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: Bureau of Safety and Environmental Enforcement Network (BSEENet)
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: June 17, 2022
Point of Contact
Name: Rowena Dufford
Title: Associate Privacy Officer
Email: privacy@bsee.gov
Phone: 703-787-1257
Address: 45600 Woodland Rd, 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 Network (BSEENet) General Support System (GSS) is the wide area network (WAN) that provides an interconnecting backbone to support a number of business-related and mission-related applications used by the Bureau of Safety and Environmental Enforcement (BSEE), Bureau of Ocean Energy Management (BOEM), and Office of Natural Resources Revenue (ONRR). BSEENet is managed by the BSEE Technology Services Division (TSD) and supports approximately 2,400 employees and contractors who are the user community. The BSEENet GSS includes servers, workstations, networking devices (routers, firewalls, switches, and intrusion detection systems), storage devices, backup devices, and print devices. BSEENet provides several services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the WAN. BSEENet services include malware protection, Voice Over IP (VOIP) services, systems management services, backup processes, Active Directory and group policy structures, and vulnerability scanning services.

This modification to the BSEENet GSS changes from a tape backup process to Druva cloud-based software-as-a-service (SaaS) backup process and removes Enterprise Risk Management System (ERMS) which was retired in FY21.

BSEENet Active Directory (AD) account information for user access authenticates to the Enterprise AD, which is assessed separately in the Enterprise Hosted Infrastructure privacy impact assessment viewable at https://www.doi.gov/privacy/pia. The BSEENet GSS does not specifically contain personally identifiable information (PII) however the user community accesses a number of services which may contain PII. It is the responsibility of the application, office or individual using BSEENet services to protect the information collected, used, maintained, or disseminated on BSEENet. These services include office automation software such as Microsoft Office, Adobe products, BisonConnect (Microsoft 365 for Government) and Geographical Information System and other products that provide access to the Department of the Interior’s (DOI) applications which support Human Resource, Payroll, Finance, Personnel Security, and other functions for BSEE, BOEM and ONRR. In addition, BSEENet provides access to major applications for BSEE, BOEM and ONRR including the Minerals Revenue Management Support System (MRMSS) and Technical Information Management System (TIMS):

- MRMSS – Manages all revenue associated with both Federal offshore and onshore mineral leases. The Leasing Division of BOEM handles all aspects of offshore Federal leasing. Federal onshore mineral leasing activities are managed by the DOI Bureau of Land Management (BLM) and the Department of Agriculture’s U.S. Forest Service. ONRR, in conjunction with the DOI Bureau of Indian Affairs, provides revenue management services for mineral leases on Indian lands. See the MRMSS PIA for evaluation on privacy risk and details on how PII is maintained.
- TIMS - Automates many of the business and regulatory functions supporting BOEM, BSEE, and ONRR. TIMS is maintained and operated by the BSEE Office of Administration. TIMS enables the BOEM, BSEE, and ONRR staff in Alaska, California, Colorado, Louisiana and Texas and the bureaus’ headquarters to share and combine data to perform multiple functions. Functions include creating and printing maps; standardizing processes, forms, and reports; promoting the electronic submission of data; and reducing the costs of setting up and maintaining duplicate databases and information storage and retrieval systems. It also allows the sharing of required information with private, state, academic and tribal stakeholders. See the TIMS PIA for evaluation of privacy risk and details on how PII is maintained.

C. What is the legal authority?

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); the E-Government Act of 2002 (Public Law 107-347) and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

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 010-000002659, 010-000002503, 010-000002535, 010-000002649, 010-000002254; BSEENet 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.*
Minerals Revenue Management Support System (MRMSS)	To manage all revenue generated by Federal offshore and onshore mineral leases.	Yes	MRMSS contains customer contact information, Tax Identification Number (TIN), Social Security Number of a sole proprietor, Individual Indian Mineral Owner account number, allottee number, bank account and routing numbers, and employee names and phone numbers. See the MRMSS PIA for an assessment of the privacy risks.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Technical Information Management System (TIMS)	Supports the business and regulatory functions of BOEM and BSEE	Yes	TIMS maintains primarily business contact information but may contain personal contact information as inputted by users. See the TIMS PIA for an assessment of the privacy risks.
Auction of Offshore Wind Lease (AOWL) System	Allows BOEM to conduct auctions of offshore wind leases.	Yes	Business contact information. See the AOWL PIA for an assessment of the privacy risks.
BSEE!Safe Direct Messaging Service	Allows BSEE to quickly notify offshore oil and gas workers and employees of new safety information posted to BSEE.gov.	Yes	Personal and business contact information. See the BSEE!Safe PIA for an assessment of the privacy risks.
Ohmsett Customer Relationship Management	Processes customer relationship management activities.	Yes	Personal and business contact information for subscription to Ohmsett publications, training information and studies. See the Ohmsett PIA for an assessment of the privacy risks.
Personnel Security System	Tracks the progress of background investigation requests and adjudications; approval of logical and physical access to facilities and computer networks at DOI and document when national security clearances are granted, withdrawn, revoked or are due for re-investigation.	Yes	Information needed for background investigations such as SSN, DOB/POB, etc. See the PSS PIA for an assessment of the privacy risks.
ServiceNow (SNow)	Support IT service desk functions including trouble ticket, incidents, change request and IT service requests management.	Yes	Business and personal contact information; disability information. See the ServiceNow PIA for an assessment of the privacy risks.
Contractor Tracking System	Allows Contracting Officer Representatives to see which contractors on each contract.	Yes	Business contact information.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Exit Clearance	This system automatically notifies the appropriate officials of the last day of employment and the process of clearing from the BOEM-BSEE rolls.	Yes	Business contact information.
Requisition Tracking	Used to track requisitions approvals and funding.	Yes	Business contact information.
ProvisioningWeb	Manages requests for new personnel accounts, Workstations, phones, VPN access, elevated accounts and local admin accounts.	Yes	Business contact information.
Financial Number Generator	Generates unique tracking numbers for payments on training, travel, GPO print orders and accruals.	Yes	First name, last name, bureau and location.
Non-Core Software	User requests for approved software applications outside of the standard applications loaded on workstations.	Yes	Business contact information.
User ID Assign	Synchronizes Active Directory login ID and PSS personnel ID.	Yes	Username and password.
PIV	Service Desk uses to temporarily disable PIV enforcement on a user workstation because the PIV card is not available or not working.	Yes	Username and password.
AD Editor	Allows the Service Desk to update select fields in AD data, ONRR version and BSEE-BOEM versions.	Yes	Business or home address and phone number.
Reservation Web	Users create events and invitations.	Yes	Business contact information.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Environmental Studies Program - ESPPAT	Tracks and evaluates performance on BOEM Environmental Studies.	Yes	Business contact information.
Event Scheduling	Users schedule meeting rooms and specify room setup.	Yes	Business contact information.
Environmental Studies Tracking	Tracks multi-year financials of BOEM Environmental Studies.	Yes	Business contact information.
Personnel Directory	Interactive phonebook for BSEE staff	Yes	Business contact information.
Award Tracking	Tracks submission of employee recognition request.	Yes	Business contact information, award information.
Druva Cloud Backup Software-as-a-Service	Backup data supported by BSEENet	Yes	Backup of business information related to the missions of the programs, offices and divisions and of personal drives.

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

☒ Yes: Active Directory records are covered by DOI-47, Logical Security Files, 72 FR 11040, March 12, 2007. Other program and user activities that may be subject to the Privacy Act are covered by various Department-wide and BSEE SORNs which are found 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
☒ Other: BSEENet uses AD information (e.g., username, password, business contact information, etc.), Personal Identification Verification (PIV) credentials, and security questions

and answers to authenticate user identity and to assign permissions to users. Due to the nature of the BSEENet GSS, there is a potential that large amounts of PII may be contained within the BSEENet environment. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose.

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

☒ Individual
☒ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

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

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

Information from AD is shared with MRMSS, TIMS and DOI AD/ Enterprise Services Network for the purpose of authenticating users and managing access. Initial information is collected by Human Resources (HR) or the Contracting Officer Representative (COR) from individuals during the on-boarding process. As part of this process, the individual is instructed to complete the required security, privacy and records training and record it in the DOI Learning Management System (LMS); subsequently, this is an annual requirement. Upon completion of the training, the individual forwards a copy of the Certificate of Completion to update the completion field(s) in the LMS. HR or the COR then creates a request which notifies TSD to create the network account(s) for BSEENet.

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

The primary use of PII is to enable and maintain authorized access to BSEENet to accomplish the business-related and mission-related applications used by BOEM, BSEE and ONRR. Initially, the information is used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests.

Access to BSEENet includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

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.*

The primary use of PII is to enable and maintain authorized access to BSEENet to accomplish the business-related and mission-related applications used by BSEE. Initially, the information is used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests.

Access to BSEENet includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

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

The primary use of PII is to enable and maintain authorized access to BSEENet to accomplish the business-related and mission-related applications used by BOEM and ONRR. Initially, the information is used to specify a username, user account and temporary password which the user is prompted to change at first use. The security questions and answers authenticate user identity for password reset requests.

Access to BSEENet includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

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

Other Federal agencies do not have direct access to the system. However, data may be shared with other Federal agencies as necessary to meet legal or mission requirements in the course of conducting official business. For example, exchange of communications or information generated from the user community. Authorized sharing with external agencies will be made pursuant to DOI mission authorities and applicable system of records notices for each use.

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

Tribal, State or Local agencies do not have direct access to BSEENet, but information may be shared with authorized users for official purposes as necessary to manage network functionality as outlined in the table located in Section 1, F. Access to BSEENet includes a number of services to the user community to enhance productivity and provide security for the information stored, processed, and transported over the network.

☒ Contractor: *Describe the contractor and how the data will be used.*

A contract company handles the BSEE Enterprise Service Desk, which assists users in obtaining unique username, assigning temporary passwords, and granting permissions. In addition, they have access to security questions and answers to validate user identity. They also handle and resolve user issues with BSEENet.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

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

☒ Yes: While an individual's supervisor or COR completes and submits the required information to create the individual's user account, this information is derived from Enter-on-Duty on-boarding forms. These forms provide the requisite Privacy Act Statement that informs the individual that providing the information is voluntarily and the consequences of not providing the information may impact employment.

☐ No:

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

☒ Privacy Act Statement: The Provisioning Web is an internal web-based onboarding system used to collect the information needed to create user accounts which are requested by HR personnel. A Privacy Act Statement is included on the onboarding forms (e.g., OF 306, Declaration for Federal Employment and SF-85P, Questionnaire for Public Trust Positions) which include the requisite information on the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: Users can also view how their information will be used in the BSEENet Privacy Impact Assessment, the DOI-47 Logical Security Files system notice, and BSEE system of records notices published on https://www.doi.gov/privacy/sorn.

☐ Other: *Describe each applicable format.*

☐ None

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

Service Desk personnel can retrieve a user's account by their name or username within BSEENet. This is typically done at the behest of users in order to reset their passwords or to resolve computer and network issues.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*
Automated scheduled and ad hoc reports may be generated to audit user activity and determine accounts which need to be disabled due to employee separation. Data will include name, username, activity date/time, location and applications accessed via BSEENet. BSEENet administrators have access to these reports.

☐ No

Section 3. Attributes of System Data

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

Data is not collected from other sources. The user can only access the BSEENet system as a valid, authorized Active Directory user with current and accurate credentials, an active PIV card, and a valid BSEENet user account.

B. How will data be checked for completeness?

Users are responsible for the completeness of the data provided in the user account request form.

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

The BSEE Information System Continuous Monitoring Plan (ISCMP) specifies the review, monitoring and assessment frequency of all National Institute of Standards and Technology (NIST) 800-53 security and privacy controls to maintain the integrity and accuracy of the data.

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

System administration or AD records are maintained under the Departmental Records Schedule (DRS)-4.1, Short Term Information Technology Files, System Maintenance and Use Records (DAA-0048-2013-0001-0013), and System Planning, Design, and Documentation (DAA-0048-2013-0001-0014). These records include IT files that are necessary for day-to-day operations but no longer term justification of the bureaus/offices activities. The disposition of these records is temporary. Records covered under DAA0048-2013-0001-0013 have a temporary disposition and will be cut off when superseded or obsolete and destroyed no later than three years after cut-off.

Records covered under DAA-0048-2013-0001-0014 have a temporary disposition and will be cut off when superseded by a newer version of upon termination of the system and destroyed three years after cut-off.

Retention periods vary depending on the user created or manage contents and purpose of the program records. Records created by individual users are retained and disposed of in accordance with applicable Departmental and bureau/office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record based on the subject or function and records series. However, the Bureau has a number of litigation holds in place which may require the retention of these records past the cut-off date.

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

The BSEE Account Management Procedures specify the procedures and disposition of data collected for BSEENet accounts. The BSEE Exit Clearance process documents the steps and procedures used to remove information when employees and contractors leave the bureau. The records management policies and procedures also govern disposal of information.

Procedures for disposition of the data stored in individual applications will vary by program office and needs of the agency. Due to the nature of BSEENet as a GSS, there may be numerous records schedules with different dispositions applicable to the records created and maintained by users. It is the responsibility of each program office and user that creates or maintains Federal records to maintain and dispose of the records in accordance with the appropriate records schedule and disposition authority that covers their program area.

Approved disposition methods for records include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1 and NARA guidelines.

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

BSEENet allows the user community to access a number of services which may contain PII. BSEENet is not designed or characterized to support the collection, use, maintenance or dissemination of PII other than that found in AD. There is minimal risk to the privacy of user information throughout the information lifecycle; user information is authenticated by AD for access to BSEENet. Risk is further reduced by following established guidance from NIST SP 800-53 on access controls. Privacy risk to BSEENet network accounts would affect usernames, passwords and security questions and answers.

These risks are mitigated by a combination of administrative, physical and technical controls. BSEENet has a Moderate system security categorization in accordance with NIST standards and Federal Information Processing Standard (FIPS) 199, and the Federal Information Security Modernization Act (FISMA). The BSEENet System Security Plan (SSP) describes appropriate security and privacy controls implemented to safeguard BSEENet information collection, use, retention, processing, disclosure, destruction, transmittal, storage and audit logging. It covers access controls, password management, firewalls, segregation of duties, and encryption of database, media and communications. The SSP documents the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following NIST, FISMA and DOI security and privacy policies.

For the applications hosted by BSEENet the data is under the control of each system owner who is responsible for protecting the privacy rights of the individuals whose information they collect, maintain, and use in each system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with privacy officials.

All access is controlled by authentication methods to validate the authorized user. All DOI employees and contractors are required to complete annual security and privacy awareness training and sign DOI Rules of Behavior. Personnel authorized to manage, use, or operate the system information are required to take additional role-based training annually.

There is risk associated with offsite backup storage. This risk is addressed through Druva's compliance with FedRAMP requirements for cloud service providers which includes privacy training. Druva regularly undergoes reviews to ensure that all security controls are in place and operating as intended. Druva reports its continuous monitoring assessments to FedRAMP monthly. Druva is rated as FISMA moderate based upon the type and sensitivity of the backup data and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Druva personnel will have no access to backup data from BSEENet nor will they access Administrative logins/passwords.

The risk posed by data on the existing backup tapes will be mitigated by their destruction. Authorized vendors will be onsite to shred the tapes once the Druva online backup is operational. The current backup servers will be taken offline and sanitized using an application called "Kill Disk" that erases the hard drives and destroys all data on them.

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*

Data collected is relevant to perform functions of BSEENet and to support BOEM, BSEE, and ONRR missions.

☐ 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?

Not applicable. BSEENet is not intended to be used in any manner that would allow the system to derive new data or create previously unavailable data.

F. Are the data or the processes being consolidated?

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

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

☒ No, data or processes are not being consolidated.

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

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

Auditors or DOI assessment management group may access the system at least annually or as described in the ISCM Plan. Individual users will have access to their own data.

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

Contractors, system administrators, and auditors are granted access in accordance with mission function. BSEENet uses the principle of least privilege access for authorized users to perform duties. Federal government information is managed and safeguarded by following FISMA, NIST guidelines, and DOI security and privacy policies.

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?*

Privacy clauses were included in the contracts within the BSEENet boundary including but not limited to:

- 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. *Explanation*

☒ No

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

☒ Yes. *Explanation*

BSEENet includes routers, firewalls, and software to establish an audit trail of creation, modification of username of the account that changed the record, and the date and time the record was changed. Logs are only accessed by authorized administrative/manager staff.

☐ No

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

Information collected is used to monitor user access (username) and activity (logins, record changes, deletions, additions, date and time-stamp) for auditing purposes.

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

Access to BSEENet is only provided to necessary authorized employees and is applied on the principle of least privilege to manage access and audit logs. Audit features track user activity and record all changes.

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. Inheriting cloud providers 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. Inheriting cloud providers 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. Inheriting cloud providers 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 Chief, Technical Services Division (TSD) is the BSEENet System Owner. The System Owner oversees and manages the protection of agency information processed and stored on BSEENet. The BSEENet System Owner and Information System Security Officer (ISSO), in collaboration with the BSEE Senior Management Team and BSEE Associate Privacy Officer, are responsible for ensuring adequate safeguards are implemented to protect individual privacy and addressing complaints in compliance with Federal laws and policies for the data managed, used, and stored on BSEENet.

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 BSEENet System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The BSEENet System Owner and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC, the DOI incident reporting portal, in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in consultation with the BSEE Associate Privacy Officer.

The BSEE Incident Response Team handles incidents in accordance with BSEE incident response policy and the DOI Privacy Breach Response Plan, which provides guidance on breach response, the process for timely notification to individuals, and other remedial actions. Druva is required to report any compromise of backup data in their SaaS environment.