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: Blaster Certification Program/Blaster Certification Tracking System
Bureau/Office: Office of Surface Mining Reclamation and Enforcement (OSMRE)
Date: August 2, 2023
Point of Contact
Name: Patrick Dege
Title: Associate Privacy Officer
Email: osmre_privacy@osmre.gov
Phone: 202-208-3549
Address: 1849 C Street NW, 1200W, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

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

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

B. What is the purpose of the system?

The Blaster Certification Program/Blaster Certification Tracking System is used to enable the Office of Surface Mining, Reclamation and Enforcement (OSMRE) to effectively issue and manage blaster certificates to individuals (blasters), to conduct blasting operations in any Federal Program State or on Indian lands under Federal jurisdiction while meeting the regulatory performance standards of the

Surface Mining Control and Reclamation Act of 1977 (SMCRA). To accomplish this, the OSMRE Blaster Certification Program (BCP): reviews blaster applicant's background, status, employment history, blasting experience and violation status to ensure compliance with specific State and Federal authority and regulations and maintain adequate control and access of record information. The OSMRE Blaster Certification Program serves as a tool for OSMRE to grant blaster applicants' certificates for issuance, renewal, reissuance and reciprocity status, administration, and notification procedure as well as to provide an adequate system of records for the Department, and for compliance within the Department for a Federal program and enable OSMRE as the regulatory authority to effectively monitor its program requirements. Additionally, the program allows OSMRE to track appropriate actions when a blasting violation occurs, or a discrepancy with application information and the affirmation by the applicant or when verification of a blasters status is requested by state or mining company official.

The certification of blasters is an important regulatory function under the Surface Mining Control Reclamation Act (SMCRA). Highly trained and skilled blasters are crucial to ensure safe, efficient, and compliant blasts in coal mining operations. Properly trained blasters can design and conduct blasts that use the best technology currently available, while meeting the regulatory performance standards of SMCRA. Highly competent and successful blasters also maintain a responsible relationship with surrounding residents, thereby reducing the number of complaints. As a regulatory authority (RA), OSMRE is responsible for certifying blaster competence based upon the right mix of experience, training, and testing.

The Blaster Certificate Tracking System (BCTS) is a resource for SMCRA regulatory program personnel to monitor blaster certifications nationally. The BCTS is a database containing information on each OSMRE certified blaster, status of their certification (e.g., active, revoked, suspended, expired), and a blasting violation history. The tracking system helps track certified blasters and facilitates reciprocity with other RAs. Furthermore, the tracking system facilitates compliance inspections and assists the OSMRE Blaster Certification Program personnel in notifying certified blasters of upcoming expirations. Personally identifiable information (PII) in the BCTS database consists of: Name, Address, City, State, ZIP, Day phone, Home Phone, Reciprocity state (if applicable), certification status and type, certification issue date and expiry date.

C. What is the legal authority?

- Surface Mining Control and Reclamation Act of 1977 (SMCRA), 30 U.S.C. 1201-1328
- Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons, as amended by Executive Order 13478
- Safe Explosives Act, Title XI, Subtitle C of Public Law 107-296, Delivery of Explosive Materials by Common or Contract Carrier, Homeland Security Act of 2002
- 18 U.S.C. § 842, § 843
- 30 CFR, Subchapter G, 750.19, Subchapter K, Part 816, Sections, 816.61, 817.61, Subchapter M, Part 850, Subchapter T, Part 900, Part 910, Part 912, Part 921, Part 922, Part 933, Part 937, Part 939, Part 941, Part 942, Part 947, Part 955

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*

This PIA is being completed to update an existing program/system under periodic review.

E. Is this information system registered in CSAM?

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

☒ No

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

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

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

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

INTERIOR/OSM-12, Blaster Certification – 64 FR 17413 (April 9, 1999); modification published 73 FR 45244 (August 4, 2008) and 86 FR 50156 (September 7, 2021). The INTERIOR/OSM-12 SORN is currently under revision.

Department of the Interior (DOI) SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☒ Yes: *Describe*

OSMRE Form 74, Application for an OSM Blaster Certificate, OMB Control No. 1029-0083, 30 CFR 955 - Certification of Blasters in Federal Program States and on Indian Lands; Expiration Date: 3/31/2024

☐ No

Section 2. Summary of System Data

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

☒ Name
☒ Gender
☒ Birth Date
☒ Education Information
☒ Social Security Number (SSN)
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

PII is collected from individuals through the OSMRE-74 form. Limited information is entered into the BCTS (an electronic database) that tracks the processing of the form, including Name, Address, City, State, ZIP, Day phone, Home Phone, Reciprocity state (if applicable), certification status and type, certification issue date and expiry date. SSNs are collected to verify an individual's identification; however, it is not included in the BCTS. A username and password are required to access the BCTS by authorized OSMRE personnel and can only be accessed via the OSMRE GSS network.

The OSMRE-74 form collects the following PII on individuals: Name, Mailing address, home and work telephone numbers, SSN (voluntary), sex, hair color, height, weight, and eye color in addition to work history and employment information. Education and training related to blasting and explosives and any currently held licenses or certificates relating to blasting or explosives.

An SSN is voluntarily requested during the application process. It is requested under the authority of Executive Order 9397 to uniquely identify a particular applicant record from those of other applicants who may have the same name. As allowed by law or Presidential directive, the SSN may be used to seek information about the applicant from employers, schools, banks, or from any other source provided on the OSM-74 form.

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

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ DOI records
☐ Third party source

☐ State agency
☐ Other: *Describe*

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

☒ Paper Format
☒ Email
☐ Face-to-Face Contact
☐ Web site
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems: *Describe*
☐ Other: *Describe*

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

The PII collected will be used to ensure and certify that all blasting operations are conducted by trained and competent persons under sections 515(b)(15)(D) and 719 of the Surface Mining Control and Reclamation Act of 1977.

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.*

Information is shared with authorized users and is used by the BCP, in OSMRE to evaluate and certify individuals as blasters. The BCTS is further utilized by OSMRE Reclamation Specialist to verify blaster status.

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

To appropriate DOI Bureaus/Offices responsible for obtaining information relevant to a Federal blaster for investigating, prosecuting, enforcing or implementing a statue, rule, regulation or order, as required.

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

Information may be directly shared with the Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, and other appropriate Federal agencies responsible for obtaining information relevant to a Federal blaster for investigating, prosecuting, enforcing or implementing a statue, rule, regulation or order, as required. This information is generally provided by the applicant as part of the blaster certification record.

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

To appropriate Tribal, State or Local agencies responsible for obtaining information relevant to a Federal blaster for investigating, prosecuting, enforcing or implementing a statue, rule, regulation or order, as required.

☐ 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.*

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.*

All information provided by individuals is voluntary as a condition of obtaining Federal blaster certification to conduct blasting operations in any Federal Program State or on Indian lands under Federal jurisdiction. Failure to provide the requested information would prevent the individual from receiving blaster certification rendering them unable to perform blasting operations in any Federal Program State or on Indian lands under Federal jurisdiction.

Not providing the requested information will impede the individual's registration as a Certified Blaster. Users who choose not to provide the required information will not be granted Certified Blaster certification.

☐ 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.*

A Privacy Act statement is provided for on the OSMRE-74, "APPLICATION FOR AN OSMRE BLASTER CERTIFICATE" form. The Privacy Act statement is under revision to ensure it meets the requirements of the Privacy Act and OMB Circular A-108.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment (PIA) and the published INTERIOR/OSM-12, SORN, (currently in revision).

☐ 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.).

Information is retrieved by OSMRE Blaster Certificate number, Certificate status, first and/or last name, Certificate type, and Residence state. Information can only viewed by authorized OSMRE personnel.

I. Will reports be produced on individuals?

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

The OSMRE Blaster Program generates reports of monthly of 90-day expirations for notification purposes to Blasters; Yearly reports to evaluate manpower needs for administrative purposes; and bi-annual reports to assist in cost recovery.

☐ No

Section 3. Attributes of System Data

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

Information is provided directly from the user, and it is their responsibility to provide accurate data. Verification is done through the application process; inaccurate information is referred back to the applicant to resolve any discrepancies or errors.

B. How will data be checked for completeness?

Information is provided directly from the user, and it is their responsibility to provide accurate data. Verification is done through the application process, missing or incomplete applications are referred to the applicant for completion.

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

Recertification of the blaster certificate and re-verification of the data are done triennially. Any changes or updates are resolved with the applicant to ensure the data is current.

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

Records in this system are maintained and disposed of in accordance with OSMRE Records Schedule N1-471-89-1, Item 201-13 – Blaster Certification Files. The disposition for these records is temporary and the records are cut-off upon expiration of certification or recertification. Records are destroyed two (2) years after cut-off.

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

Approved destruction methods for temporary records that have met their retention period include shredding or pulping paper records and erasing or degaussing electronic records in accordance with Departmental policy and NARA guidelines.

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

There is a privacy risk to individuals due to the variety of PII data that is collected. This risk is mitigated by a combination of technical, physical, and administrative controls. Applications and supporting data are keep in locked files cabinets in locked offices in OSMRE federal office buildings. Data collected is restricted to blaster certification applicants who are requesting certifications.

For information held electronically, there is a privacy risk to individuals that is mitigated by the security and privacy controls implemented to safeguard privacy and the limited collection of PII from individuals. As a part of the OSMRE GSS, the controls implemented protect data and substantially lower privacy risks. PII maintained in the BCTS is constrained to Name, Address, City, State, ZIP, Day phone, Home Phone, Reciprocity state, certification status and type, certification issue date and expiry date of applicants. Additionally, username, password, and official email address that are required to create and manage user accounts for authorized OSMRE personnel. OSMRE complies with DOI, NIST, and other Federal requirements for data security as part of a formal program of assessment and authorization, and Continuous Diagnostics and Mitigation (CDM) monitoring. Scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any network equipment. The use of OSMRE IT systems is conducted in accordance with the appropriate OSMRE and DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail includes the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are available and any suspected attempts of unauthorized access or scanning of the system are reported immediately to OSMRE IT Security and the DOI Office of the Chief Information Officer.

There is a risk of unauthorized access, use or disclosure of the records in the program. These risks are mitigated by safeguards including access restrictions based on least privilege, use of username and password, role-based training, and other controls to ensure the confidentiality, integrity, and availability of the records. The authorized personnel and system administrator's complete privacy, security, records, Section 508, Paperwork Reduction Act, and Controlled

Unclassified Information awareness training along with privacy and security role-based training on an annual basis. Access to records in the system is limited to authorized personnel whose official duties require such access. Electronic data is protected through user identification, encrypted passwords, database permissions and software controls. All data, including PII, delivered to and from an individual's web browser is encrypted using approved federal encryption protocols that meet National Institute of Standards and Technology (NIST) standards. These security measures establish different degrees of access for different types of users. Use of the system requires Multi-Factor Authentication, at the point of entry as another security control to mitigate the risk of unauthorized access, use or disclosure of the records in the system. The Privacy Act statement and continuous system monitoring notices are posted prominently.

There is a risk that users may not receive adequate notice of the purpose and uses of their information. This risk is mitigated by the notice provided in the Privacy Act statement included in the OSM-74 form and via the published INTERIOR/OSM-12 Blaster Certification SORN, and this PIA. Users may update their account information by contacting the Blaster certification program to make corrections. Access to data collected, stored, and utilized is limited to system developers and administrators, and authorized program officials. Data shared outside of the system will be limited to derived summary reports that do not contain PII.

There is a risk that records may be maintaining longer than authorized or necessary to meet a business need. Records are maintained in accordance with a NARA approved schedule. Once the retention period is deemed to be over, the records are destroyed in accordance with approved methods as outlined in DOI policy and the applicable records schedule.

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 information is used to efficiently manage the certification of applicants as Federal blasters in compliance with SMCRA and related regulations.

☐ 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?

N/A - The system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

OSMRE Blaster program coordinators involved in the certification of blasters and OSMRE Reclamation Specialists responsible for verifying that blasting operations are conducted by certified blasters during routine inspections and are able to access the BCTS.

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

Information Owner/Steward grants access in accordance with mission requirements utilizing the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following OMB, DHS and DOI policies, directives, and memorandums.

Access is restricted to the OSMRE Blaster program. Current DOI Rules of Behavior (RoB) apply to access and use of data.

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?*

☒ 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*

☒ No

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

The system does not actively monitor portal users and is not programmed to do so. Audit logs are maintained in the system and track login attempts and errors. Audit log records username, date/time, actions. Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and timestamp) for auditing purposes.

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

Access is only provided to authorized personnel and is applied on the principle of least privilege. Audit features track user activity and record all changes. In addition, continuous monitoring along with routine credentialed vulnerability scans are performed to identify viable weaknesses in the environment.

An audit trail of activity sufficient to reconstruct security-relevant events is available. Audit trails include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed as required, and any suspected attempts of unauthorized access or scanning of the system is reported immediately to OSMRE IT Security. Access to administrative functions is strictly controlled.

All OSMRE personnel must complete IT security, records, and privacy awareness training and sign DOI's RoB before being granted access to any OSMRE system during the initial on-boarding process, and at least annually thereafter. All users must annually agree to the DOI RoB.

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 Blaster Certification Program Coordinator serves as the Blaster Certification Program manager and BCTS system owner and is the official responsible for the oversight and management of security controls and the protection of information processed and stored in the application. The Program Coordinator, Information System Security Officer (ISSO), Privacy Act System Manager, and the OSMRE Associate Privacy Officer (APO) share the responsibility of protecting the privacy rights of the public and employees. Privacy Act complaints and requests for redress will be handled jointly between these entities.

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

The Blaster Certification Program Coordinator is responsible for oversight and management of the Blaster Certification Program and BCTS security and privacy controls, and for ensuring to the greatest possible extent that OSMRE and DOI agency data is properly managed and that all access to data has been granted in a secure and auditable manner. They are also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to the OSMRE APO and the OSMRE Incident Response Team in accordance with the DOI Privacy Breach Response Plan and the OSMRE Incident Response Plan.

All employees and contractors are required to report any potential loss or compromise to the Blaster Certification Program Coordinator, ISSO and the OSMRE APO in accordance with the DOI Privacy Breach Response Plan.