United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Personnel Security Systems 2.0 (PSS 2.0)		**System Owner:** Eileen Arnold	
Preparer: Eileen Arnold		**Office:** EPA/OFA/SIMD/MOB	
Date: 3/11/26		**Phone:** 202-564-1313	
Reason for Submittal:			
New: ☐	Revised: ☐	Annual Review: X	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	Rescindment/Decommission: ☐		

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The Personnel Security System 2.0 (PSS) assists the Security Management Division with tracking the documentation associated with security investigations for Federal and non-Federal personnel working for EPA. This includes reporting requirements that meet the Security Executive Agent Directive (SEAD) 3, which establishes reporting requirements for all "covered individuals" who have access to classified information or who hold a sensitive position. PSS has been updated to support the process of managing and coordinating Insider Threat inquiries. Reporting requirements cover PSS covers individuals who have access to classified information or hold a sensitive position, as well as those personnel in non-sensitive positions.

PSS provides critical data to, or obtains data from, other systems, to ensure effective EPA operations. For

example, PSS integrates with the HRLoB for federal personnel data, with USAccess for PIV card management, with OFA EI eBusiness for provisioning – PSS is a central data point for these and other systems.

EPA developed an Insider Threat Program (ITP) module to manage insider threat inquiries within EPA. The ITP is mandated by Executive Order 13587, which requires Federal agencies to establish an insider threat detection and prevention program. The purpose of the insider threat detection and prevention program is to detect, deter, and mitigate insider threats. EPA will use the PSS to manage and coordinate insider threat inquiries; identify and track potential insider threat inquiries to EPA; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; generate statistical reports and meet other insider threat reporting requirements.

Section 1. Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, sec. 5113)

• Electronic Government Act (Pub. L. 104-347, sec. 203); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)

• Federal Property and Administrative Act of 1949, as amended.

• Title 44 USC section 501.

• Executive Order 12968 - Access to Classified Information

• Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information

• Executive Order 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust

• Executive Order 13526 - Classified National Security Information

• Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

• Executive Order 13764 - Amending the Civil Service Rules of EO 13488 and EO 13467

• Code of Federal Regulations, Title 5, Part 731 - Suitability

• Code of Federal Regulations, Title 5, Part 732 - National Security Positions

• Code of Federal Regulations, Title 5, Part 752 - Adverse Actions

• Code of Federal Regulations, Title 5, Part 1400 - Designation of National Security Positions

• Code of Federal Regulations, Title 32, Part 2001 - Classified National Security Information

• Intelligence Community Directives.

• Security Executive Agency Directives (SEADs).

• Office of Personnel Management's (OPM's) Suitability Handbook.

• OPM Federal Investigations Notices (FINs)

• Government Organization and Employees (5 U.S.C. 301)

• Public Buildings under the control of Administrator of General Services (40 U.S.C. 3101)

• Federal Information Security Management Act of 2002 (44 U.S.C. 3541)

• E-Government Act of 2002 (44 U.S.C. 101)

• Paperwork Reduction Act of 1995 (44 U.S.C. 3501)

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

A system security plan has been completed for this application and the ATO that covers the system expires on August 31, 2028.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FEDRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide? PII data will be stored at the EPA NCC and not in a cloud environment.

PII data will be stored at the EPA NCC and not in a cloud environment

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

PSS contains business information, which includes personal information. All information contained in PSS is for business purposes and is retrieved by a unique personal identifier (PID) (unrelated to their SSN, date of birth or other PII). Access to the information is controlled through role-based user accounts.

A separate module contained within PSS will be utilized specifically for the Insider Threat Program (ITP) inquiries. The following data elements are maintained in the system: Employee name, social security number, date and place of birth, organization, office and home addresses,

office and home and cell phone, job series, pay grade, previous employments, overseas travel, military service, credit information, fingerprint results, OPM's background investigation reports, driver's license information, passport information, photograph, emergency contact, foreign passport, foreign travel, foreign involvement, foreign contacts, ownership of foreign property, bank accounts, arrests in foreign countries, insider threat inquiry summary.

2.2 What are the sources of the information and how is the information collected for the system?

The data maintained in PSS 2.0 is obtained from subjects of a background investigation, individuals interviewed as part of a background investigation or insider threat inquiry, current and prospective EPA personnel, internal EPA systems such as the Human Resources Line of Business (HRLoB) system (EPA–93), external systems such as the General Service Administration (GSA)'s USAccess system (GSA/GOVT– 7), and from other external sources such as vendors, applicants, other federal agencies, other law enforcement systems and other public source materials.

PSS receives a daily download of Federal employee information from Human Resources using a database link. EPA uses the eFile application in Entellitrak to collect contractor personnel data. The data is encrypted both at rest and when moving. DCSA transmits encrypted data files with fingerprint results and background investigation results.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Information is provided by the employee or contractor. Users validate information by matching provided information in two identification documents.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included

Privacy Risk:

The risk that is associated with PSS 2.0 is that it processes a large amount of PII and SPII. Information encoded to the PIV card is collected directly from the individual during the on-boarding process. Information is also retrieved securely from other ISA-sanctioned systems [e.g., eBusiness].

Mitigation:

NIST 800-53 security and privacy controls are applied to PSS 2.0. The accuracy of the data is affirmed during collection from the individual. Privacy risk is significantly lowered as information is collected directly from individuals during the on-boarding process. ISA is in place to ensure implementation of required controls on the interfaces for sharing information. Elevated access requires a dotted account and use of CyberArk for server access.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

Yes, authorized users are granted access to PSS based on their role. The system employs database role-based security, and the organization exercises the principle of least privilege so only the minimum required access rights are applied at the time of request.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

PSS adheres to the EPA Policy and Procedure, CIO 2150.3 EPA Information Security Policy and CIO -P-01.02 Access Control Procedure by controlling and limiting access to those with an operational need to access the information. There are three core sets of user populations:

1. Users with administrative responsibilities for system operation and maintenance of the PSS infrastructure (e.g., System and Database Administrators)

2. Users with privileged application access (e.g., System and Agency Security Officers)

3. PSS Application Role Holders (i.e., non-privileged users) who are provided with access to PSS application for carrying out role-specific functions in EPAs PIV issuance and maintenance lifecycle (e.g., Sponsors, Registrars, and Adjudicators).

Administrative personnel and privileged users are subject to rigorous background checks before they are allowed access to the system. Access is granted and managed by PSS Administrators. A "least-privilege" role-based access system is employed that restricts access to data on a "need-to-know" basis; access to the data is limited to those with an operational need to access the information. Additionally, all web-based access to the application requires PIV-based Multi-Factor Authentication (MFA).

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other components with assigned roles and responsibilities within the system.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

OPM's FSEM-PS will access PSS to review background investigation forms, paperwork and results. They will use secure EPA-approved methods for access to view and update data.

Internal parties include adjudicators, case initiators, HR Shared Service Center (SSC) Managers, HR SSC Specialists, Human Resources Officers, program officers, security. managers, security specialists, Contracting Officers' Representatives, badging office personnel, IT personnel, HSPD-12 support personnel, OECA Inspector Program personnel, OLEM On-Scene Co-Ordinator Program personnel, and Insider Threat Program personnel.

Yes, contractors accessing the system have the appropriate FAR clauses included in the contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The information collected within PSS is maintained in the database according to NARA records retention schedules appropriate to the retention of background investigation related data. Records are kept from one to five years except in cases involving a litigation hold. The following retention schedules apply:

• GRS 2.1, Employee Acquisition Records

• GRS 4.2, Information Access and Protection Records

• GRS 5.6, Security Records.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

There is risk that information is retained beyond the period authorized in the schedules.

Mitigation:

Annual reviews of retention schedules ensure that only necessary information is retained.

Section 4. Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local governments, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes. OPM's FSEM-PS will access PSS to review background investigation forms, paperwork and results. They will use secure EPA-approved methods for access to view and update data.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

External sharing of information to the organizations outside of EPA listed in 4.1 is for the purpose of completing a background investigation.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

Information that is shared within EPA and outside of EPA must have an authorized MOU and/or ISA in place before connections are granted. For inside the organizations, office directors authorize the use of data sharing via an MOU. Data is not shared unless both parties sign the required MOU/ISA. For outside the organization, an MOU/ISA must be in- place and signed by required signatories before connections are tested and/or turned on. Also, the National Privacy Program reviews all external agreements that share PII for reporting purposes.

4.4 **Does the agreement place limitations on re-dissemination?**

Limitations outlined within the contract discuss how the use of information is for the intended purposes, to conduct a background investigation of job applicants.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Background information that we share may be compromised at the recipient agency or contractor's end. Information is shared only in support of background investigations. Minimum insider threat exists.

Mitigation:

ISA is in place that detail the controls to be implemented on the interface at the recipient's end.

Section 5. Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

Risk Management Framework is deployed to manage risk and security information, we conduct assessments, we assess risk periodically, maintain required logging practices, continuously monitor information use and system configuration.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

Employees and contractors take the EPA Annual Information Security and Privacy Awareness Training and Controlled Unclassified Information Awareness Training. A Rules of Behavior (ROB) form contains a thorough list of standards governing the appropriate use of the information system. Prior to accessing PSS, users will be required to read and sign the PSS ROB, which effectively holds users accountable for their actions. As part of the access request process, SMD is responsible for ensuring the ROB is signed by users prior to gaining access.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is a risk related to auditing and accountability, arising from changes to the system configuration and unaccounted information, audit logging Risk of improper/untimely audit is low.

Mitigation:

PSS audit logs are used to enhance the supervision checks and audit trails to report all access and operation of the system. Periodic risk assessments are done. Continuous monitoring and OIG oversight is conducted. PSS collects, stores and transmits only necessary information.

Section 6. Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information

List each use (internal and external to the Department) of the information collected or maintained.
Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The PSS is the Agency personnel security database for all suitability and security background investigations as well as insider threat inquiry management. Collection of PII sensitive data used to process and adjudicate background investigations for EPA personnel.

6.2 How **is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☒ No: ☐ If yes, what identifier(s) will be used.**

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

Personal information can be retrieved based on SSN, name, and date of birth. Data elements that are used are SSN, name, employee ID, and date of birth.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. **What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.**

Administrative & technical controls limiting access through roles and using technical controls using group policy, identity management, logging, auditing and physical control with guarded access to areas that also corelate individual identity management to their physical location and common access card.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. EPA-83

Privacy Risk:

Low risk of data misuse.

Mitigation:

PSS auditing logs are used to enhance the supervision checks and audit trails to report all access and operation of the system. Assessments, continuous monitoring and OIG oversight ensure PII is used as authorized.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of the collection or sharing of their information?

Information collected is based on statutory requirements. Users qualify for employment on grounds that they provide information to facilitate background checks. Applicants do not access PSS 2.0 directly. Federal and non-Federal individuals are provided notice when they provide information via OPM's Electronic Questionnaires for Investigations Processing (e-QIP), which is a required form when onboarding at federal agencies. They also receive additional notice on the OF- 306 form they are required to complete.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information.

Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

There is risk that individuals provide information without knowing their rights, but a risk is that individuals do not know the extent of use and that the individual will not know that information collected by PSS will be used in other systems that interface with PSS.

Mitigation:

Individuals are notified of their rights in all forms that collect information and are made aware that eligibility for jobs depends on providing required information. EPA ensures proper handling of that information. The PIA and the very nature of PSB provide notice to EPA employees and POCs provide notice to non-federal personnel that information collected is needed for employment and will be used by PSS for required business functions.

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

Risk that individuals are not fully aware of the scope of their data subject rights under the Privacy Act. The risk is that the data may be incorrect or misused.

Mitigation:

Forms of redress are identified and explained on the Standard Forms that personnel complete during the onboarding process. EPA's public-facing portal provides information on the modernized Privacy Act Request Procedure that allows for digital applications.

I attest as the Agency Privacy Officer that **Personnel Security Systems 2.0 (PSS 2.0)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

ROBERT KELLY
Digitally signed by ROBERT KELLY
Date: 2026.09.04 14:58:11 -04'00'

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt Branch
EPA/OFA