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: ServiceNow – BSEE Enterprise IT Service Desk
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE**)**
Date: December 5, 2023
Point of Contact
Name: Melissa Allen
Title: Associate Privacy Officer (Acting)
Email: privacy@bsee.gov
Phone: 571-474-7967
Address: 45600 Woodland Road, Mail Stop: VAE-TSD, Sterling, VA 20166

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

B. What is the purpose of the system?

The Bureau of Safety and Environmental Enforcement (BSEE), Technology Services Division (TSD), Enterprise Information Technology (IT) Service Desk (referred to as “Service Desk” hereafter) is responsible for IT service request management. The Service Desk serves as the single point of contact for logging, assigning, tracking, reporting, and resolving service requests for the employees and contractors of BSEE, the Bureau of Ocean Energy Management (BOEM), and the Office of Natural Resources Revenue (ONRR) (collectively referred to herein as internal customers), and authorized Industry, State, and Tribal users (referred to herein as external customers).

ServiceNow is a FedRAMP-certified cloud service provider solution that allows organizations to quickly build new apps directly into ServiceNow leveraging existing platform services, applications, and integrations to support IT service automation, resource management, and shared support services. This PIA describes TSD's use of ServiceNow to support IT service desk functions. The Service Desk serves as the single point of contact for logging, assigning, tracking, reporting, and resolving service requests from internal and external customers and separate monitoring systems. Service Desk personnel use ServiceNow to log tickets, classify tickets according to impact and urgency, assign tickets to appropriate groups, escalate incidents, and manage tickets through to resolution.

Several IT systems hosted on the BSEE Network are integrated with ServiceNow with data flowing unidirectionally to ServiceNow. Some of the systems are used by internal customers to initiate service tickets for software/hardware requests, the creation of events and invitations, requests for approval to use non-core software, and personnel exit requests for employees and contractors (i.e., ProvisioningWeb, ReservationWeb, Non-Core Software Request, and Exit Clearance System) while others are used by Service Desk staff (i.e., SolarWinds monitoring, Microsoft Active Directory (AD), and IBM Identity & Access Management (IAM)).

Separate monitoring systems send event information (e.g., malware event, server down, etc.) to ServiceNow, which is turned into a ticket. Internal Service Desk customers can initiate a Service Desk ticket through the self-service portal or by contacting the Service Desk by phone or email. If an internal customer submits a request online, the internal customer's information is automatically pre-populated based on the user's Personal Identity Verification (PIV) card profile from AD. The self-service portal also offers a chat interface to enhance communication between Service Desk personnel and customers. Once a customer initiates the chat function, the customer's name is pre-populated based on the user's PIV card profile. The customer can provide a short summary of the request in a free-text field before connecting with a Service Desk representative to obtain service support. Internal customers can also upload documents to assist with their request and view the status of their own tickets.

Once information is entered in ServiceNow through a reported monitoring event or a customer service request, a system-generated ticket with a unique ticket number is created and the ticket is classified based on priority. The Service Desk ticket is assigned to an appropriate IT Service Desk technician who is responsible for driving the ticket to completion. BSEE Enterprise IT Service Desk technicians can update the status of the service request ticket by entering work notes and other updates.

After the reported issue is resolved, the Service Desk technician marks the ticket as resolved and no further action is performed on the ticket. The ServiceNow application sends the customer a summary and a brief customer satisfaction survey. This survey is voluntary and helps TSD improve its operations. While the survey does not collect personally identifiable information

(PII), the survey is linked to the customer's Service Desk ticket number. Closed incidents are filtered out of view but will remain in ServiceNow for reference and reporting purposes. Closed incidents can be reopened if the customer or Service Desk technician reports that the service request was not sufficiently resolved.

A subset of external Service Desk customers (i.e., Industry, State, and Tribal Users) can initiate a single type of ticket known as the External Minerals Revenue Management Support System Application Request Form (EMARF) through a publicly available Web form hosted by ServiceNow. The Minerals Revenue Management Support System (MRMSS) is the ONRR mission-critical system for the collection and disbursement of revenues to States, Tribes, and other Federal agencies. Once an EMARF Web form is received, the external customer receives an email with a ticket number for future reference and the granting of access to MRMSS follows the normal ServiceNow work process. ONRR grants authorized State and Tribal users an AD account through ProvisioningWeb so these users can call or go into the ServiceNow self-service portal to request access to ONRR MRMSS applications to create and submit reporting data related to ONRR functions. However, external customers cannot access their own tickets in the self-service portal.

C. What is the legal authority?

BSEE is authorized to collect and maintain information for Service Desk functions under 5 U.S.C. 301 – Departmental Regulations, 3101, 5105–5115, 5501– 5516, 5701–5709; 31 U.S.C. 66a, 240– 243; 40 U.S.C. 483(b); 43 U.S.C. 1467; 44 U.S.C. 3101; Homeland Security Presidential Directive 12 (HSPD-12); and Executive Order 11807 – Occupational Safety and Health Programs for Federal Employees.

ONRR collects information through the EMARF Web form to facilitate access to MRMSS applications as authorized by the Federal Oil and Gas Royalty Management Act of 1982, 30 U.S.C. 1701–1759; 25 U.S.C. Chapter 12, addressing the lease, sale, or surrender of allotted or unallotted lands found at 25 U.S.C. 391–416j; 30 U.S.C. Chapter 3A, addressing leases and prospecting permits, found at 30 U.S.C. 181–196; and the Outer Continental Shelf Lands Act, 43 U.S.C. 1331–1356b.

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

E. Is this information system registered in the Governance, Risk, and Compliance platform?

☒ Yes: UII Code 10-000001311; BSEE ServiceNow System Security and Privacy Plan

☐ 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: INTERIOR/DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - 72 FR 11040 (March 12, 2007); modification published 86 FR 50156 (September 7, 2021) covers how DOI collects information from personnel in order to provide authorized individuals with access to DOI information technology resources.

INTERIOR/DOI-58, Employee Administrative Records - 64 FR 19384 (April 20, 1999); modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021) covers records involving the administrative or operational relationship between employees and the office in which they work.

INTERIOR/OS-30, Minerals Revenue Management Support System (MRMSS) - 81 FR 16207 (March 25, 2016); modification published 86 FR 50156 (September 7, 2021) covers records relating to the general administration of the MRMSS and records relating to minerals revenue asset management, compliance management, and financial management.

The SORNs may be accessed through the DOI-wide SORNs Web page.

☐ No

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

☐ Yes

☒ No

Section 2. Summary of System Data

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

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Disability Information
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☒ Other: Other PII collected from customers includes their non-sensitive business-related contact information and security questions and answers to verify a customer's identity. Typically, personal contact information is not collected. However, a customer may provide personal contact information as an alternative contact method in rare cases (e.g., if a customer is working remotely).

Regarding disability information, the system maintains a checkbox status for customers who self-report disabilities such as sight or hearing impairment. The Service Desk uses this information to better accommodate IT support for these individuals and comply with Section 508 of the Rehabilitation Act, as amended in 1998.

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: A supervisor or Contracting Officer's Representative may submit a service request on behalf of other employees and contractors.
☐ State agency
☒ Other: Industry, State, and Tribal customers who complete the EMARF Web form hosted by ServiceNow to acquire access to the ONRR MRMSS.

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: Data is pulled from AD twice a day to ensure customer data is accurate and current.

Internal customer-initiated processes from ProvisioningWeb, ReservationWeb, Exit Clearance, and Non-Core Software Request automatically push data into ServiceNow to fulfill service requests.

☒ Other: Internal customers may initiate a service request or ask a question via the chat function. They may also upload documents to assist with their request. The Service Desk uses the uploaded information only for reference purposes.

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

The Service Desk collects and uses different information about the IT system, software, technology, and customer to determine how to resolve an issue. Once the information is entered in ServiceNow, the system generates a ticket with a unique number and assigns it to the appropriate Service Desk personnel to handle. The Service Desk may use the following information to create a ticket:

- Full name or AD username
- Phone number (if applicable) and e-mail address
- Location of equipment
- IT Technician Assignment Group
- Configuration item (government asset name/computer name)
- Service Level due date
- Description of service request
- Relevant files such as screenshots or error logs (as attachments)
- Ticket number for an existing service request

A customer's username is used by the Service Desk to create accounts, assign permissions, and track security incidents. Security questions are used to verify a customer's identity.

AD and IAM information are contained within the system to streamline the incident reporting process and allow support technicians to easily follow up with customers who have open service requests.

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

☒ Within the Bureau/Office: The Service Desk will use PII and other information provided by internal and external customers to create network accounts, incident tickets, problem tickets, and service request tickets, as well as gather data on security incidents. The Service Desk will share collected information internally with personnel who have an official need-to-know. When supervisory approval is needed to complete a request for a BSEE customer, the Service Desk will notify the BSEE supervisor to act. BSEE customers can view and amend their service requests in the self-service portal.

☒ Other Bureaus/Offices: The Service Desk performs the same functions described above for BOEM and ONRR under a reimbursable service agreement. BOEM and ONRR customers can view and amend their service requests in the self-service portal. The Service Desk performs the same function with regard to Citrix application access for Bureau of Land Management (BLM) users/customers.

Tickets may involve security incidents that BSEE would report to the DOI Computer Incident Response Center (DOI-CIRC).

☒ Other Federal Agencies: Tickets may involve security incidents that BSEE would also report to the Department of Homeland Security Cybersecurity & Infrastructure Security Agency.

☒ Tribal, State or Local Agencies: Through ProvisioningWeb, ONRR grants authorized State and Tribal users an AD account. These users can call the Service Desk or use the ServiceNow self-service portal to request access to ONRR MRMSS applications to create and submit reporting data related to ONRR functions. These users can also contact the Service Desk to obtain information pertaining to their own requests.

☒ Contractor: The Service Desk and BSEE Enterprise IT are staffed by contractor personnel who are authorized to access information in accordance with the least privilege principle to carry out their duties for the U.S. Federal Government.

☒ Other Third Party Sources: ServiceNow stores encrypted information in a FedRAMP-certified cloud storage facility in the US.

Industry users can contact the Service Desk to obtain information pertaining to their own requests.

System records may be shared with oversight organizations during audits or reviews of security programs pursuant to Federal law and other requirements.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: Internal customers can choose to not provide their information to address their service request. However, failure to provide certain information (e.g., personal contact information if working remotely) may impede or delay Service Desk personnel from resolving their service request or issue.

External customers voluntarily complete the EMARF Web form to provide information to ONRR to facilitate their access to MRMSS applications. Failure to provide information may impede or delay ONRR personnel from resolving their service request or inquiry.

Each internal customer voluntarily provides minimum information and consents to rules of behavior before being granted access to the DOI computer network and information systems. Requesting access and using the services are voluntary. However, the employee information is required to create and activate user accounts to access the services. Not providing information will prevent the user from acquiring access to the network and information systems. Internal customers who have acquired an AD account through the employee onboarding process cannot decline the daily updates from AD and IAM into ServiceNow for Service Desk use.

☐ No

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: The EMARF Web form contains a Privacy Act Statement that provides individuals with notice of ONRR's authority to collect the information, purpose of the collection, routine uses of the information, and whether providing the information is voluntary and the consequences of failing to provide information.

☒ Privacy Notice: BSEE provides a general notice of the collection, intended use, and sharing of customer information through the publication of this PIA. Notice is also provided through the Enterprise Hosted Infrastructure PIA to cover the collection and use of AD information, as well as the applicable SORNS (INTERIOR/DOI-47, HSPD-12: Logical Security Files and INTERIOR/DOI-58, Employee Administrative Records). ONRR provides notice through the MRMSS PIA and INTERIOR/OS-30 Minerals Revenue Management Support System (MRMSS). The DOI, BSEE, and ONRR PIAs may be accessed for review through the DOI PIA Web page. The DOI and ONRR SORNs may be accessed for review through the DOI-wide SORNs Web page.

Service Desk technicians provide a verbal notice to customers who submit a request via phone concerning the use of their data during the identity verification process.

☒ Other: Customers on a government computer and signed into an AD-authenticated account view a privacy warning banner at the time of logging onto the government network.

Industry, State, and Tribal customers completing the EMARF Web form also have the opportunity to review a privacy warning banner on the form before submitting it.

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 incident identification number, customer name, change request number, reference number, automatic reports, and/or customer email address.

I. Will reports be produced on individuals?

☒ Yes: Service-level records by Service Desk personnel are produced to track performance. Reports will be produced on customer service requests. The Service Desk can view the incident/service request ticket history for customers when they call for assistance, as well as the details of any assigned government-furnished computer equipment.

☐ No

Section 3. Attributes of System Data

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

Service Now – BSEE Enterprise IT Service Desk prepopulates the information of customers from their AD account for identification and authentication. The accuracy of this data is ensured by the source system.

If an internal or external customer contacts the Service Desk, the Service Desk technician will confirm the customer's identity by mapping the identity information provided by the customer to the customer's information in AD. Other information provided to the Service Desk by customers is assumed to be accurate at the time of collection. It is the responsibility of customers to provide accurate and relevant information to the Service Desk.

Information in EMARF is collected directly from the Industry, State, and Tribal customers and assumed to be accurate at the time of collection. It is the responsibility of Industry, State, and Tribal users to provide accurate information.

B. How will data be checked for completeness?

For internal customers, data is checked for completeness by the employee or authorized user providing the data and customer identity is cross-referenced with existing DOI databases (e.g., AD).

For external customers submitting an EMARF Web form, data is collected directly from the customer and is presumed to be complete at the time of submission.

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

Service Desk technicians verify information when customers call the Service Desk to submit a service request. Data stored in ServiceNow is updated annually as required by an annual ongoing authorization, pulled twice daily from AD, and pushed once daily from IAM.

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

The records in BSEE ServiceNow – BSEE Enterprise IT Desk are covered by DOI Records Schedule DAA-0048-2013-0001-0013, System Maintenance and Use Files. Records are cut off when superseded or obsolete then destroyed no later than 3 years after cutoff. BSEE plans to destroy service request tickets, including the attachment containing PII, three years after the ticket is resolved, or when no longer needed for business use (i.e., ongoing investigations), whichever is appropriate. BSEE maintains historical service request tickets to analyze recurring problems and analyze records.

ONRR records related to EMARF fall under the bureau's Admin schedule and are retained for three years.

BSEE and ONRR may preserve records longer if required to do so to comply with a litigation hold.

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

Records management policies and procedures govern disposal of information. The BSEE Exit Clearance process documents the steps and procedures used to remove or archive information when employees and contractors leave the agency. Procedures are also documented in section MP-06 of the Media Protection (MP) Standard Operating Procedure. The approved disposition methods include shredding or pulping for paper records and purging, degaussing, or erasing for electronic records in accordance with NARA Guidelines and Departmental policy.

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.

The potential privacy risks created by the Service Desk's use of ServiceNow to take care of IT service management requests include lack of notice, collection of more information than is necessary, collection of inaccurate information, potential Web form vulnerabilities, unauthorized disclosure of information, unauthorized access, insider threats, inappropriate use of information, inappropriate storage of information, and retention of data for longer than necessary to accomplish the purpose for which the information was originally collected.

There is a risk that individuals may not be aware that their information is contained within ServiceNow or how it will be used by the Service Desk. This risk is partially mitigated through the notice provided by this PIA and the corresponding source system PIAs and SORNs for ingested data (i.e., the Enterprise Hosted Infrastructure PIA, INTERIOR/DOI-47, HSPD-12: Logical Security Files, and INTERIOR/DOI-58, Employee Administrative Records). Customers on a government computer and signed into an AD-authenticated account view a privacy warning banner at the time of logging onto the government network. Internal customers who submit information through the self-service portal will have notice of the collection and use of their information at the time of collection. Service Desk technicians will provide a verbal notice to customers who submit requests via phone. For the EMARF Web form, ONRR provides notice through the MRMSS PIA and INTERIOR/OS-30 Minerals Revenue Management Support System (MRMSS). The EMARF Web form also contains a privacy warning banner and a Privacy Act Statement that provides individuals with notice of ONRR's authority to collect the information, purpose of the collection, routine uses of the information, whether providing the information is voluntary, and the consequences of failing to provide information. The DOI, BSEE, and ONRR PIAs may be accessed for review through the DOI PIA Web page. The DOI and ONRR SORNs may be accessed for review through the DOI-wide SORNs Web page.

There is a risk that information will be included in the system that is not necessary or relevant to accomplish the system's purpose. This risk is partially mitigated. The Service Desk requests only the minimum amount of information necessary from customers to create a service request ticket. Internal customers who have access to the self-service portal may upload additional supporting documents when creating a service request ticket. Although ServiceNow has technical safeguards in place to limit the types and sizes of the uploaded files, there are no technical restrictions on the type of PII or sensitive PII the uploaded documents may contain. Also, there is no disclaimer in the self-service portal that reminds internal customers to limit the information they include in a service request to only what is required. Service Desk technicians are trained to report any unnecessary PII that users provide via the self-service portal, at which point the spillage of PII will be investigated and processed as a potential privacy breach. The PII is also scrubbed from ServiceNow. If customers must input PII to fulfill a service request, only approved personnel who have an official need-to-know and ServiceNow administrators can view the information. ONRR uses the EMARF Web form to collect the minimum information necessary to facilitate MRMSS access for Industry, State, and Tribal users. These users agree not to disclose information covered by the Privacy Act or Trade Secrets Act to unauthorized individuals.

There is a risk that information will be inaccurately entered into ServiceNow. The ServiceNow – BSEE Enterprise IT Service Desk self-service prepopulates the information of customers from their AD account for identification and authentication. The accuracy of this data is ensured by the source system. If an internal or external customer contacts the Service Desk by phone, the Service Desk technician will ensure that the information entered into ServiceNow is attributed to the appropriate individual by asking a series of questions to confirm the individual's identity. Other information provided to the Service Desk by customers is assumed to be accurate at the time of collection. It is the responsibility of internal customers to provide accurate and relevant information to the Service Desk whether initiating a service ticket by phone or through the self- service portal – including but not limited to requests initiated on behalf of another employee or contractor. ONRR collects information through the EMARF Web form directly from the Industry, State, and Tribal customers and assumed to be accurate at the time of collection. It is the responsibility of Industry, State, and Tribal users to provide accurate information when completing an EMARF Web form or contacting the Service Desk by phone.

Use of the EMARF Web form could introduce unknown vulnerabilities to form data and/or cause denial of service. This Web form is public internet-facing and does not require authentication for submission. However, there are internal compensating security controls such as encryption to mitigate these risks in accordance with OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, and OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services. To further mitigate risk, authentication to the MRMSS system requires validation and approval by ONRR before access is granted.

The Service Desk mitigates the risks posed by unauthorized access, insider threats, and the inappropriate use of information through the implementation of appropriate administrative and technical safeguards to protect the system and data. The ServiceNow software is made available to multiple BSEE program offices on individual server sites that are walled off from any other site's content, thus ensuring that one program office does not have access to another's information or data without authorization and for a legitimate business purpose. ServiceNow pulls customer contact information from AD, which facilitates single sign-on and ensures that user data is accurate and current. System administrators set user roles to ensure appropriate access and use by authorized personnel with a valid need-to-know to perform official duties. All system user activity is monitored and logged to ensure only appropriate use of the system and data. Employees and contractors are also required to annually complete Information Management and Technology (IMT) Awareness Training (which includes modules on privacy and security awareness, Controlled Unclassified Information, and the Paperwork Reduction Act) and the Information Systems Security Rules of Behavior Acknowledgement. Employees and contractors with significant privacy and/or security responsibilities must complete role-based privacy and/or security training before acquiring access and annually thereafter.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or the vendor may not handle or store information appropriately according to DOI policy. The ServiceNow – BSEE Enterprise IT Service Desk software is provided and hosted by a FedRAMP-certified service provider and has met all requirements for information categorized as Moderate in accordance with FISMA. The system requires strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system at the Moderate level. The cloud service provider is subject to all the Federal legal and policy requirements for safeguarding Federal information and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

There is a risk that the system may retain data longer than necessary to accomplish the purpose for which the information was originally collected. To mitigate this risk, the Service Desk maintains and disposes of records in accordance with a NARA-approved records schedule and users complete IMT Awareness Training and role-based security and privacy training before acquiring system access and annually thereafter. Information collected and stored within ServiceNow by the Service Desk is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

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: The Service Desk uses ServiceNow to collect data to create and track IT-related service requests and follow up with individuals if more information is needed to fulfill a service request.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

Not applicable. This 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.

☐ Yes, processes are being consolidated.

☒ 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: Officials delegated to handle certain incident types have access to information based on the need-to-know principle to implement applicable incident response procedures.

Auditors have access to information based on the need-to-know principle when there is an active audit (typically on an annual basis).

Internal customers have access to their own contact information and service requests within the system. External customers do not have self-service access to the system and may call the Service Desk or receive emails for request status updates and details.

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

Internal customers have access to create, amend, and view their own tickets. External customers do not have self-service access to ServiceNow – BSEE Enterprise IT Service Desk. They may call the Service Desk or receive emails for updates on the status of service requests.

The access of Service Desk personnel and IT technicians is granted using role-based security and access controls. User access to data is determined by the user's job description and need-to-know as contained in the BSEE Account Management Procedure and implemented NIST 800-53 security and privacy controls.

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: The contract for the Service Desk is ordered off the Government-wide Acquisition Contract and includes the applicable required privacy contract clauses by reference.

☐ 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

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes: Access and changes to ServiceNow – BSEE Enterprise IT Service Desk records are captured in audit logs that are assigned to privileged individuals with appropriate system roles to monitor the audit logs.

☐ No

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

ServiceNow logs every system and records change by capturing the Name, Login ID, timestamp, and modified fields.

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

A warning banner informs individuals that they are accessing a DOI system, are subject to being monitored, and must have no expectation of privacy during use of the system.

ServiceNow – BSEE Enterprise IT Service Desk access is limited to authorized personnel. Audit logs are used to prevent unauthorized monitoring. Audit logs are accessible only by system administrators who are responsible for monitoring the audit logs. Service Desk personnel must complete IMT Awareness Training, role-based privacy and security training, and the Information Systems Security Rules of Behavior Acknowledgment before they gain access to BSEE systems and applications and annually thereafter.

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: ServiceNow maintains its own FedRAMP certified data centers and implements all the required physical controls.

(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: ServiceNow maintains its own FedRAMP certified data centers and implements all the required technical controls.

(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: ServiceNow maintains its own FedRAMP certified data centers and implements all the required administrative controls.

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 Information System Owner (ISO) (Enterprise Operations Chief in the Enterprise Operations & Support Branch), Information System Security Officer (ISSO), and BSEE APO share responsibility for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies. The BSEE System Manager, in consultation with the BSEE APO, is responsible for protecting the privacy rights of internal customers and addressing privacy complaints in a timely manner. The ONRR MRMSS System Manager, in consultation with the ONRR APO, is responsible for protecting the privacy rights of Industry, State, and Tribal users who complete the EMARF Web form and addressing privacy complaints in a timely manner.

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 ISO and ISSO are responsible for the oversight and management of the ServiceNow – BSEE Enterprise IT Service Desk's security and privacy controls. The ISO, ISSO, and authorized users are responsible for immediately reporting any suspected or confirmed loss, compromise, and unauthorized access or disclosure of data from the system in accordance with the Information Systems Security Rules of Behavior Acknowledgement and DOI policy. The BSEE Incident Response Manager is responsible for coordinating the investigation of reported violations from users, ensuring that any suspected or confirmed loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and established DOI procedures, and for working with the BSEE APO to ensure appropriate remedial activities are taken to mitigate any impact to individuals.