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: BSEE T-Metrics Call Center
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: 25 February 2025
Point of Contact
Name: Dianna Taylor
Title: Associate Privacy Officer
Email: privacy@bsee.gov
Phone:703-787-1763
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 BSEE T-Metrics Call Center is a FedRAMP-certified call management system used by the Bureau of Safety and Environmental Enforcement (BSEE) to efficiently handle and route incoming customer calls. It is the backbone of the BSEE Enterprise IT Service Desk, commonly called the "Service Desk."

The BSEE Enterprise IT Service Desk is the primary contact point for logging, assigning, tracking, reporting, and resolving service requests. It supports BSEE, the Bureau of Ocean Energy Management (BOEM), and the Office of Natural Resources Revenue (ONRR) (collectively known as internal customers), as well as authorized Industry, State, and Tribal users (external customers).

Customers can reach the Service Desk using various phone options, including personal, home, or Microsoft Teams phones. Once a call is received, the T-Metrics Call Center's Automatic Call Distributor (ACD) module processes it. The system displays the caller ID (which may include the trunk number tied to the 10-digit phone number) and the time the call has been waiting in the queue. The ACD then analyzes the nature of the call and the caller's history to determine the appropriate skillset, ensuring the routing of the call to the most qualified agent.

The T-Metrics Call Center enhances call routing efficiency by integrating the phone system with Microsoft Teams and ServiceNow, the IT service request management system for the BSEE Enterprise IT Service Desk. ServiceNow was assessed separately under its own Privacy Impact Assessment (PIA), available at the DOI PIA Website. This integration enables a streamlined, one-way data flow that improves communication and optimizes service request management. As the central hub for managing all incoming calls to the Service Desk, the system plays a vital role in supporting safety, regulatory compliance, and BSEE's mission of environmental protection in offshore energy-related activities. Improving service delivery reinforces confidence in BSEE's ability to meet customer needs.

C. What is the legal authority?

The legal authorities that authorize BSEE to use T-Metrics include the E-Government Act of 2002 (Public Law 107–347, 116 Stat. 2899, 44 U.S.C. § 3101, H.R. 2458/S. 803); U.S Code Title 31, U.S.C. § 1348(b); 43 CFR 20138-007; Federal Information Security Modernization Act (FISMA) of 2014; Office of Management and Budget (OMB) Circular A-130; 5 U.S.C. 301 Departmental Regulation.

The Office of Natural Resources Revenue (ONRR) collects information through the Electronic MRMSS Access Request Form (EMARF) to manage access to the Minerals Revenue Management Support System (MRMSS). Multiple federal laws have approved this collection: 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, 43U.S.C. 1331–1356b.These authorities provide the legal foundation for the ONRR to collect and manage data necessary to administer federal and Indian mineral resources properly.

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: [010-000002649]. The System Security and Privacy Plan for BSEE T-Metrics Call Center.

☐ 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	Not applicable

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

☐ Yes:

☒ No
The T-Metrics Call system does not require a published Privacy Act System of Records Notice (SORN) because it does not retrieve or store information using a unique identifier. The T-Metrics Call Center does not track, maintain, or store personally identifiable information (PII). It functions solely as a call management solution supporting ServiceNow, BSEE's Enterprise IT Service Desk, by facilitating call routing and service request management. However, applicable SORNs cover records maintained within ServiceNow, as it may store and retrieve information in a manner subject to the Act of 1974. BSEE and BOEM have an Information Technology Services, Enterprise Services Network, and Mission IT inter/intra-agency agreement.

BSEE, BOEM, and ONRR provide privacy notices through telephone communication and the Enterprise Hosted Infrastructure PIA, which covers the collection and use of AD information and includes the applicable SORNs, such as 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) and 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) and INTERIOR/DOI-36, Telephone Call Detail Records - 59 FR 7260 (February 15, 1994); modification published 73 FR 8342 (February 13, 2008) and 86 FR 50156 (September 7, 2021). Additionally, ONRR provides privacy notices through the MRMSS PIA and the INTERIOR/OS-30 Minerals Revenue Management Support System. The SORNs may be accessed on the DOI-wide SORNs Web page.

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 Phone Number
☒ Home Telephone Number
☒ Other: Limited non-sensitive, business-related PII such as the customer's Microsoft Teams phone number.

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: A Customer Agent may share the customer's name and phone number with another agent who can handle the customer's request.

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: Customer agents manually enter non-personally identifiable data, such as the reported issue and the solution provided, into the ServiceNow system for tracking and resolution purposes.
☐ Other:

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

The T-Metrics Call Center collects customer information to route calls from BSEE, BOEM, and ONRR customers to a Customer Agent. The Customer Agent is key in providing direct assistance or escalating the call for further IT support. Collected information is manually entered into the ServiceNow system to facilitate issue resolution and track support 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.

☒ 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.
BSEE may share T-Metrics data related to reported security and privacy incidents with the DOI Computer Incident Response Center (DOI-CIRC).

☒ Other Federal Agencies: BSEE may share T-Metrics data related to reported security and privacy incidents to the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency.

☒ Tribal, State or Local Agencies: Through Provisioning Web, 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: T-Metrics Call Center solution stores encrypted information in a FedRAMP-certified cloud storage facility in the United States.

BSEE, BOEM, and ONRR personnel can contact the BSEE Enterprise IT Service Desk to obtain information about 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 not to provide information to address their service requests. However, failure to provide certain information may impede Service Desk personnel from referring or resolving their service request or issues.

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 accessing 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 and enter them into ServiceNow for Service Desk use.

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 ONRR personnel from resolving their service request or inquiry. Internal customers can choose to not provide their information to address their service request. However, failure to provide certain information may impede or delay Service Desk personnel from resolving their service request or issue.

☐ 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, BOEM, and ONNR provide privacy notices through telephone communication and the Enterprise Hosted Infrastructure PIA, which covers the collection and use of AD information and includes the applicable SORNs, such as INTERIOR/DOI-47 (HSPD-

12: Logical Security Files) and INTERIOR/DOI-58 (Employee Administrative Records), INTERIOR/DOI-36, Telephone Call Detail. Additionally, ONRR provides privacy notices through the INTERIOR/OS-30 Minerals Revenue Management Support System, SORN. The DOI, BSEE, and ONRR PIAs may be accessed for review through the DOI PIA Website. The DOI and ONRR SORNs may be accessed for review through the DOI SORNs Web page.

Customers who contact the BSEE Enterprise IT Service Desk by phone receive a greeting that informs them their call may be monitored or recorded for quality assurance purposes.

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

BSEE also provides a notice through this PIA made available on the BSEE PIA Web page hosted by the DOI Privacy Office.

☐ None

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

Data is neither stored nor retrieved by a personal or unique identifier ensuring compliance and minimizing risks associated with sensitive information retention. The T-Metrics ACD (Automated Call Distribution) collects essential customer information including names, Microsoft Teams, personal and home phone numbers. This data is displayed in real-time on the customer agent dashboard to facilitate immediate and informed interactions.

I. Will reports be produced on individuals?

☒ Yes: Customer Agent Supervisors will generate tailored reports using each agent's assigned user account. These reports access customer agents' performance and monitor key performance indicators (KPIs) such as average handle time, first call resolution rate, and customer satisfaction scores, and do not include customers' personally identifiable information.

☐ No

Section 3. Attributes of System Data

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

Data is collected directly from all BSEE, BOEM, and ONRR customers who seek assistance from the BSEE Enterprise IT Service Desk and is presumed to be accurate when provided.

When an internal or external customer contact the Service Desk, the Customer Agent verifies the customer's identity by comparing the provided information with the customer's details in Active Directory (AD). Any additional information the customer shares is deemed accurate at the time of collection. Customers are responsible for ensuring that the information they provide to the Service Desk is accurate and relevant.

B. How will data be checked for completeness?

Data is collected directly from all BSEE, BOEM, and ONRR customers who seek assistance from the BSEE Enterprise IT Service Desk and is presumed to be complete.

For internal customers, the completeness of the data is verified by the employee or authorized user submitting the information. The customer's identity is also cross-referenced with existing Department of the Interior (DOI) databases, such as Active Directory (AD), to ensure accuracy.

The data for external customers is collected directly through the Electronic MRMSS Access Request Form (EMARF) Web form. It is assumed to be complete upon submission, as there is no additional verification process at the time of collection.

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

Data is collected directly from BSEE, BOEM, and ONRR customers at the time they seek assistance from the BSEE Enterprise IT Service Desk and is presumed to be current when provided.

Data is neither synchronized nor transferred, so there is no requirement to maintain data currency within T-Metrics.

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

The BSEE T-Metrics Call Center records and reports are retained in accordance with DOI's Administrative Departmental Records Schedule, System Maintenance and Use Files (DAA-0048-2013-0001-0013). Records are cut off when superseded or obsolete then destroyed no later than 3 years after cutoff. BSEE 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?

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 BSEE T-Metrics Call Center presents a limited risk to privacy of individuals for the collection and use of official contact information to identify and refer reported issues. There is an increased risk to privacy due to the collection and use of personal phone number or other contact information within T-Metrics and the associated risks of hosting it within the infrastructure of a cloud service provider, potential lack of notice on the purpose, uses, sharing and disposal of PII, and any potential unauthorized access, misuse, or compromise of PII. However, these risks are mitigated through several key measures and mitigating controls. The cloud service provider, Amazon Web Services (AWS), holds FedRAMP certification, which ensures compliance with Federal security standards and best practices. 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. Additionally, the system operates under FISMA Moderate classification standards, enforcing rigorous security protocols to protect sensitive data. AWS also implements a range of robust security controls designed to ensure data confidentiality, integrity, and availability, including encryption, access controls, and continuous monitoring.

Individuals may face limited risks to their privacy if they are unaware of the purpose for collecting their information, how their information is stored, or how the Service Desk intends to utilize it. These risks are effectively mitigated by the notice provided through the publication of this PIA and the associated PIAs and SORNs for the related systems that collect the data. These include the Enterprise Hosted Infrastructure PIA; ServiceNow PIA; INTERIOR/DOI-47, HSPD-12: Logical Security Files; INTERIOR/DOI-58, Employee Administrative Records; INTERIOR/DOI-36, Telephone Call; and INTERIOR/OS-30 Minerals Revenue Management Support System. By ensuring that these documents communicate data collection and usage practices, stakeholders are better informed about managing and protecting their information.

There is no risk of maintaining PII longer than authorized since customer records are not retained or stored in T-Metrics. The Service Desk reduces the risks of unauthorized access, insider threats, and improper use of information by implementing appropriate administrative, physical, and technical safeguards to protect the system and data. System administrators assign user roles to ensure that only authorized personnel with a valid need-to-know can access and use the system to perform their official duties. The system logs and monitors all user activity to ensure proper system and data use. Additionally, employees and contractors must complete annual Information Management and Technology (IMT) Awareness Training, which includes modules on privacy and security, Controlled Unclassified Information, and the Paperwork Reduction Act, as well as 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 gaining access and annually thereafter.

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 BSEE T-Metrics Call Center offers a FedRAMP-compliant contact solution, allowing the bureau to deliver help desk, ticketing, and workflow services to internal customers and BOEM and ONRR

☐ 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?

This is not applicable, the T-Metrics Call Center does not generate new data or aggregate previously unavailable information about individuals. It solely processes existing data without changing its scope or context.

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).

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

Role-based security and access controls govern the BSEE T-Metrics Call Center user access. An individual's job responsibilities and need-to-know determine their access as outlined in the BSEE Account Management Procedure, which aligns with NIST 800-53 security and privacy controls. Users are assigned roles according to their duties, including Customer Service Agents, who handle incoming calls; Customer Service Supervisors, who can view agent and queue statistics; and System Administrators, who manage call flow and oversee overall call center operations. Access to data is restricted to what is necessary for each role, ensuring that users only access data relevant to their responsibilities.

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 system is hosted by a Cloud Service Provider (CSP). Contractors supporting the BSEE Enterprise IT Help Desk will utilize the system for maintenance and operational tasks. Privacy clauses are included in the contract. The contract includes the following Privacy Act clauses:

- Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)
- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52.239-1 Privacy or Security Safeguards (Aug 1996)
- FAR 52.224-3 Privacy Training (Jan 2017)

☐ 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. Audit logs capture all Customer Agent's actions and record changes in the BSEE T-Metrics Call Center. Access to the audit logs is limited to the System Administrator.

Administration Portals allow the System Administrator to manage system settings, user accounts and access controls.

Supervisors can view agent statuses and current activities in real-time through a live dashboard display.

☐ No

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

The BSEE T-Metrics Call Center collects and maintains the date and time of all user actions within the system in the audit log, which the System Administrator reviews. Customer information, including names, contact details, and other relevant data, is obtained during interactions with the Customer Agent. Customer Agent Supervisors can generate reports on Customer Agent performance, such as call handling times, the number of interactions, and resolution rates, to identify trends over time and assess productivity and efficiency.

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

Access to the BSEE T-Metrics Call Center is limited to authorized personnel. Audit logs prevent unauthorized monitoring and are accessible only by System Administrators. Service Desk personnel must acknowledge the DOI Rules of Behavior (Information Systems Security Rules of Behavior Acknowledgment) and complete annual security, privacy, records management, Controlled Unclassified Information (CUI) awareness training, and role-based privacy and security training before they gain access to BSEE systems and applications and annually after that.

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. Amazon Web Services (AWS) hosts T-Metrics, which is FedRAMP-compliant. The AWS System, Security, and Privacy Plan outlines AWS US East / US West FedRAMP Moderate facility 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. Amazon Web Services (AWS) hosts T-Metrics, which is FedRAMP-compliant. The AWS System, Security, and Privacy Plan outlines AWS US East / US West FedRAMP Moderate facility 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. Amazon Web Services (AWS) hosts T-Metrics, which is FedRAMP-compliant. The AWS System, Security, and Privacy Plan outlines AWS US East / US West FedRAMP Moderate facility 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), the Information System Security Officer (ISSO), and the BSEE APO share

responsibility for the implementation of adequate safeguards 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 internal customers' privacy rights and promptly addressing privacy complaints. The ONRR MRMSS System Manager, in consultation with the ONRR Privacy Official, is responsible for protecting the privacy rights of Industry, State, and Tribal users who complete the EMARF Web form and promptly addressing privacy complaints. Additionally, the ONRR System Manager oversees and manages the protection of information processed in the BSEE T-Metrics Cloud Center, collaborating with the BSEE APO, BSEE T-Metrics Cloud Center Information System Owner, and ISSO to safeguard individual privacy. The BSEE APO will promptly process privacy complaints or requests and refer them to the appropriate BSEE or ONRR officials. The BSEE APO will also notify and collaborate.

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 BSEE T-Metrics Call Center Information System Owner oversees and manages security and privacy controls. The Information System Owner and the Information System Security Officer are accountable for ensuring that any loss, compromise, unauthorized access, or disclosure of agency PII is reported to DOI-CIRC within 1 hour of discovery, in compliance with federal policy and established procedures. Authorized T-Metrics users must also protect individual privacy and report any suspected or confirmed privacy breaches by Federal and DOI policies. The Information System Owner and Information System Security Officer are responsible for coordinating with the BSEE APO to implement appropriate remedial actions to mitigate any impact on individuals resulting from a privacy breach. T-Metrics adheres to specific FedRAMP and Cybersecurity and Infrastructure Security Agency (CISA) requirements for breach notification and response.