



ENVIRONMENTAL PROTECTION AGENCY

[FRL-10082-02-OMS]

Privacy Act of 1974; System of Records

AGENCY: Security Management Division, Environmental Protection Agency (EPA).

ACTION: Notice of a modified system of records.

SUMMARY: The U.S. Environmental Protection Agency's (EPA or Agency) Personnel Security Branch (PSB) is giving notice that it proposes to modify a system of records pursuant to the provisions of the Privacy Act of 1974. The Personnel Security System (PSS) 2.0 is being modified to include a new module, which the Agency will use to administer its Insider Threat Program. The new module will collect records about individuals to assist the Agency with insider threat inquiry management and coordination. The module will retain insider threat inquiry-related data and help EPA personnel coordinate responses to those inquiries. Collecting this data ensures the effective and timely processing of records.

DATES: Persons wishing to comment on this system of records notice must do so by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Submit your comments, identified by Docket ID No. EPA-HQ-OMS-2019-0371, by one of the following methods:

Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the online instructions for submitting comments.

Email: docket_oms@epa.gov. Include the Docket ID number in the subject line of the message.

Fax: (202) 566-1752.

Mail: OMS Docket, Environmental Protection Agency, Mail Code: 2822T, 1200 Pennsylvania Ave., NW, Washington, D.C. 20460.

Hand Delivery: OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW, Washington, D.C. 20460. Such deliveries are only accepted during the Docket's normal hours of operation, and special arrangements should be made for deliveries of boxed information.

Instructions: Direct your comments to Docket ID No. EPA-HQ-OMS-2019-0371. The EPA's policy is that all comments received will be included in the public docket without change and may be made available online at <https://www.regulations.gov>, including any personal information provided, unless the comment includes information claimed to be Controlled Unclassified Information (CUI) or other information for which disclosure is restricted by statute. Do not submit information that you consider to be CUI or otherwise protected through <https://www.regulations.gov>. The <https://www.regulations.gov> website is an "anonymous access" system for the EPA, which means the EPA will not know your identity or contact information. If you submit an electronic comment, the EPA recommends that you include your name and other contact information in the body of your comment. If the EPA cannot read your comment due to technical difficulties and cannot contact you for clarification, the EPA may not be able to consider your comment. If you send an e-mail comment directly to the EPA without

going through <https://www.regulations.gov>, your e-mail address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Electronic files should avoid the use of special characters, any form of encryption, and be free of any defects or viruses. For additional information about the EPA public docket, visit the EPA Docket Center homepage at <https://www.epa.gov/dockets>.

Docket: All documents in the docket are listed in the <https://www.regulations.gov> index. Although listed in the index, some information is not publicly available, e.g., CUI or other information for which disclosure is restricted by statute. Certain other material, such as copyrighted material, will be publicly available only in hard copy. Publicly available docket materials are available either electronically in <https://www.regulations.gov> or in hard copy at the OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW, Washington, D.C. 20460. The Public Reading Room is normally open from 8:30 a.m. to 4:30 p.m., Monday through Friday excluding legal holidays. The telephone number for the Public Reading Room is (202) 566-1744, and the telephone number for the OMS Docket is (202) 566-1752. Further information about EPA Docket Center services and current operating status is available at <https://www.epa.gov/dockets>.

FOR FURTHER INFORMATION CONTACT: John Goldsby, Branch Chief, Personnel Security Branch, Environmental Protection Agency, William Jefferson Clinton North Building, Mail Code 3206A, 1200 Pennsylvania Avenue, NW, Washington, D.C. 20460; telephone number: (202) 564-1569; email address: Goldsby.John@epa.gov.

SUPPLEMENTARY INFORMATION: Currently, EPA's Personnel Security Branch (PSB) uses PSS 2.0 to track and maintain background investigation documents for federal and non-federal personnel working for EPA. This includes background investigation documents for all

“covered individuals” who have access to classified information or who hold a sensitive position. EPA is required to maintain this information for the employee onboarding process, and to manage background investigations for personnel during their time at the EPA (i.e., when there are promotions, position changes, etc.).

PSB is adding a new Insider Threat module to PSS 2.0 that provides EPA with insider threat inquiry management and coordination capabilities. Specifically, the Agency is modifying PSS 2.0 to include an inquiry management function to maintain and safeguard insider threat-related data. PSS 2.0 will also allow the Agency to easily share necessary information with authorized personnel to conduct insider threat inquiries. The insider threat module will contain records derived from EPA security incidents, summaries, or reports containing information about potential insider threats or the data loss prevention program; information related to analytical efforts by EPA insider threat personnel; reports about potential insider threats obtained through the management and operation of the EPA Insider Threat Program; and reports about potential insider threats obtained from other Federal Governments sources. The records contained in this system could include information related to actual, potential, or alleged criminal, or administrative violations and law enforcement actions.

The insider threat module will contain information relevant to insider threat inquiries on cleared individuals with access to EPA resources, including facilities, information, equipment, networks, and systems. The insider threat module may also contain information obtained as a result of a background investigation conducted on cleared personnel. Further, at a later date, and once relevant authorities are updated, the insider threat module will also contain information on uncleared individuals with access to EPA resources.

SYSTEM NAME AND NUMBER: Personnel Security System (PSS) 2.0, EPA-83.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: The system will be managed by the Personnel Security Branch, Environmental Protection Agency, 1301 Constitution Ave. NW, Washington, D.C. 20460. Electronically stored information is hosted at the EPA National Computer Center (NCC), 109 TW Alexander Drive, Research Triangle Park, Durham, NC 27711.

SYSTEM MANAGER(S): John Goldsby, Branch Chief, Personnel Security Branch, Environmental Protection Agency, William Jefferson Clinton North Building, Mail Code 3206A, 1200 Pennsylvania Avenue, NW, Washington, D.C. 20460; Telephone Number: (202) 564-1569; Email address: goldsby.john@epa.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Executive Order 13467, Reforming Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters *as amended*; Code of Federal Regulations 5, Parts 731 (Suitability), 732 (National Security Positions), 736 (Personnel Investigations), and 1400 (Designation of National Security Positions in the Competitive Service, and Related Matters); 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 13741 – Amending EO 13467 To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; Executive Order 13764 – Amending the Civil Service Rules, Executive Order 13488; EO 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and

Credentialing, and Related Matters; Responsibilities for the Maintenance of Records About Individuals by Federal Agencies [OMB Circular A-108, as amended]; Trusted Workforce 2.0, Managements Responsibility for Internal Control [OMB Circular A-123, Revised 12/21/04]; Managing Information as a Strategic Resource [OMB Circular A-130]; Records Management by Federal Agencies [44 USC 31]; Federal Information Security Modernization Act (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504).

PURPOSE(S) OF THE SYSTEM: The purpose of PSS 2.0 is to assist PSB with coordinating and managing background investigations on federal and non-federal personnel working for EPA by collecting, maintaining, and tracking the documentation associated with such background investigations. Data in the system will be transferred to the identity card management provider so that access cards can be issued to personnel. The data in the system will also be used by the Agency to start the employee onboarding process, and to manage personnel throughout their employment at EPA. Additionally, the insider threat module will be used by OHS to collect information on individuals, relevant to insider threat inquiries. EPA will use the insider threat module to manage information related to the inquiries, and support EPA's responses to such inquiries.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Federal employees, contractors, grantees, students, interns, volunteers, other non-federal employees, and individuals formerly in any of these positions including individuals who require access to EPA-controlled facilities, information technology systems, or information classified in the interest of national

security, and applicants for employment or to work on a contract, grant or other activity for the Agency.

CATEGORIES OF RECORDS IN THE SYSTEM: Information in the system may include: an individual's first, middle, and last name; social security number (SSN); date and place of birth; employment organization; office and home addresses; office, home, and cell phone numbers; job series; pay grade; current and previous employment details; dates and locations of overseas/foreign travel; military service information; financial and credit information; court documents; biometric data including fingerprint results; Office of Personnel Management's or Defense Counterintelligence and Security Agency's background investigations; driver's license information; passport and visa information; photographs; emergency contacts; business or other involvement with foreign governments or foreign nationals; foreign contacts; ownership of foreign property information; foreign bank account information; information on arrests in foreign countries; and insider threat inquiry details.

RECORD SOURCE CATEGORIES: 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.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: The routine uses below are both related to and compatible with the original purpose for which the information was collected.

General routine uses A, B, C, D, E, F, G, H, I, J, K, L, and M apply to this system (86 FR 62527).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: These records are maintained electronically on computer storage devices located at the EPA National Computer Center (NCC), 109 TW Alexander Drive, Research Triangle Park, Durham, NC 27711.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Personal information may be retrieved using an individual's SSN, name, date of birth, email address, personal identification number or background investigation case number. The SSN is used in the Suitability, Credentialing and Security Executive Agents' systems, and is therefore used as the connecting data to enable the various systems to communicate with each other and transfer data when needed. PSS 2.0 displays a reminder about the appropriate PII and SPII handling procedures every time a user begins to enter data for a new background investigation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with National Archives and Records Administration (NARA) records retention schedules appropriate to the retention of background investigation related data, as well as EPA's Records Schedules 100 & 1008.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: 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, "Security and Privacy Controls for Information Systems and Organizations," Revision 5.

1. Administrative Safeguards: Personnel are instructed to lock their computer when they leave their desks. Personnel are regularly reminded about appropriate sensitive personally identifiable

information (SPII) and personally identifiable information (PII) handling procedures. All personnel are required to take annual Information Technology Security and Privacy Training. In addition to the agency's Rules of Behavior, PSS 2.0 users are required to sign a PSS 2.0-specific Rules of Behavior document prior to their access being granted to the system.

Additionally, Contracting Officer's Representatives will also be required to review and understand PSS 2.0 user guides, which explain how SPII / PII should be handled.

2. *Technical Safeguards:* Electronic records are maintained in a secure, password-protected environment. Access to records is limited to those who have a need to know. Electronic records are restricted to authorized users with appropriate security privileges, including the use of 2-factor PIV Card authentication and permission level assignments. After 15 minutes of inactivity, a user is automatically logged out of the system. Additionally, PSS 2.0 displays a reminder about the appropriate PII and SPII handling procedures each time a user begins to enter data for a new background investigation.

3. *Physical Safeguards:* All records are maintained in secure, access-controlled areas or buildings. EPA employees and contractors involved in the management, design, development, implementation, and execution of the program will have monitored access to the application. Only individuals who have the proper authorization and who perform functions related to PSS 2.0 are allowed to access information.

RECORD ACCESS PROCEDURES:

Pursuant to 5 U.S.C. 552a(k)(2), certain records maintained in PSS 2.0 are exempt from specific access and accounting provisions of the Privacy Act. See 40 CFR 16.12. However, EPA may, in its discretion, grant individual requests for access if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect. Requests for access

must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16.

Specifically, all requests for access to personal records should cite the Privacy Act of 1974 and reference the type of request being made (i.e., access). Requests must include: (1) the name and signature of the individual making the request; (2) the name of the Privacy Act system of records to which the request relates; (3) a statement whether a personal inspection of the records or a copy of them by mail is desired; and (4) proof of identity. A full description of EPA's Privacy Act procedures for requesting access to records is available at 40 CFR Part 16.

CONTESTING RECORD PROCEDURES: Pursuant to 5 U.S.C. 552a(k)(2), certain records maintained in PSS 2.0 are exempt from specific correction and amendment provisions of the Privacy Act. See 40 CFR 16.12. However, EPA may, in its discretion, grant individual requests for correction and amendment if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect. Requests for correction and amendment must identify the record to be changed and the corrective action sought and must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16.

NOTIFICATION PROCEDURES: Pursuant to 5 U.S.C. 552a(k)(2) and (k)(5), certain records maintained in PSS 2.0 are exempt from specific notification provisions of the Privacy Act. See 40 CFR 16.12. However, EPA may, in its discretion, grant individual notification requests if it determines that notification will not interfere with an interest that the exemption is intended to protect. Generally, individuals who wish to be informed whether a Privacy Act system of records maintained by EPA contains any record pertaining to them, should make a written request to the EPA, Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW, Washington,

D.C. 20460, or by email at: privacy@epa.gov. A full description of EPA's Privacy Act procedures is included in EPA's Privacy Act regulations at 40 CFR part 16.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Under 5 U.S.C. 552a (k)(2), certain records in PSS 2.0 are exempt from the following provisions of the Privacy Act of 1974, as amended, subject to the limitations set forth in this subsection: 5 U.S.C. 552a(c)(3); (d); (e)(1). In particular, the following types of records in PSS 2.0 are exempt from the aforementioned provisions under subsection (k)(2): (1) background investigation records compiled to investigate personnel/an applicant that is/would be responsible for law enforcement and/or national security matters; 2) background investigation records compiled to investigate personnel suspected of illegal or inappropriate activity; 3) information compiled to identify potential insider threats and facilitate insider threat inquiries; 4) information compiled to identify patterns of illegal activity, or that may form the predicate or be the catalyst of a law enforcement investigation; and 5) information otherwise compiled to identify violations of law or national security breaches. However, if any individual is denied a right, privilege, or benefit to which the individual would otherwise be entitled by Federal law or for which the individual would otherwise be eligible, access will be granted, except to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality. Further, under 5 U.S.C. 552a(k)(5), investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information that, if disclosed, would reveal the identity of a confidential source is exempt from 5 U.S.C. 552a (c)(3) and (d), subject to the limitations set forth in the subsections.

EPA may maintain in PSS 2.0 records obtained from other agencies or components, which have exempted those records from certain Privacy Act requirements under 5 U.S.C. 552a (j) and (k). As such records do not lose exempt status when added to another system, these records will continue to be exempt in PSS 2.0 on the same basis and from the same requirements as in the source system. Although certain records in PSS 2.0 have been exempted from certain provisions of the Privacy Act, EPA may, in its discretion, fully grant individual requests for access and correction if it determines that the exercise of these rights will not interfere with an interest that the exemption is intended to protect. However, if any individual is denied any right, privilege, or benefit that they would otherwise be entitled by federal law, or for which they would otherwise be eligible, as a result of the maintenance of these records, the records shall be provided to the individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence.

HISTORY: 85 FR 32380 (May 29, 2020).

Vaughn Noga,

Senior Agency Official for Privacy.

[FR Doc. 2023-24492 Filed: 11/3/2023 8:45 am; Publication Date: 11/6/2023]