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 (SNow)
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: November 12, 2020
Point of Contact:
Name: Rowena Dufford
Title: BSEE Associate Privacy Officer
Email: privacy@bsee.gov
Phone: 703-787-1257
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
- ☒ Others: Industry, State and Tribal Users
- ☐ 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 Bureau of Safety and Environmental Enforcement (BSEE), Technology Services Division (TSD), Enterprise Service Desk is responsible for information technology (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), authorized Industry, State and Tribal users, in the PIA herein as Service Desk customers.

TSD utilizes ServiceNow to support IT service desk functions including trouble ticket, incidents, change request and IT service requests management. ServiceNow offers three avenues to for customers to submit a service request: Service Desk customers may initiate a service desk ticket through the self-service portal, by contacting the Service Desk by phone or email to report a service incident. Another method to create tickets comes from separate monitoring systems. These monitoring systems send event information (malware event, server down, etc.) to ServiceNow, which is turned into a ticket assigned to the proper IT support team. Once the information is entered in ServiceNow, 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 IT Service desk technicians can update the status of the service request ticket by entering work notes and other updates. The ticket is also accessible by the user in the self-service portal.

A subset of Service Desk Customers, i.e., Industry, State and Tribal Users, will also be allowed to initiate a single type of ticket known as the External Minerals Revenue Management Support System (MRMSS) Access Request Form (EMARF) through a public webform hosted by ServiceNow. MRMSS is the ONRR mission-critical system for the collection and disbursement of revenues to States, Tribes and other Federal agencies. Once this information is received, the customer receives an email with a ticket number for future reference. Then the creation of the access to MRMSS follows the normal ServiceNow work process. The public webform is accessible to anyone with the universal resource locator (URL), it follows DOI standards for public-facing internet websites.

After the reported issue is resolved, the IT service technician marks the service desk ticket as resolved and no further action is performed on the ticket. The ServiceNow sends the user a summary and brief customer satisfaction survey. This survey is voluntary and helps TSD improve operations. No PII is collected; however, the survey is linked to the user'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 user or IT service technician reports that service request was not sufficiently resolved.

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. The application pulls customer contact information from Active Directory (AD) and facilitates single sign-on (SSO). Currently, the following IT systems are integrated with ServiceNow with data flowing unidirectionally to ServiceNow: SolarWinds monitoring, Microsoft AD, IBM Identity & Access Management (IAM), ProvisioningWeb, ReservationWeb,

Exit Clearance, and Non-Core Software Request. All the ServiceNow information and processes are located off premises in the cloud provider's FedRAMP certified data centers.

C. What is the legal authority?

5 U.S.C. 301, 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; HSPD-12; and, Executive Order 11807.

EMARF-specific authorities: 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: *Describe*

E. Is this information system registered in CSAM?

☒ 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			

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)*

HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) - Interior, DOI-47 Employee Administrative Records - Interior, DOI-58. The EMARF form is maintained under ONRR's Minerals Revenue Management Support System (MRMSS), OS-30. The 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*
☒ 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: *Specify the PII collected.*

Other PII include business contact information, username, password, and security questions and answers to verify identity. Personal contact information may be provided by customers working remotely; typically, personal contact information is not collected however a customer may provide them as alternative contact methods.

Regarding disability information, the system maintains a checkbox status for customers who self-report Section 508 disabilities. This information is utilized by the service desk to better accommodate IT support for these individuals.

A new ticket is created for every service request. The following information may be utilized to create a service desk ticket:

a. Full name or Active Directory username.
b. Business, mobile phone number (if applicable) and e-mail address.
c. Location of equipment
d. IT technician Assignment Group
e. Configuration item (government asset name / computer name)
f. Service Level due date
g. Description of service request
h. Relevant files such as screenshots or error logs are attached
i. Ticket number for existing service request.

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: Industry, State and Tribal Users

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:* Data is pulled from Active Directory twice a day to ensure user data is accurate and current. User initiated processes from ProvisioningWeb, ReservationWeb, Exit Clearance, and Non-Core Software Request automatically push data into ServiceNow to fulfill service requests. For example, when a new user account needs to be created, an existing one needs to be disabled or if a customer needs to have Non-Core software installed; these applications automatically notify ServiceNow with the data needed to fulfill the request.
☒ Other: *Describe*: Legal holds or notices that identify records that may need to be retained.

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

Depending on the customer submitting a service request, the Service Desk collects different information about the IT system, software, or technology-related information and the customer in order to best determine how to resolve an issue. AD and IAM information are contained within the system to streamline the incident reporting process and to allow support technicians to easily follow up with customers who have open service requests. Username is used to create accounts, assign permissions and track security incidents. Security questions are used to verify a customer's identity.

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.*
Data collected will be used by IT staff to create network accounts, incident tickets, problem tickets, service request tickets and gather data on security incidents. When supervisory approval is needed to complete a request, the supervisor is notified.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*
The Service Desk performs the same functions above to BOEM and ONRR under a reimbursable service agreement. It performs the same function with regard to Citrix application access for the Bureau of Land Management (BLM) users/customers.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*
Tickets may involve security incidents which would be reported to DOI-CIRC or other internal organization and, in turn, reported to the Department of Homeland Security US-CERT.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*
Through ProvisioningWeb, ONRR grants authorized State and Tribal users an AD account. These state or tribal users can call or go into ServiceNow self-service portal to request access to ONRR MRMSS applications to create and submit reporting data related to ONRR functions. Data collected will be used by IT staff to create network accounts, incident tickets, problem tickets, service request tickets and gather data on security incidents.

☒ Contractor: *Describe the contractor and how the data will be used.*
The Service Desk and Enterprise IT are staffed by contractor personnel. Other contractors are used by BSEE, BOEM and ONRR to fulfill their missions and BLM contractors who need access to Citrix. Data collected will be used by IT staff to create network accounts, incident tickets, problem tickets, service request tickets and gather data on security incidents.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*
ServiceNow stores information which is encrypted in a FedRAMP certified cloud storage facility in the US.

Data collected will be used by IT staff to create incident tickets, problem tickets, service request tickets and gather data on security incidents for authorized Industry, State and Tribal users.

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.*

Internal employees and authorized users voluntarily submit service requests and may choose but are not required to provide information such as personal contact information if working remotely, however it could impede or delay resolution of their issue or service request.

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Internal employees and authorized users are provided an AD account through the employee onboarding process and access request forms, and cannot decline the daily updates from AD and IAM into ServiceNow.

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

☒ Privacy Act Statement: The EMARF Form contains the following:

AUTHORITY: 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.

PRINCIPAL PURPOSE: To request for and obtain an account for access to the Minerals Revenue Management Support System (MRMSS), validate identity of lease and permit holders, current and former landowners, royalty payors, production operators, who report bonuses, rents, and royalty payments, general ledger activity, who report the collection of revenues as lease holder(s) of mineral leases on Federal or Indian lands.

ROUTINE USE: Disclosure of this information is also subject to all published routine uses identified in the Privacy Act System of Records Notice OS-30, Minerals Revenue Management Support System, Vol.81, No. 58 FR 16207; March 25, 2016, which may be seen at: https://www.doi.gov/privacy/sorn.

DISCLOSURE IS VOLUNTARY: If the individual does not furnish the information requested, there will be no adverse consequences. However, failure to furnish information requested on the form may delay or impair processing the customer service request.

☒ Privacy Notice: *Describe each applicable format*.

Privacy notice is provided through the publication of this privacy impact assessment; the publication of DOI-47, Logical Security Files SORN, and DOI-58, Employee Administrative Records SORN and Minerals Revenue Management Support System (MRMSS), OS-30.

Customers are on a government computer and signed into an AD authenticated account, so a privacy notice is provided at the time of logging into the government computer.

☒ Other: *Describe each applicable format.*
The DOI privacy policy appears at the bottom of the EMARF webform.

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

I. Will reports be produced on individuals?

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

Reports will be produced on individuals to track their service requests. The service desk can view the incident/service request ticket history for each customer when they call for assistance. In addition, they can see the details of any assigned government furnished computer equipment.

Service level records by IT Service Desk personnel are produced to track performance.

☐ No

Section 3. Attributes of System Data

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

Information in ServiceNow is generally obtained from DOI records. Information in EMARF is collected directly from the individual or Industry, State and Tribe authorized user and assumed to be accurate at the time of collection.

B. How will data be checked for completeness?

Data is checked for completeness by the employee or authorized user providing the data and cross-referenced with the existing DOI databases, such as AD.

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

Information is verified as users call the Service Desk to submit a service ticket. User data is kept current by daily updates from AD and asset inventories are updated annually as required by an annual ongoing authorization.

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 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 fall under their Admin schedule and are retained for three years.

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

Electronic records shall be deleted. Though no longer collected via hard copy, those records shall be shredded or pulped. Backup tapes are reinitialized and reused. The BSEE Exit clearance process documents the steps and procedures used to remove or archive information when employees and contractors leave the agency. The records management policies and procedures govern disposal of information. Procedures are also documented in section MP-06 of the Media Protection (MP) Standard Operating Procedure. ONRR records are shredded and electronically deleted.

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 principle of least privilege is observed during all phases of the information lifecycle. The potential privacy risks identified include inadvertent disclosure, unauthorized access, surveillance and theft of data. The risk is mitigated through security and privacy controls to protect the system and data. Any unauthorized disclosure may reveal details of an individual's IP address, contact information and service request history. All data is stored and maintained in secure systems and is protected from unauthorized access by firewalls, intrusion detection systems, antivirus and the Active Directory domain environment. User activity is monitored and logged to ensure only appropriate use of the system and data.

To mitigate the insider threat, collected data is protected by access controls including two-factor authentication, least privilege principles and restricted access limited to authorized users. Employees are required to complete annual Information Management and Technology (IMT) Awareness Training, which includes privacy and security training and affirming the BSEE Rules of Behavior. Those with access to PII are required to also complete mandatory role-based privacy training annually. The data is not shared outside of BSEE/DOI. BSEE computers are secured and monthly scans are conducted in accordance with the BSEE Continuous Monitoring Program Plan.

There is a risk with the use of the EMARF webform that it could introduce unknown vulnerabilities to access form data and/or cause denial of service. This webform is public internet-facing and doesn't require authentication to submit, however, there are internal compensating security controls like encryption which conform to applicable NIST and DOI security policies to mitigate these risks such as 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. In addition, authentication to the MRMSS system requires validation and approval by ONRR before access is granted

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. ServiceNow 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 use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy and NIST guidelines. 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 individuals requesting access via the EMARF webform may not fully understand the need for that information. This is mitigated through the Privacy Act notice at the point of collection and ONRR's Minerals Revenue Management Support System (MRMSS), OS-30, and this privacy impact assessment which serve as constructive notice. The EMARF webform only collects name and business contact information which mitigates the risk to individual privacy.

There is a risk that the system may collect, store or share more information than necessary, or the system will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Access to data is restricted and authorized personnel only retrieve and process service requests as authorized and necessary to perform official functions. Data maintained is limited to the minimal amount of data needed to meet Federal records requirements and the applicable retention schedules.

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 data collected is only used to create and track service requests and to follow up with individuals if more information is needed.

☐ 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?

Data is updated as the employee contacts the service desk. The technician verifies the required field for relevance and accuracy. The data is updated annually as required by an annual ongoing authorization and pulled twice daily from AD and pushed once daily from IAM.

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: Officials delegated to handle certain incident types.

Auditors: Access is based on a need to know when there is an active audit, typically on an annual basis.

End-Users (customers), excluding Industry, State and Tribe users: Have access to their own contact information and service requests. Industry, State and Tribe users do not have self-service access to ServiceNow they may call-in or receive emails for status and details.

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

Authorized users, excluding Industry, State and Tribe users, have access to create and amend their own user tickets. Access is granted only to Service Desk personnel and IT technicians 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 NIST 800-53 security and privacy controls.

Industry, State and Tribe users do not have self-service access to ServiceNow they may call-in or receive emails for status and details.

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?*

The contract for the Enterprise Service Desk is ordered off the Government-wide Acquisition Contract and includes all privacy contract clauses by reference such as:
52.204-21, Basic Safeguarding of Covered Contractor Information Systems
52.224-1, Privacy Act Notifications

52-224-3, Privacy Training
52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a)

☐ 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?

ServiceNow logs every change to the records and system by capturing the Name, Login ID, timestamp and what fields were changed.

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

All changes are logged by ServiceNow and audit logs are used to prevent unauthorized monitoring.

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 their own FedRAMP certified data centers with 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. *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 Information System Owner, Information System Security Officer and the BSEE Privacy Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in accordance with Federal laws and policies for the data managed and stored by the Enterprise IT Service Desk. The System Manager in consultation with the BSEE Privacy Officer is responsible for protecting the privacy rights of the employees for the information collected and maintained in ServiceNow. The management of the EMARF data and webform is the responsibility of the ONRR System Manager and Privacy Officer for protecting individual privacy obtained from the EMARF webform.

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 Information System Owner and Information System Security Officer are responsible for oversight and management of the Enterprise Service Desk's security and privacy controls. All authorized users are responsible for immediately reporting any suspected loss, compromise, unauthorized access or disclosure of data from the system in accordance with the rules of behavior and DOI policy. The BSEE Incident Response Manager coordinates the investigation of reported violations from users. The Incident Response Manager is also responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and procedures.