U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form 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 our Privacy Office Support Request Page. For further guidance, consult the DOI PIA Guide.

System Information

System or Project Name:	Borealis Stakeholder Relationship Management (SRM) Tool
System or Project Acronym:	**Borealis SRM**
Date submitted for review:	April 13, 2026
System Operational Status:	Implementation

Point of Contact

Name:	Laura Mansfield
Title:	Social Scientist
Office:	Office of Environmental Programs, Division of Environmental Assessment
Phone:	571-567-1194
E-mail:	laura.mansfield@boem.gov

Section 1: System Overview

1. What triggered this PIA? (Check one)

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

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

The purpose of the Borealis Stakeholder Relationship Management (SRM) Tool is to enable the Bureau of Ocean Energy Management (BOEM) and the Bureau of Safety and Environmental Enforcement (BSEE) to capture, manage, and integrate communications with community stakeholders in a centralized system. The tool supports stakeholder engagement by documenting communications received through email, telephone calls, stakeholder engagement events (such as National Environmental Policy Act (NEPA) public meetings), and public comments or other submissions related to environmental reviews, leasing decisions, and other Bureau activities.

By maintaining a centralized history of stakeholder interactions, the Borealis SRM Tool supports consistent stakeholder engagement, improves coordination across the Bureaus, and provides a comprehensive record of communications that inform or influence Bureau policy, regulatory actions, environmental reviews, and operational decisions.

This PIA covers the initial implementation of the Borealis Stakeholder Relationship Management (SRM) Tool for BOEM and BSEE. Any future expansion of the system to additional DOI bureaus or offices will be evaluated through the DOI Privacy Program to determine whether updates to this PIA or other privacy documentation are required. 3

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.

The Borealis SRM Tool is currently in implementation and has not yet been registered in BisonGRC. The system will be registered in BisonGRC as part of the applicable DOI cybersecurity review and authorization process.

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

These authorities support BOEM and BSEE public participation, environmental review, consultation, and stakeholder-engagement activities for which Borealis maintains records.

The Privacy Act of 1974 governs DOI's maintenance, use, disclosure, access, and safeguarding of records about individuals maintained in systems of records. Applicable System of Records Notices provide public notice of DOI's Privacy Act recordkeeping practices; they do not independently establish the underlying program authority for collecting stakeholder information.

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

Borealis maintains records about individuals and permits retrieval by personal identifiers, including name, email address, Tribal affiliation, organization, and other stakeholder attributes. Privacy Act System of Records Notice coverage is therefore required.

INTERIOR/DOI-21, eRulemaking Program, 85 FR 33701 (June 2, 2020), applies to rulemaking documents, public comments, and supporting materials maintained in Borealis that fall within the scope of the DOI eRulemaking Program.

Borealis also maintains stakeholder engagement, consultation, contact, and communication records that extend beyond the eRulemaking records described in INTERIOR/DOI-21. The Department Privacy Office must complete the SORN coverage determination for those additional Borealis records and identify the applicable published SORN coverage before this section is finalized.

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

Reduction Act?

☐ Yes
☒ No

Borealis supports multiple public and stakeholder engagement activities. PRA applicability is determined for the underlying information collection rather than by the fact that the information is subsequently maintained in Borealis.

Public comments submitted through rulemaking or other processes may fall within applicable PRA exemptions, existing OMB approvals, or other authorized collection mechanisms. BOEM and BSEE will coordinate with the responsible PRA official to ensure that each applicable public collection is covered by the appropriate PRA determination before use.

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

None

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

Borealis also maintains user identifiers and user-linked audit information associated with authorized access, record activity, exports, and administrative actions.

Tribal affiliation, employment or professional affiliation information may be collected.

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

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

☒ Local Agency ☒ Other: *Describe Below*

Information may also be received from nonprofit organizations and environmental organizations that participate in stakeholder engagement or consultation activities.

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

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

Information is entered into Borealis from stakeholder communications received through email, telephone, in-person meetings, paper records, websites, and public-engagement processes.

Public comments originating in Regulations.gov and Tribal contact information originating from DOI/BIA records may also be entered or imported into Borealis. The system documentation will identify whether those transfers occur through manual entry, file import, or an automated system interface.

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

The PII collected is used to identify individuals participating in public and tribal engagement activities, document communications with the government, maintain stakeholder engagement records, facilitate government-to-government consultation and public participation processes, and support informed decision-making related to environmental reviews and other official bureau activities.

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

Borealis limits stakeholder information to the identity, contact, organizational or Tribal affiliation, communication history, and engagement information necessary to support authorized BOEM and BSEE stakeholder-engagement and consultation activities.

Users are expected to enter only information relevant to the applicable engagement, consultation, environmental-review, or other authorized Bureau activity and to avoid entering unrelated personal information.

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.

Information may be shared across BOEM, BSEE, or with other Federal agencies when they are engaged in the same rulemaking, public consultation, or program activities involving the same stakeholders or Tribes, and the sharing is necessary to support those decisions or activities consistent with INTERIOR/DOI-21.
Contractors or fellows acting on behalf of the Department may be authorized to update the stakeholder database or use the information to support public comment processing, reporting, or other official program activities, consistent with their assigned responsibilities and applicable privacy requirements.

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

While information may be shared with other Federal agencies when permitted under INTERIOR/DOI-21—specifically when agencies are engaged in the same program, regulatory, or consultation activities involving the same stakeholders or Tribes such sharing occurs under the Privacy Act and published routine uses, not through a formal interagency agreement. If future program needs require structured, recurring information exchange, an appropriate MOU, MOA, or ISA would be established at that time in accordance with DOI policy.

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 generally choose whether to submit public comments, participate in stakeholder-engagement activities, or provide optional contact information. The applicable engagement process identifies any information required for participation.

Borealis also maintains official stakeholder and Tribal contact information used to support BOEM and BSEE engagement and consultation activities. Government-to-government Tribal consultation is conducted as an official relationship with Tribal governments and is not characterized as individual consent to DOI's maintenance of consultation records.

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

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

Notice is provided through the applicable public-comment, consultation, meeting, email, website, or other engagement process through which information is originally collected.

Additional transparency regarding Borealis is provided through this PIA and the applicable published System of Records Notice or Notices.

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

Records may be retrieved by authorized users using an individual's name, organization name, Tribal affiliation, email address, or other stakeholder attributes, as appropriate for their official duties. Authorized users may also retrieve records through other system features, such as communication history and engagement records, based on their assigned permissions and business needs.l

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

Reports may include names and contact information, as appropriate. Access to reports is limited to authorized users with an official need to know. Reports are provided to decision-makers supporting stakeholder engagement or tribal consultation activities to facilitate communication with stakeholders and Tribes. Information contained in the reports supports rulemaking, consultation requirements, environmental analyses, and other authorized policies or operational decision-making related to the applicable program or activity.

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

Individuals providing comments are responsible for providing accurate contact information at the time of submission. Contact information obtained from external sources, such as the Bureau of Indian Affairs' list of Federally Recognized Tribes, is verified and updated, as appropriate, during communications with the applicable Tribe.

Section 4: Data Management and Retention

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

Borealis contains multiple categories of records that may be subject to different approved disposition authorities.

BOEM environmental-coordination records covered by BOEM Bucket Schedule #4, including Schedule 4D(3) and Schedule 4E(2), are retained for 25 years in accordance with those approved schedules.

BOEM/BSEE stakeholder profiles, consultation records, public-comment records, correspondence, reports, AI-generated content retained for official use, audit logs, and other Borealis records will be retained and disposed of under the NARA-approved disposition authority applicable to the respective record series.

The responsible Records Officer will validate the applicable schedule coverage and identify the recordkeeping copy for each material Borealis record category before automated disposition is implemented.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?
Tribal liaisons and engagement staff will review data entries and update information, as needed, based on ongoing communications with stakeholders and Tribes. A Standard Operating Procedure (SOP) will be developed during implementation of Borealis to provide consistent guidance for completing stakeholder profiles. Each liaison is responsible for ensuring the information they enter is accurate and complete.

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

☒ Yes
☐ No

Only authorized users with a software license have access to the system. User activity is monitored, and system administrators oversee the system, manage user access, and can restore or remove user access when appropriate. Monitoring includes changes to organization and individual profiles, as well as records of stakeholder communications.

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?

The Borealis Stakeholder Relationship Management (SRM) Tool supports BOEM's responsibilities by consolidating public comments and related stakeholder communications into a single, centrally managed environment. Because individuals often include personally identifiable information (PII) when submitting public comments, the use of Borealis introduces privacy considerations across every stage of the information lifecycle. These risks are identified and addressed through safeguards documented in the system's Privacy Impact Assessment, along with DOI privacy and security policies.

During the collection phase, the primary privacy risk arises from individuals voluntarily submitting more information than BOEM requires to fulfill its statutory responsibilities. Public commenters may include contact details or other personal information that is not necessary for BOEM to evaluate their input. To mitigate this, BOEM provides clear instructions that limit what the public is asked to provide, and privacy notices inform individuals of how their information will be used. Borealis itself is configured to collect only the minimum PII required for stakeholder engagement and administrative recordkeeping.

Once information enters the system, privacy risks shift toward use of the data. Unauthorized access or use of PII for purposes beyond the scope of BOEM's mission could undermine individual privacy and violate federal requirements. Borealis mitigates these risks by restricting access to authorized BOEM and BSEE personnel who need the information to carry out their duties. Role-based access controls and least-privilege principles limit the ability to view or manipulate PII, ensuring it is used only for legitimate and documented program needs.
During the retention stage, the risk lies in keeping PII longer than necessary or maintaining inconsistent data sets across different systems. BOEM mitigates this through alignment with DOI-approved records schedules and NARA requirements. The Borealis PIA stipulates that stakeholder communication records, including public

comments, must follow applicable retention requirements. Regular reviews help verify that the system's retention practices remain accurate and compliant.

The disclosure phase presents its own risks, particularly because public comments may become part of the administrative record and be subject to public release under the National Environmental Policy Act (NEPA) or the Freedom of Information Act (FOIA). Without careful review, personal information unintentionally included in a comment could be disclosed publicly. To address this, BOEM conducts PII review and redaction, when necessary, before making comments publicly accessible. Any sharing of information with external parties such as contractors or partner agencies is tightly controlled and must comply with the Privacy Act, routine use provisions, and DOI data-sharing requirements.

Security safeguards apply throughout the lifecycle, reducing risks associated with storage and protection of PII. Unauthorized access, data compromise, or insider threats are mitigated through DOI's baseline security controls, including authentication, encryption, auditing, and continuous monitoring of the Borealis environment. Users with access to the system must complete annual privacy and security training, reinforcing their responsibilities for safeguarding PII.

Finally, at the disposal stage, the principal risk is the improper destruction of records containing PII, which could leave residual data vulnerable to misuse. Borealis follows DOI's approved disposition procedures, ensuring that records are securely destroyed once they meet their retention period. Disposal actions are logged to ensure accountability and traceability.

Through these combined measures, data minimization, transparency at collection, strict access controls, adherence to record schedules, controlled disclosures, strong security protections, and compliant disposal practices BOEM mitigates the privacy risks associated with collecting, using, retaining, and disclosing PII within Borealis during the consolidation of public comments.

Safeguards to mitigate privacy risks include having a limited number of authorized users, developing clear standard operating procedures for collection, use, retention and disclosure of PII, and holding annual training for authorized users to review and update the standard operating 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

Borealis generates derived information through AI-assisted functions, including summarization, translation, writing assistance, insight generation, and reporting.

These outputs are based on information already available within the authorized user's Borealis environment and are intended to assist staff in reviewing and working with stakeholder information. AI-generated outputs are subject to human review before official reliance.

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

☒ Yes: Provide explanation below

☐ No

AI-generated outputs may be stored in designated fields within Borealis. Content is identified as AI-generated and requires authorized user review before it is incorporated into standard or official system fields or relied upon for official purposes.

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

☐ Yes: *Provide explanation below*
☒ No

Borealis does not independently make eligibility, legal, financial, employment, regulatory, or other consequential determinations about individuals. AI-generated information may assist staff in reviewing stakeholder communications, but authorized personnel remain responsible for the underlying analysis and any official decision.

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

AI-generated summaries, translations, insights, reports, and other outputs are reviewed by authorized users against the underlying source information before being relied upon for official purposes. Users are responsible for correcting inaccurate, incomplete, misleading, or contextually inappropriate AI-generated content before incorporating it into an official record or decision process.

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?

Borealis does not develop, train, or fine-tune the underlying commercial AI models.

Authorized users review AI-generated summaries, translations, writing assistance, insights, and reports against the underlying source information before relying on those outputs for official purposes. Identified performance or accuracy issues may be documented and reported through the applicable system support process.

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

☐ Yes
☒ No

Borealis does not independently make AI-based decisions affecting individuals. AI capabilities provide assistive outputs such as summaries, translations, writing assistance, insights, and reports that may support staff review

of stakeholder information. Authorized personnel retain responsibility for validating the source information and making all official decisions.

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

☒ Yes
☐ No

The AI capabilities within Borealis are limited to assistive functions and are not used to make or support automated decisions that affect individuals or determine eligibility, rights, or benefits. AI-generated outputs are advisory only and are reviewed by authorized users, who exercise professional judgment before using the information for official business purposes. This human oversight helps minimize the risk of bias, inaccuracies, or unintended consequences.

Borealis implements multiple administrative and technical safeguards to support the responsible use of AI, including:

- Limiting AI capabilities to assistive use cases that support, rather than replace, human decision-making.
- Requiring human review and validation of AI-generated content before it is used for official business purposes.
- Enforcing the principle of least privilege through role-based access controls (RBAC).
- Restricting the data provided to AI services to the minimum necessary to perform the requested function.
- Utilizing built-in safety features and content filtering provided by Azure OpenAI.
- Encrypting data in transit and at rest.
- Restricting AI service access to secure backend APIs and protecting API keys and secrets.
- Preventing direct end-user access to AI models or training environments.
- Maintaining audit logs to provide traceability for AI-generated content retained within the system.
- Implementing security and privacy controls consistent with ISO 27001 and applicable DOI security requirements.

These safeguards help ensure AI capabilities are used responsibly, transparently, and under appropriate human oversight, reducing the potential for bias or unintended consequences.

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

☒ Yes
☐ No

Borealis does not develop, train, or retrain its own AI models. AI capabilities are provided through commercially available services, such as Azure OpenAI, which are maintained and updated by the service provider. As Borealis software is updated, AI capabilities and configurations are reviewed to ensure they continue to support authorized business functions, operate as intended, and remain consistent with DOI security, privacy, and AI governance requirements. Operational performance is also monitored through user feedback, quality assurance activities, audit logging, and issue tracking. When necessary, AI features may be modified, restricted, or disabled to maintain reliability and appropriate system performance.

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

☐ Yes
☒ No

Federated learning is not used by Borealis. The system does not develop or train AI models using customer data, nor does it perform distributed model training across decentralized devices or servers. AI capabilities are provided through commercially available services, and customer data is not used to train or fine-tune foundation models. Therefore, federated learning is not applicable to the Borealis AI implementation.

Section 7: Security and Access Controls

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

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

Access to data maintained within the Borealis platform is limited to authorized DOI personnel, including BOEM and BSEE users, designated system administrators, and authorized contractor personnel who require access to perform official duties. Access is determined, authorized, and restricted in accordance with DOI privacy and security policies and the principle of least privilege.

Periodic access is managed through the following controls:

- **Role-Based Access:** Users are assigned roles based on their job responsibilities, ensuring they can access only the information necessary to perform their official duties.
- **Need-to-Know:** Access is granted only to personnel whose responsibilities require interaction with stakeholder communication records or system administration functions.
- **Formal Authorization:** User accounts and access privileges are approved through DOI's established account management and governance processes before access is granted.
- **Periodic Access Reviews:** User access is reviewed periodically to verify that permission remains. appropriate and to promptly remove or modify access when job responsibilities change or employment ends.
- **Technical Security Controls:** Access is protected through DOI security controls, including user authentication, role-based access control (RBAC), logical access restrictions, audit logging, and continuous monitoring consistent with DOI security requirements.

These administrative and technical controls help ensure that project data, including any PII maintained within Borealis, is accessible only to authorized individuals with a legitimate business need

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

Borealis operates within the BOEM/BSEE Azure environment described in this PIA and uses approved cloud-based services to support system functionality.

The AI capabilities described in Section 6 include Azure OpenAI and AWS Translate. This section should be updated so the cloud-services description is consistent with the AI services identified elsewhere in the PIA.

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

The Borealis Stakeholder Relationship Management (SRM) Tool supports the monitoring and detection of unauthorized access, use, or attempted exfiltration of PII through a combination of application audit logging and DOI enterprise security monitoring capabilities.

- **Application Audit Logging:** Borealis records user activity, including login, record access, edits, exports, and other administrative actions. Audit logs capture the user ID, date and time of the activity, and the action performed. These logs are protected from unauthorized modification and may be integrated with DOI's enterprise monitoring environment through security telemetry or exported to the Security Information and Event Management (SIEM) platform using secure application programming interfaces (APIs).
- **DOI Enterprise Security Monitoring:** Audit logs and security events are monitored through DOI's Security Information and Event Management (SIEM) platform, where they are correlated with other enterprise security data to identify suspicious activity, including repeated failed login attempts, unusual access patterns, excessive record downloads, or other indicators of potential unauthorized access or data exfiltration.
- **Incident Detection and Response**: Security alerts are automatically generated and reviewed by DOI's Computer Incident Response Center (DOI-CIRC) and/or the BSEE Enterprise Security Team. Suspected security incidents involving PII are investigated and escalated to the appropriate System Owner, Information System Security Officer (ISSO), and Privacy Officer in accordance with the DOI Privacy Breach Response Plan and applicable Federal incident reporting requirements.
- **Log Review and Continuous Monitoring:** The ISSO and designated system administrators periodically review audit logs and security events, in addition to automated monitoring and alerting capabilities, to identify anomalous activity and support timely incident response.

These monitoring and auditing capabilities help ensure that unauthorized access, misuse, or attempted exfiltration of PII is promptly detected, investigated, and addressed in accordance with DOI security policy and the security controls defined in NIST Special Publication (SP) 800-53 Revision 5.

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 Borealis Stakeholder Relationship Management (SRM) Tool and DOI's Security Information and Event Management (SIEM) capabilities monitor user activity to protect system security, safeguard PII, support auditing, and meet Federal security requirements. The system does not track individuals beyond maintaining records necessary to support its authorized business functions.

Monitored Activities:

- User authentication, including successful and failed login attempts.

- Access to records containing PII.
- Creation, modification, deletion, and export of records.
- Administrative actions and changes to user accounts or permissions.
- Unusual access patterns or large-volume data exports that may indicate unauthorized activity.

Controls for Appropriate Use:

- Monitoring information is accessible only to authorized personnel, including the Information System Security Officer (ISSO), designated system administrators, and security personnel with an official need to know.
- Audit logs and security events are protected from unauthorized modification and are reviewed periodically to identify suspicious or unauthorized activity.
- Security events and anomalies are investigated and, when appropriate, escalated through DOI's Computer Incident Response Center (DOI-CIRC) in accordance with established incident response procedures.
- Users are notified through DOI Rules of Behavior, system security notices, and login banners that their activity may be monitored for authorized security, auditing, and compliance purposes.
- Monitoring information is used only for authorized operational, security, auditing, and incident response purposes and is protected in accordance with DOI privacy and security policies.

These controls help ensure that user activity monitoring is conducted only for legitimate security and operational purposes and is not used to monitor individuals for purposes unrelated to the system's authorized mission.

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

☒ Design
☒ Development
☒ Maintenance

The Borealis software vendor and BSEE contractor personnel support the Borealis Platform in the areas of design, development, and maintenance.

- **Design:** The Borealis vendor designs and enhances the application to support system functionality and business requirements.
- **Development:** The Borealis vendor develops the software, implements application updates, integrations, security enhancements, and new functionality as part of the established release cycle.
- **Maintenance:** BSEE contractors perform system administration, software updates, patch management, troubleshooting, and operational support. Certain maintenance activities are coordinated with Borealis support personnel when vendor assistance is required.

Contractors with access to the system or PII must comply with all applicable Federal and DOI privacy and security requirements. This includes completing required background investigations, signing the DOI Rules of Behavior, completing annual privacy and security awareness training, and accessing the system only as

authorized through role-based access controls and the principle of least privilege. Contractor activities are subject to audit logging, monitoring, and oversight to ensure compliance with DOI policies, contractual requirements, and applicable Federal laws and regulations.

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

Physical Controls

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

The Borealis Platform employs multiple layers of physical controls to protect facilities and infrastructure supporting the storage and processing of PII. Physical safeguards are provided through Microsoft Azure's FedRAMP Moderate authorized data centers and DOI facility security requirements.

Other Physical Controls: Visitor access is restricted to authorized personnel and requires identity verification, visitor logging, and escorted access. Microsoft Azure data centers also employ environmental safeguards, including fire detection and suppression systems, redundant power, and climate controls to protect information systems and support service availability.

Technical Controls

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

PII is protected through technical safeguards that comply with DOI security requirements and NIST Special Publication (SP) 800-53 Revision 5.

Other Technical Controls:

- Multi-factor authentication (MFA) is required for privileged and user accounts.
- Endpoint Detection and Response (EDR) and antivirus technologies help detect and prevent malicious code and malware.
- Cloud workload protection continuously monitors workloads for configuration vulnerabilities and malicious activity.
- Azure platform security provides encryption services, workload isolation, and host-level protections

through the Azure compute fabric and hypervisor architecture.
- Automatic session timeouts and user logoff after periods of inactivity reduce the risk of unauthorized access.

Administrative Controls

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

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

Individuals who wish to submit a Privacy Act complaint related to the Borealis system may do so via email at DOI_Privacy@ios.doi.gov or U.S. mail by sending a written complaint to: Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240.

All complaints are logged by the Departmental Privacy Office and reviewed to determine whether a potential violation of the Privacy Act has occurred. The Privacy Office coordinates with the Borealis System Owner and relevant bureau officials to gather necessary information, assess the concern, and take appropriate corrective action when warranted. Individuals receive a response consistent with DOI policy and federal privacy requirements, and issues involving potential unauthorized disclosures are further evaluated and handled in accordance with DOI's established privacy and incident response procedures.

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

Individuals may request access to their information through established DOI Privacy Act processes as documented in the DOI Privacy Act regulations (43 CFR Part 2, Subpart K). To obtain their records under the Privacy Act, individuals must submit a request to the DOI bureau that maintains the information (i.e., BOEM or BSEE), identifying the records sought and providing sufficient detail to enable a search, along with verification of identity such as a signed request, notarization, or submission under penalty of perjury. Individuals may submit their request via postal mail or electronically via the DOI Privacy Act Public Access Portal.

Before access is granted, DOI verifies the requester's identity to ensure that records are only released to the individual to whom they pertain. This may require confirming contact information, requesting additional documentation, and using approved identity verification procedures. Once identity is verified, the bureau searches for responsive records within the tool and DOI provides the individual with the accessible portions of their information, subject to applicable Privacy Act exemptions.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?
Privacy Act requests for correction must be submitted in writing to the System Manager identified in the applicable SORN, must be signed, and must meet requirements identified in the SORN and DOI Privacy Act regulations. System Managers may require additional information or proof of identity, including a notarized

statement or a statement signed under penalty of perjury affirming that the requester is the individual to whom the record pertains.

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 Project Lead is responsible for the day-to-day operational oversight of the Borealis Stakeholder Relationship Management (SRM) Tool and for ensuring that privacy and security controls are implemented and maintained. The Project Lead is also responsible for helping ensure that data is appropriately managed and that access is granted in a secure, authorized, and auditable manner.

The Information System Owner (ISO), Information System Security Officer (ISSO), System Administrators, and authorized users are responsible for promptly reporting any actual or suspected loss, compromise, unauthorized access, use, or disclosure of PII to the DOI Computer Incident Response Center (DOI-CIRC) in accordance with applicable Federal and DOI incident reporting requirements. These officials also coordinate with the Departmental Privacy Officer and other appropriate stakeholders to investigate incidents and implement corrective actions to mitigate risks to affected individuals, when appropriate.

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?

If a potential privacy breach involving unauthorized access, loss, or disclosure of PII is detected, users must immediately report the incident to the DOI Computer Incident Response Center (DOI-CIRC) in accordance with applicable DOI cybersecurity and privacy incident reporting requirements. DOI-CIRC initiates the Department's incident response process, and system administrators implement appropriate containment measures, such as restricting access to affected accounts or systems, isolating compromised components, and reviewing audit and authentication logs to prevent further unauthorized activity.

Following containment, the Departmental Privacy Office, in coordination with the System Owner, Information System Security Officer (ISSO), and other appropriate officials, conducts a privacy risk assessment to determine the scope of the incident, the types of PII involved, the number of individuals potentially affected, the likelihood of harm, and whether misuse of the information has occurred. Because Borealis supports stakeholder engagement activities, the assessment also considers whether stakeholder communications or contact information were improperly accessed or disclosed.

If the assessment determines that notification is appropriate, the Departmental Privacy Office coordinates notifications to affected individuals in accordance with DOI breach response procedures. Notifications generally describe the nature of the incident, the types of information involved, actions the Department has taken to mitigate the incident, and recommended steps individuals may take to protect themselves. The Departmental Privacy Office also determines whether additional mitigation measures, such as credit monitoring or other protective services, are warranted based on the circumstances of the incident.

When required, DOI reports the incident to appropriate Federal oversight agencies in accordance with applicable laws, regulations, and government-wide reporting requirements.

Following incident resolution, DOI-CIRC, the System Owner, the ISSO, and the Departmental Privacy Office conduct a post-incident review to identify root causes, evaluate the effectiveness of the response, implement corrective actions, and update security and privacy controls, policies, or procedures as appropriate to reduce the likelihood of future incidents.

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

Borealis will be reviewed annually through the applicable DOI Privacy Threshold Analysis process and when a material change to system functionality, PII, stakeholder populations, collection methods, sharing, retention, cloud services, AI capabilities, integrations, or operational use may affect privacy risk.

The PIA will be updated when a material change makes the current assessment inaccurate or incomplete. When no material privacy change has occurred, the PIA may be reaffirmed in accordance with DOI privacy procedures.