voluntary; therefore, individuals can decline to provide their PII. Individuals cannot consent to specific uses of their PII because their PII is never shared outside of the USGS NMIC. Contact information for the USGS NMIC appears on each collection instrument, which individuals can use to request they be removed from the mailing list.

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: *Describe each applicable format.*

The USGS NMIC discloses that responding to the minerals information canvasses is voluntary and that the data furnished on the completed forms will be treated in confidence.

Privacy Notice: *Describe each applicable format.*

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.).

Establishments, such as mines, refineries, or smelters, are canvassed and assigned Respondent ID Numbers. Completed forms are not indexed with any PII identifiers to enable retrieval by that method. Minerals data are retrieved from the system only in aggregate.

I. Will reports be produced on individuals?



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

No

Section 3. Attributes of System Data

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

All data in the system are self-reported by individuals. The USGS NMIC assumes that the contact information provided is accurate. No PII will be associated with the data published. As such, verifying individual data for accuracy and reliability cannot (and should not) be done if privacy is to be maintained; however, all PII data will be examined, and obviously incorrect data will be flagged.

B. How will data be checked for completeness?

All PII data will be quality-controlled by USGS NMIC staff that will look at each response to check for completeness.

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

PII data is immediately updated with more current information provided by the respondent. The PII data are not connected to other data reported on the canvasses; therefore, how current the data are will not affect other data.

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

Under the USGS General Records Disposition Schedule 1301-01, the records are permanent Federal records. Electronic transfer of the official copy to NARA is in 5-year blocks. Paper copies of each record follow Schedule 1302-01 and are destroyed when no longer needed or, by convention, after 3 years.

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

At the end of the retention period, files transferred to the MARS Administrator are reviewed before disposition and, for historical purposes, all electronic files from these canvasses will remain stored indefinitely on secure USGS servers as reference materials and also at NARA.



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.

Any electronic files containing PII are password-protected and stored on firewall-protected USGS secure HTTPS servers in a data center with restricted access. Software is regularly updated to prevent system vulnerabilities. Only USGS NMIC staff are able to access the PII in the Minerals Information Data System and Minerals Archival and Retrieval System, after logging in with two-factor authentication. All staff members have undergone information security and privacy awareness training.

Paper canvasses are returned in business reply envelopes that are not pre-printed with return names and addresses on them. These paper forms are secured by USGS NMIC staff in locked filing cabinets in locked rooms in a USGS secure facility (a USGS Federal ID badge is required to enter the building without an escort). Respondents who choose to respond online are sent email reminders to give them ample opportunity to complete the canvasses, if they wish to do so. For individuals who have already completed canvasses, no “second-request” paper forms will be sent and, for individuals replying via the Web interface, no reminder notices will be sent.

Minerals information data published are presented only in aggregate. There are no risks associated with this reporting as no individual PII is ever included.

There is no risk to individual privacy because while the system contains personal contact information, that information is only associated with the establishments for whom respondents work (and, if they are company officers, may already be public record) rather than with residences or personal cell phone numbers.

There is no risk to PII information in association with any Freedom of Information Act request because the information disclosed in these canvasses is proprietary and therefore not subject to that Act.

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: *Explanation*

The collection of basic non-sensitive PII is necessary for the USGS NMIC to meet its mission to collect, store, evaluate, analyze, and publish aggregated information on the occurrence, production, and consumption of nonfuel minerals and materials essential to the U.S. economy, the national security, and protection of the environment. Without this PII, it would not be



possible to maintain an engaged universe of respondents or to follow up with individuals for further information about their submitted data.

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

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

Yes: *Explanation*

No

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

Not applicable. There are no new data being derived.

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?

Access permissions are restricted on a need-to-know basis. For example, USGS NMIC statistical assistants are able to access PII associated only with canvasses to which they have been assigned.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed? Yes.*

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. *Explanation*

Session information is captured as part of security and troubleshooting. Both the USGS and online canvass software system can identify and monitor a user's actions in the system through server logs, which record log on attempts, user names, files accessed, dates and times of access, and success or failure of actions taken. If an individual attempts to access a password-protected file on a USGS server and fails, that action is logged. Any action or modification to components of the system containing PII is automatically tracked in audit logs by recording the user name, time, and date of the change.



No

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

Dates and times for logons and logon attempts, user names, files accessed along with dates, and times of access.

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

Controls used to prevent unauthorized network monitoring include regular security scans, security audit logs accessible only by the system administrators, the HTTPS protocol, and storage of data only on servers housed in a secure and conditioned room and located behind firewalls. Software is regularly updated to prevent system vulnerabilities. Access to servers is limited physically and through security configurations for staff with a need-to-know function. If unauthorized monitoring is identified, the issue is resolved promptly. A system of user names and passwords based on the least permissions needed is used to limit access. All system administration and development personnel are required to complete not only Federal Information Security and Privacy Awareness training, but also Role Based Security Training and Role Based Privacy Training.

Before users log on, they see a banner consenting to monitoring and warning of unauthorized access. Only the system administrators have administrative privileges and least privileges are in place on a need-to-know basis.

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. *Describe*

(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 Director of the USGS NMIC (Steven Fortier) serves as the Information System Owner and the official responsible for oversight and management of the USGS NMIC security and privacy controls, including the protection of information processed and stored by the USGS NMIC program. The Information System Owner and the NMIC Privacy Act System Manager (Michael Magyar) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored by the USGS NMIC program. The System Manager is responsible for protecting the privacy rights of the public for the information collected, maintained, and used in the system of records, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as addressing complaints and requests for redress or amendment of records in consultation with the USGS Privacy Officer according to the processes outlined in the USGS Guide for Handling Privacy Act Records.



Each canvass instrument provides a USGS NMIC address and phone number for questions concerning completion of the form. Additionally, for canvasses which are included in the USGS NMIC's seven information collections, an email address is provided for comments regarding the collection of information.

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?

As the Information System Owner, the Director of the USGS NMIC is responsible for oversight and management of the USGS NMIC security and privacy controls and for ensuring, to the greatest possible extent, that USGS NMIC data is properly managed and that all access to USGS NMIC data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the USGS Computer Security Incident Response Team (CSIRT) immediately upon discovery in accordance with Federal policy and established procedures. All NMIC staff members who become aware of such an event have the responsibility to inform their assigned CSIRT Point of Contact.



Section 5. Review and Approval

Information System Owner

Name: Steven Fortier

Title: Center Director

Bureau/Office: U.S. Geological Survey/National Minerals Information Center

Phone: (703) 648-4920

Email: sfortier@usgs.gov

Signature: STEVEN
FORTIER

Digitally signed by STEVEN
FORTIER
Date: 2019.03.22 11:59:11
-04'00'

Date: March 22, 2019

Information System Security Officer

Name: Morganai K. Kelley

Title: Information Technology Specialist

Bureau/Office: U.S. Geological Survey/National Minerals Information Center

Phone: (703) 648-4932

Email: mkkelley@usgs.gov

Signature: MORGANAI
KELLEY

Digitally signed by
MORGANAI KELLEY
Date: 2019.03.22 16:27:51
-04'00'

Date: March 22, 2019

Privacy Officer

Name: Alan Wiser

Title: Associate Privacy Officer (Acting)

Bureau/Office: U.S. Geological Survey/Office of Enterprise Information

Phone: (865) 322-0241

Email: awiser@usgs.gov

Signature: *Alan T. Wiser*

Digitally signed by ALAN
WISER
Date: 2019.03.26 08:05:01
-04'00'

Date: March 26, 2019

Reviewing Official

Name: Timothy S. Quinn

Title: Associate Chief Information Officer

Bureau/Office: U.S. Geological Survey/Office of Enterprise Information

Phone: (703) 648-6839

Email: tsquinn@usgs.gov

Signature: TIMOTHY
QUINN

Digitally signed by TIMOTHY
QUINN
Date: 2019.04.12 15:57:34
-04'00'

Date: April 12, 2019