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; handwritten 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: Personnel Security System (PSS) Next
Bureau/Office: Bureau of Safety and Environmental Enforcement
Date: April 23 2025
Point of Contact
Name: Dianna Taylor
Title: BSEE 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 Bureau of Safety and Environmental Enforcement (BSEE) is responsible for regulating the offshore energy industry across America's 1.76 billion acres of underwater territory. To effectively meet this challenge, BSEE focuses on building, training, and motivating a skilled team of professionals. The BSEE Personnel Security Branch (PSB) is critical in delivering personnel security services. To support these services, PSB uses the Personnel Security System (PSS) Next, which includes multiple modules hosted on ServiceNow, a cloud-based software-as-a- service (SaaS) platform.

The PSS Next monitors background investigation requests, adjudications, and the approval of logical and physical access to DOI facilities and computer networks. Additionally, it manages national security clearances, including those granted, withdrawn, revoked, or pending reinvestigation.

The system tracks the status of investigations, reinvestigations, and final adjudications while maintaining related records and supporting documents for background investigations and suitability determinations. It also tracks personnel from organizations that BSEE has entered into reimbursable service agreements with, including the Bureau of Ocean Energy Management (BOEM), the DOI Office of the Secretary (excluding the Office of the Chief Information Officer), the Office of Surface Mining Reclamation & Enforcement, Smithsonian Institution personnel security staff, the Advisory Council on Historic Preservation, the Commission of Fine Arts, and the National Gallery of Art.

C. What is the legal authority?

The legal authorities for operation of PSS Next include the following: Executive Order 10450, Security Requirements for Government Employment (April 27, 1953); Executive Order 10865, Safeguarding Classified Information Within Industry (February 20, 1960); Executive Order 12333, United States Intelligence Activities (December 4, 1981); Executive Order 12356, National Security Information (April 2, 1982); Executive Order 12968, Access to Classified Information (August 2, 1995); 5 United States Code (U.S.C) 301- Departmental Regulations (Pub. L. 89-554, 80 Stat. 379); 5 U.S.C. 3301 – Civil service; generally (Pub. L. 89–554, 80 Stat. 417); 5 U.S.C. 9101 – Access to criminal history records for national security and other purposes; 42 U.S.C 2165 – Security restrictions; 42 U.S.C. 2201 – General duties of Commission; 50 U.S.C Chapter 23 - Internal Security; 5 Code of Federal Regulations (CFR) 731 – Suitability; 5 CFR 732 – National Security Positions; 5 CFR 736 - Personnel Investigations. Homeland Security Presidential Directive 12, Policies for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004); and the Federal Information Security Act (Pub. L. 104-106, Sec. 5113). The collection of the Social Security numbers of applicants is authorized by Executive Order 9397 (November 22, 1943)

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: PSS Next leverages the bureau’s use of ServiceNow to initiate and manage background
investigation and onboarding tasks requests.

E. Is this information system registered in Bison +GRC?

☒ Yes: UII Code 10-000001311. The BSEE ServiceNow System Security and Privacy Plan is being updated to reflect the bureau's expanded uses of the ServiceNow Platform
☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

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

☒ Yes: INTERIOR/DOI-45, Personnel Security Program Files - 87 FR 54242 (September 2, 2022), INTERIOR/DOI-46, Physical Security Access Files - 85 FR 3406 (January 21, 2020), and 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) SORNs. Personnel Vetting Records System, DUSDI 02-DoD. (October 17, 2018; 83 FR 52420).The SORNs are available for review on the DOI-wide SORNs Web page.

☐ No

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

☐ Yes:
☒ No: PSS Next does not invoke the Paperwork Reduction Act (PRA). However, information from OF-306, Declaration for Federal Employment, OMB 3206-0182, Expires 10/31/2022, SF-85, Questionnaire for Non-Sensitive Positions OMB No. 3206-026, expires 9/30/2024, Questionnaire for Selected Positions OMB No. 3206-0258 SF-86 expires 6/30/2027.

Section 2. Summary of System Data

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

☒ Name
☒ Citizenship
☒ Sex

☒ Birth Date
☒ Marital Status
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Law Enforcement
☒ Education Information
☒ Driver's License
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information
☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: Previous Background Investigation Types, Assessment Scores, and Adjudication Results

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:
PSS Next accesses the candidate's investigative history in the Central Verification System (CVS), a web-based records system that is controlled by the Defense Counterintelligence and Security Agency (DCSA). PSB reviews the data in CVS to determine whether a new investigation is necessary and updates PSS Next with that investigative history.

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:

When a candidate begins the onboarding process, they provide information to either a Contract Officer's Representative (COR) if the candidate is a contractor or to a Human Resources (HR) specialist for Federal employment, internship or volunteer candidates, or any other category of personnel. This initial collection of information consists of the candidate's resume, a completed Declaration for Federal Employment (OF-306), a signed Release to Obtain a Credit Report, and an investigative request form. The investigative request form is Contractor Request Form (BSEE-5400) for contractors and the HR Background Investigation Check/eAPP/DOI Access Request Form for all others.

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

Data is used to review the candidate's investigative history in Central Verification System (CVS) to determine whether a new investigation is necessary. When a new investigation is necessary, the data from the investigative request package is used by PSB to create a new user account for the candidate in Defense Counterintelligence and Security Agency (DCSA) Electronic Application (eAPP) system. The candidate can then access eAPP to complete the appropriate security questionnaire that is commensurate for the position. The questionnaire is reviewed by PSB before being released to DCSA to conduct the background investigation.

PSS Next is updated to reflect the progress of the candidate's investigative request (e.g., eAPP, etc.), the access credentialing process (e.g., requesting credentials, submitting fingerprints, etc.), and approval to onboard.
Adjudicative determinations made by PSB are documented in the candidate's PSS Next record such as when a candidate is approved to enter on duty based on the advance results of a

background investigation, the approval of access credentials or a final determination regarding the
candidate's suitability based on the full background investigation.

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

☒ Within the Bureau/Office: The advance result of the background investigation and interim determination will be shared with HR and the hiring official, or the COR, as well as other BSEE personnel involved in the onboarding/provisioning process, to notify them that the onboarding process can or cannot continue. Once the full investigation is complete and adjudicated, HR and the candidate are notified of the final determination.

☒ Other Bureaus/Offices: The advance result of the background investigation and interim determination will be shared with HR and the hiring official, or the COR, as well as other BSEE personnel involved in the onboarding/provisioning process, to notify them that the onboarding process can or cannot continue. Once the full investigation is complete, HR is notified of the final determination.

☒ Other Federal Agencies: Information is shared with the Defense Counterintelligence and Security Agency to provide notification on final adjudication of investigations. The advance result of the background investigation and interim determination will be shared with HR and the hiring official, or the COR, of a customer agency, as well as other personnel involved in the onboarding/provisioning process, to notify them that the onboarding process can or cannot continue. Information may be shared with other Federal agencies under the routine uses published in the Interior DOI-45: Personnel Security Program Files system of records notice.

☐ Tribal, State or Local Agencies:

☐ Contractor: Contractor staff providing Personnel Security service have access to PSS Next to fulfill their duties, e.g. creating new entries in PSS Next, updating PSS Next data as candidates' investigations and access credentials are requested. Contractors also provide system and database management support.

☐ Other Third Party Sources:

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

☒ Yes: Although it is an HR specialist or a COR that collects and submits the necessary information to the PSB to initiate the background investigation and credentialing process, the information is, in part, derived from forms that include the requisite Privacy Act Statement which informs the individual that providing the information is voluntary and that the consequence of not providing the requested information may have an impact on the individual’s employment.

☐ No:

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

☒ Privacy Act Statement: PSS Next is an internal web-based system used to collect information to request background investigations and access credentials. A Privacy Act Statement is included on the onboarding forms (e.g., OF 306, Declaration for Federal Employment) which provide the Authority, Purpose, Routine Uses, and Disclosure for collecting the information.

☒ Privacy Notice: Privacy notice is provided through the publication of this PIA, the BSEE ServiceNow PIA, BSEE BOS PIA, INTERIOR/DOI-45, Personnel Security Program Files - 87 FR 54242 (September 2, 2022), 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). The SORNs are available for review on the DOI-wide SORNs Web page.

☒ Other: A warning banner on both the network and PSS Next login screen provides all system users
with privacy and security notices consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance

☐ None

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

PSB personnel can retrieve an individual’s record within PSS Next by searching for their first and last name or social security number.

I. **Will reports be produced on individuals?**

☒ Yes: Ad hoc reports may be generated to audit PSB records, to determine which individuals are due for periodic re-investigations, and to review PSB performance and timeliness. These reports will include name, the risk level and sensitivity of the individual’s position, the individual’s investigative history, employing organization, and clearance level.

Access and changes to PSS Next records are captured in audit logs that are assigned to privileged individuals with appropriate system roles to monitor the audit logs.

☐ No

Section 3. Attributes of System Data

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

PII data is collected from DCSA's CVS to track the investigative cycle for new and re-investigations. This information is an individual's investigative history, i.e. the types of investigations conducted, the dates the investigations were conducted, the adjudicative status of the investigations, and what clearances, if any, were issued, suspended, and/or terminated.

The individual certifies that the information provided is truthful and complete and acknowledges that a false statement may be grounds for an adverse suitability determination to be made, and which may be punishable by a fine or imprisonment. Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information must have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

B. How will data be checked for completeness?

PSB personnel review the documentation for completeness before creating a new record in PSS Next. Attempting to create a PSS Next record with incomplete or missing data results in an error in the system; a new record cannot be created without complete data.

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

PSS Next contains a snapshot of the data at the time the information was certified by an individual as accurate and complete and suitability determination was made. However, PSB personnel update the system to reflect any changes in the progress and status of an investigation and the onboarding process.

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 PSS Next track suitability actions, but do not contain detailed investigation records or suitability determination records. Records are maintained under the Departmental Records Schedule (DRS)-4.1. They are Long-term Administration Records (DAA-0048-2013-0001- 0002). The disposition of these records is temporary and the retention period, 7 years, begins when an individual separates from BSEE or one of the organizations serviced by BSEE. Service Organizations may request BSEE identify the equivalent General Records Schedule citation for the records of the serviced organization.

Records retention periods are also subject to litigation holds, court orders, and preservation notices issued by the Office of the Solicitor and may require the retention of these records past their cutoff 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 Exit Clearance Process outlines the steps and procedures for removing information when employees and contractors separate. When an individual separates from the organization, PSB updates their record in the PSS Next and disposes of the information in accordance with the appropriate records schedule.

BSEE maintains records in accordance with records retention schedules approved by NARA and is responsible for the disposal of the records in accordance with the approved disposition methods, which 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.

There is a moderate risk to individual privacy due to sensitive personally identifiable information contained in the system. PSS Next requires strict security and privacy controls to protect the system's confidentiality, integrity, and data availability. BSEE mitigates the privacy risks throughout the information lifecycle. The potential privacy risks created by BSEE's use of PSS to modernize and manage the delivery of personnel security services include lack of notice, collection of more information than is necessary, collection of inaccurate information, unauthorized disclosure of information, unauthorized access, insider threats, inappropriate use of information, improper storage of information, and retention of data for longer than necessary to accomplish the purpose for which the information was originally collected. Disclosure of data to other agencies and organizations is in accordance with the published DOI-45 system of records notice and is subject to all applicable Federal laws and regulations.

There is a risk that employees and applicants may not receive adequate notice or the opportunity to consent to the use of their information following collection. regarding the purpose, use, maintenance, and dissemination of their information. Individuals are notified at various points of collection that providing information is voluntary but that if they do not consent to the collection of the required information, it may affect the completion of onboarding tasks, including but not limited to their background investigation. Individuals are also provided notice through the publication of this PIA, the ServiceNow PIA, the BOS PIA, and the applicable SORNs published by DOI and DCSA. Individuals do not have the ability, once they have agreed to a background investigation, to consent to some uses of their information and decline to consent to other uses. Individuals are also provided with a current OMB Control Number if the PRA applies to a collection. According to the PRA, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
Inaccurate information may cause individual harm or loss or denial of a benefit. There is a risk of maintaining inaccurate information from applicants that may result in unfavorable adjudicative determinations. This risk is mitigated through established verification procedures to validate that the information submitted is accurate and complete. Applicants under investigation must certify

their information is truthful, complete, and accurate. They acknowledge that any false or incomplete information may delay the investigation or adjudication process and impact their eligibility for a security clearance, resulting in denial of employment, termination, or debarment from Federal employment.HR personnel and CORs provide PSB with accurate and relevant information when initiating a service ticket in the Bureau Onboarding System (BOS).

BSEE mitigates the risks of unauthorized disclosure, access, and insider threats by implementing physical, administrative, and technical safeguards to protect the system and data. When PSS Next becomes inoperable, staff securely store paper records in locked cabinets and display Privacy Act Warning Notices as necessary.

The ServiceNow software is made available to multiple BSEE program offices on individual server sites that are walled off from any other site's content, thus ensuring that one program office cannot access another's information or data without authorization and for a legitimate business purpose. System administrators set user roles to ensure appropriate access and use by authorized personnel with a valid need-to-know to perform official duties.

Additionally, PSS Next users access the instance of ServiceNow using SSO for validation with PIV card authentication, which authenticates privileged users by mapping their AD account information. All system user activity is monitored and logged to ensure only appropriate access to the system and data.

There is a risk that PII may be misused or used for unauthorized purposes. Employees and contractors must also complete Information Management and Technology (IMT) Awareness Training and the Information Systems Security Rules of Behavior Acknowledgement annually before acquiring network and/or system access. IMT Awareness Training includes modules on Cybersecurity, Privacy Awareness, Records Management, Section 508 Compliance, Controlled Unclassified Information, and the PRA. Personnel with significant privacy and security responsibilities must also complete role-based privacy and security training before acquiring network and/or system access and annually thereafter. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions, potential employment termination, and criminal, civil, and administrative penalties.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or the vendor may not handle or store information appropriately according to DOI policy. Contractors must use and store records containing PII in accordance with Federal and DOI requirements. The ServiceNow software is provided and hosted by a FedRAMP-certified service provider and has met all requirements for information categorized as Moderate in accordance with the Federal Information Security Modernization Act. 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. BSEE employees and contractors must promptly report any suspected or confirmed privacy breach. For any suspected or confirmed privacy breach, the BSEE Associate Privacy Officer (APO) will implement the DOI Privacy Breach Response Plan. The BSEE Incident Response Procedures define and document the steps to be taken by the BSEE personnel and its contract staff in the event of a confirmed or suspected privacy breach involving the BSEE network and/or information systems and data will also apply.

Maintaining records beyond the approved retention period or failing to dispose of them properly poses a risk. BSEE mitigates this by managing records in accordance with a NARA-approved records schedule, following established disposition procedures, and requiring PSS Next users to complete IMT Awareness Training and role-based security and privacy training before gaining system 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 data collected is relevant and necessary to perform the functions of PSB, i.e. to request background investigations, manage national security clearances, and request/sponsor access credentials. These functions support the mission of BSEE and the organizations that it services.

☐ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

☐ Yes:

☒ No

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

Not applicable. PSS Next 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.

☒ Yes, processes are being consolidated. PSS Next will streamline processes and modernize employee workflows in the BSEE PSB as a single point of entry to create and manage tickets for background investigation and onboarding tasks.

☐ 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:
PSS Next developers are contractors. Contractors involved with the maintenance of the system and will have limited access to PSS Next data as they provide system support.

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

User access to data stored in the PSS Next is based on the user's job description and need-to-know, as outlined in the BSEE Account Management Procedure and enforced through NIST SP 800-53 security and privacy controls. Access to the PSS Next is restricted to PSB personnel and contract support staff. It is tightly controlled via Active Directory groups, and only a select few, as approved by the Branch Chief of PSB, can access the PSS Next application.

Federal government information is managed and safeguarded by following federal guidelines and DOI security and privacy policies. The final step of the exit clearance process automates the deactivation of a person's network login after Branch Chief, PSB approves removal.

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: All Privacy Act contract clauses are included in the NuAxis contract which supports PSS Next development/maintenance such as:
Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification (Apr 1984)

- FAR 52.224-2, Privacy Act (Apr 1984)
- FAR 52-224-3, Privacy Training
- FAR 52.239-1, Privacy or Security Safeguards (Aug 1996)

☐ 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. System access and changes to PSS Next records are captured in audit logs that are assigned to
privileged individuals with appropriate system roles to monitor the audit logs.

☐ No

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

PSS Next logs every system and record change by capturing the Name, Login ID, timestamp, and modified fields.

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

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems, and other DOI policies are fully implemented to prevent unauthorized monitoring. PSS Next access is limited to authorized personnel and their level of access is based on their need-to-know to perform their official duties. Audit logs are used to prevent unauthorized monitoring. Audit logs are accessible only by system administrators who are responsible for monitoring the audit logs. PSS Next users must complete IMT Awareness Training and the Information Systems Security Rules of Behavior Acknowledgment before acquiring network and/or system access and annually thereafter. Individuals with significant privacy and security responsibilities must also complete annual role-based privacy and security training before acquiring network and/or system access and annually thereafter. Embedded within the Information Systems Security Rules of Behavior is the warning banner which is displayed upon logging into any DOI computer system. The warning banner clearly states all agency computer systems may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. It further states, by logging into an agency computer system, the user acknowledges and consents to monitoring of this system. These security protocols help BSEE monitor user actions for appropriate use and to mitigate the risk of 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 its own FedRAMP certified data centers and implements all the required physical controls.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. ServiceNow maintains its own FedRAMP certified data centers and implements all the required physical controls.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII

☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. ServiceNow maintains its own FedRAMP certified data centers and implements all the required physical 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 Security Branch Manager is the System Manager for PSS Next and is responsible for protecting the privacy rights of the public and employees including addressing Privacy Act and requests for amendment of records. The BSEE Authorizing Official designates an Information System Security Officer (ISSO) who is responsible for monitoring the contractors managing the protection of information processed and stored in PSS Next. The System Owner and the ISSO in collaboration with the BSEE Associate Privacy Officer are responsible for ensuring adequate safeguards are in place to protect individual privacy in compliance with Federal laws and policies.

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 Security Branch Manager is the PSS Next system owner and is responsible for protecting the information it contains. The ISO and ISSO are responsible for the oversight and management of PSS Next security and privacy controls. The PSS Next System Manager and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to the DOI Computer Incident Response Center (DOI-CIRC) within one hour of discovery in accordance with Federal policy and established DOI procedures, as well as working with the BSEE APO to ensure appropriate remedial activities are taken to mitigate any impact to individuals in accordance with the DOI Privacy Breach Response Plan and Federal policy and procedures.

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.