United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 08/2018)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance contact your LPO.

System Name: Personnel Security Systems (PSS) 2.0	
Preparer: Carlos R. Rivera	**Office:** Security Management Division SMD) Office of Administration (OA) Office of Mission Support (OMS)
Date: June 21, 2019	**Phone:** (202) 564-1806
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☒ Implementation ☐	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **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 (PSS) 2.0 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 2.0 has been updated to support the process of identifying and mitigating Insider Threats at federal agencies. Reporting requirements of PSS 2.0 covers individuals who have access to classified information or hold a sensitive position, as well as those personnel in non-sensitive positions.

PSS 2.0 provides critical data to, or obtains data from, other systems, to ensure effective EPA operations. For example, PSS 2.0 integrates with the HRLoB for federal personnel data, with USAccess for PIV card management, with OMS EI eBusiness for provisioning – PSS 2.0 will become a central data point for these and other systems.

Section 1.0 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 will be completed for this application and there will be an ATO

issued to cover the system. The planned authorization date is August 2019.

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.

Section 2.0 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 2.0 contains business information, which includes personal information. All information contained in PSS 2.0 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.

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.

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

PSS 2.0 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. OPM 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.

Role-based access is used to ensure only authorized users are allowed access. Users must be familiar with the application they are using to ensure data entered is accurate. Because information is provided by the employee or contractor, this ensures that the most relevant, up to data and accurate information exists.

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:

Privacy and mitigation risk are considered moderate for PSS 2.0. If for some reason, information cannot be collected, the integrity of existing data will not be impacted.

Mitigation:

All administrators are required to have a high-level background investigation due to the nature of information that is viewable.

Section 3.0 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 2.0 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 What procedures are in place to determine which users may access the information and how does the system determine who has access?

PSS 2.0 adheres to the EPA Policy and Procedure, CIO 2150.3 EPA Information Security Policy and CIO -P-01.02 Access Control Procedure by controlling an 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 2.0 infrastructure (e.g., System and Database Administrators)

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

3. PSS 2.0 Application Role Holders (i.e. non-privileged users) who are provided access to PSS 2.0 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 2.0 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 require 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 2.0 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, and IT 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 2.0 is maintained in the database according to NARA records retention schedules appropriate to the retention of background investigation related data. The record control schedule established for this system follows the record schedule 0740, Office of Administrative Services Information System (OASIS).

The record control schedule established for this system follows the record schedule 0740, Office of Administrative Services Information System (OASIS).
https://www.epa.gov/sites/production/files/2019-05/documents/20190308_epa_records_schedules_in_final_status.pdf

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:

Records are stored in the PSS 2.0 database according to NARA records retention schedules appropriate to the retention of background investigation related data.

Mitigation:

Review data regularly to determine whether the information is still relevant and necessary.

Section 4.0 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 government, 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.

OPM's FSEM-PS will access PSS 2.0 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 are for the purposes 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 (NPP) should review all external agreements that share PII for reporting purposes.

4.4 Does the agreement place limitations on re-dissemination?

Limitations outlined within the contract discusses how the use of information is for the intended purposes, to conduct a background investigation on 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:

Information is shared outside the Agency for intended purposes as stated above.

Mitigation:

PII data is encrypted and stored and forwarded to OPM for processing. MOUs and ISAs are in place with external parties to share information and provide required services.

Section 5.0 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 in accordance with stated practices in this PIA?

PSS 2.0 ensures that the information is used for its intended purposes by limiting access to the information collected.

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 Privacy and Information Security Awareness Training. A Rules of Behaviour (ROB) form contains a thorough list of standards governing the appropriate use of the information system. Prior to accessing PSS 2.0, users will be required to read

and sign the 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

Privacy Risk:

None.

Only individuals who have the proper authorization and who perform functions related to PSS 2.0 can access any information. Each individual is assigned a role that gives him or her access limited only to the data he or she needs to perform his or her job function. PSS 2.0 auditing logs are used to enhance the supervision checks and audit trails to report all access and operation of the system.

Mitigation:

None

Section 6.0 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.

The Personnel Security System (PSS) is the Agency personnel security database for all suitability and security background investigations. 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 _X_ 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 Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EPA-83

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.

Privacy Risk:

None.

Privacy notifications are stated within each support contract as well as any Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA). Security controls used to protect personal sensitive data in PSS 2.0 are commensurate with those required for an information system rated MODERATE for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 3.

Privacy notifications are stated within each support contract as well as any Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA). Security controls used to protect personal sensitive data in PSS 2.0 are commensurate with those required for an information system rated MODERATE for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

None

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 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.

Federal and non-Federal individuals are provided notice when they provide information via OPM's Electronic Questionnaires for Investigations Processing (e-QIP). They also receive additional notice on the OF-306 form they are required to complete.

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. Individuals do not access PSS 2.0 directly.

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:

None. PSS 2.0 employs monitors and filters to identify and block unauthorized attempts to upload or change information, cause disruptions or interruptions of service, or otherwise cause damage to information.

Mitigation:

None

Section 8.0 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?

Record Access Procedure: Requests for access must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16. Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances.

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

8.3 How does the system notify individuals about the procedures for correcting their information?

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA Privacy Officer, MC2831T, 1200 Pennsylvania Avenue, N.W., Washington, DC 20460.

8.4 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 FOIA.

Privacy Risk:

None. Risks evaluated:

- Laws and regulations are violated as a result of individuals not having the ability to access their personal information as stored by the agency.
- Laws and regulations are violated as a result of individuals not having the ability to choose how their personal information is to be used.
- Violations to privacy laws, and regulations cannot be enforced due to ill-defined policy.
- The extent of a security breach of personal information and possible damage(s) may not be identified

Mitigation:

None