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: Personnel Security System (PSS)
Bureau/Office: Bureau of Safety and Environmental Enforcement (BSEE)
Date: December 17, 2020
Point of Contact:
Name: Rowena Dufford
Title: BSEE Associate Privacy Officer
Email: privacy@bsee.gov
Phone: 703-787-1257
Address: 45600 Woodland Road, Mail Stop: VAE-TSD, Sterling VA 20166

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☒ Volunteers
- ☐ All

☐ No

B. What is the purpose of the system?

The Personnel Security System (PSS) is used by the Personnel Security Branch (PSB) within the Bureau of Safety and Environmental Enforcement (BSEE) to track the progress of background investigation requests and adjudications; track when PSB approves logical and physical access to facilities and computer networks at the Department of the Interior (DOI); and document when national security clearances are granted, withdrawn, revoked or are due for re-investigation. PSS only tracks the status of investigations and reinvestigations, and final adjudications, and does not

contain detailed records or supporting documents on background investigations or suitability determinations. PSS maintains tracking information for personnel from other organizations with whom BSEE has entered into a reimbursable service agreement to provide personnel security services, (i.e. the Bureau of Ocean Energy Management (BOEM), DOI Office of the Secretary (except for the Office of the Chief Information Officer), Office of Surface Mining Reclamation & Enforcement, personnel security staff at the Smithsonian Institute, the Advisory Council on Historic Preservation, the Commission of Fine Arts, and the National Gallery of Art). The system is used to ensure that BSEE's Personnel Security Program is in compliance with re-investigative timelines as mandated by regulations and policy.

PSS is hosted on the BSEE Network (BSEENet) General Support System (GSS) which is a wide area network. BSEENet provides an interconnecting backbone to support a number of business-related and mission-related applications used by BSEE, BOEM, and the Office of Natural Resources Revenue.

C. What is the legal authority?

Executive Orders 10450, 10865, 12333, 12356 and 12968; 5 United States Code (USC) 301, 3301 and 9101; 42 USC 2165 and 2201; 50 USC 781 to 887; 5 Code of Federal Regulations 731, 732, and 736; Homeland Security Presidential Directive 12, Policy 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).

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 CSAM?

☒ Yes: PSS is included in the BSEENet CSAM registration: UII Code 010-000001271; 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.*
None			

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

☒ Yes: DOI-45: HSPD-12: Identity Management System and Personnel Security Files. The SORN may be viewed at https://www.doi.gov/privacy/sorn.

☐ No

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

☐ Yes

☒ No Information in PSS is not collected from members of the Public. However, information from OF-306, Declaration for Federal Employment, is used to populate fields in PSS; OMB 3206-0182, Expires 10/31/2022.

Section 2. Summary of System Data

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

☒ Name
☒ Social Security Number (SSN)
☒ Citizenship
☒ Security Clearance
☒ Birth Date
☒ Personal Email Address
☒ Other Names Used
☒ Employment Information
☒ Place of Birth
☒ 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

PSB accesses the candidate's investigative history in the Central Verification System (CVS), a web-based records system that is controlled by the Office of Personnel Management (OPM). PSB reviews the data in CVS to determine whether a new investigation is necessary and updates PSS 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/e-QIP/DOIAccess 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 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 OPM's Electronic Questionnaires for Investigations Processing (e-QIP). The candidate can then access e-QIP to complete the appropriate security questionnaire that is commensurate for the position. The questionnaire is reviewed by PSB before being released to OPM to conduct the background investigation.

PSS is updated to reflect the progress of the candidate's investigative request (e.g., e-QIP, 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 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 Office of Personnel Management 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 DOI-45: Identity Management System and Personnel Security Files system of records notice, which may be viewed at: https://www.gpo.gov/fdsys/pkg/FR-2007-03-12/html/E7-4407.htm.

☐ Tribal, State or Local Agencies

☒ Contractor:

Contractor staff providing Personnel Security service have access to PSS to fulfill their duties, e.g. creating new entries in PSS, updating PSS 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 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: Users can also view how their information will be used through the publication of this privacy impact assessment and the DOI-45 HSPD-12: Identity Management System and Personnel Security Files system notice, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ Other

☐ 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 are able to retrieve an individual's record within PSS by searching for their 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.

☐ 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 OPM'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.

B. How will data be checked for completeness?

PSB personnel review the documentation for completeness before creating a new record in PSS. Attempting to create a PSS 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 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 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.

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 documents the steps and procedures used to remove information when employees and contractors separate. The records management policies and procedure also govern disposal of information.

When an individual separates from the employing organization, PSB updates that individuals' record in PSS. PSB disposes of PSS information in accordance with the appropriate records schedule, as cited above.

Approved disposition methods for records include shredding or pulping 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.

There is a moderate risk to individual privacy due to the sensitive personally identifiable information contained in the system. There is a risk that DOI will collect more information than is necessary to make appropriate suitability determinations. This risk is mitigated by only requesting the information necessary to effectively meet Federal requirements for background investigations and suitability determinations as part of the onboarding and reinvestigation process.

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. Also, individuals ensure that the information they submit through employment forms is accurate during the investigation process.

There is a risk that unauthorized individuals may access the information in PSS or use it for an unauthorized purpose, or resulting from curiosity browsing by the PSS user population. This risk is mitigated by ensuring effective access controls are implemented, and only authorized personnel are granted access to PSS, and users agree to adhere to the DOI Rules of Behavior. There is also a risk that information in PSS may be used outside the scope of the purpose for which it was collected. This risk is mitigated by the access controls implemented to ensure only authorized personnel have access to the records needed to perform official duties. Therefore access to PSS is limited to PSB employees and contractors. These users have significant information privacy responsibilities so they must complete role-based privacy training every year in addition to the annual Privacy Awareness training.

The privacy risks are mitigated throughout the information lifecycle. Data is collected directly from individuals during the hiring or reinvestigation process. Individuals are provided a Privacy Act statement during the hiring process that explains the authority, purpose, uses and impacts for not providing requested information. 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.

PSS is hosted on the BSEENet General Support System (GSS) which is a wide area network. Access security controls for privacy and information are implemented in compliance with the Privacy Act, Federal Information Security Modernization Act of 2014 (FISMA), OMB Circular A-130, A-123, Managing Information as a Strategic Resource, Management's Responsibility for Internal Controls and NIST 800 -53 - Security and Privacy Controls for Federal Information Systems and Organizations.

Access to PSS is limited to PSB personnel and contract support staff. Access to PSS is tightly controlled using Active Directory groups. Only a few people can access the PSS application as approved by Chief, PSB. The system as a whole, including the PII it maintains, is encrypted and one must be a member of the AD group to be able to access to the system.

PSS follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. Upon the Chief PSB approval, the final step of the exit clearance process is the deactivation of the person's network access.

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 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.

☒ 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:

The PSS web application can only be accessed by members of the "PSS Users" and "PSS Admin" security group. To protect the information transmitted over the network, the system uses encryption certificates from Microsoft RSA SChannel for its encryption.

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

Access to PSS is limited to PSB personnel and contract support staff. Access to PSS is tightly controlled using Active Directory groups. Only a few people can access the PSS application as approved by Chief, PSB.

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 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 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.

☒ No

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

Information is collected by BSEENet to monitor PSS user access (username) and activity (record creations, changes, additions, date and time-stamp) for auditing purposes.

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

Access to PSS is only provided to necessary, authorized employees. Audit features found in BSEENet 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.

(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.

(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.

The PSS web application uses a standard web encryption certificate on SQL Server 2008 and uses Cryptographic service provider: The PSS web site uses current NIST-approved standard web encryption certificate that is issued by DOI and is renewed every two years. We use Microsoft RSA SChannel Cryptographic Provider Bit Length: 4096.The SQL Server databases are backed up daily.

Encrypted backups are transferred to tape which are then stored at Recovery Point in compliance with the records retention schedule.

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, Personnel Security Branch is the System Manager for PSS and is responsible for protecting the privacy rights of the public and employees, including addressing Privacy Act complaints and requests for redress or amendment of records. The BSEE Authorizing Official designates an Information System Security Officer (ISSO) who monitors contractors managing the protection of information processed and stored on PSS. The System Owner and ISSO in collaboration with the BSEE Senior Management Team and BSEE Associate Privacy Officer are responsible for ensuring adequate technical safeguards are in place to protect individual privacy. The PSS System Manager addresses complaints in compliance with Federal laws and policies for the data managed, used, and stored on PSS.

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 Chief, Personnel Security Branch is the PSS system owner and is responsible for protecting the information it contains. The BSEENet System Owner is responsible for daily operational oversight and management of the PSS 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 PSS System Manager and ISSO are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to the 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.