6560-50-P

ENVIRONMENTAL PROTECTION AGENCY

[FRL-10009-74-OMS]

Privacy Act of 1974; System of Records

AGENCY: Office of Mission Support, Environmental Protection Agency (EPA).

ACTION: Notice of a New System of Records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, the Office of Mission Support (OMS) gives notice that it proposes to create a new system of records for the Personnel Security System (PSS) 2.0. OMS is replacing the current PSS (1.0), which is a module of the Office of Administrative Services Information System (OASIS, EPA-41), with a new stand-alone system, PSS 2.0, outside of the OASIS portal. All exemptions and provisions included in the SORN for PSS 1.0 under the OASIS portal will transfer to the new SORN for PSS 2.0.

DATES: Persons wishing to comment on this system of records notice must do so by **[INSERT 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**. New routine uses for this new system of records will be effective **[INSERT 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

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

Regulations.gov: www.regulations.gov Follow the online instructions for submitting comments

Email: oei.docket@epa.gov

Fax: 202-566-1752.

Mail: OMS Docket, Environmental Protection Agency, Mailcode: 2822T, 1200 Pennsylvania Ave., NW., Washington, DC 20460.

Hand Delivery: OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW, Washington, DC. 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 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 www.regulations.gov. The www.regulations.gov website is an "anonymous access" system for EPA, which means the EPA will not know your identity or contact information unless you provide it in the body of your comment. Each agency determines submission requirements within their own internal processes and standards. EPA has no requirement of personal information. If you send an e-mail comment directly to the EPA without going through 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. 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. 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's public docket visit the EPA Docket Center homepage at http://www.epa.gov/epahome/dockets.htm.

Docket: All documents in the docket are listed in the 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 www.regulations.gov or in hard copy at the OMS Docket, EPA/DC, WJC West Building, Room 3334, 1301 Constitution Ave., NW., Washington. DC. The Public Reading Room is 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.

FOR FURTHER INFORMATION CONTACT: Jon Ross, Office of Mission Support, Environmental Protection Agency, William Jefferson Clinton North Building, Mailcode 3206A, 1200 Pennsylvania Avenue, N.W., Washington, DC 20460; telephone number, (202) 564-6153; e-mail address, Ross.Jon@epa.gov.

SUPPLEMENTARY INFORMATION: The Office of Mission Support (OMS) plans to replace the current PSS (1.0), which is a module of OASIS (EPA-41), with a new system, PSS 2.0, outside of the OASIS portal. OMS is creating a stand-alone Privacy Act system of records for the Personnel Security System (PSS) 2.0. All exemptions and provisions included in the SORN for PSS 1.0 under the OASIS portal will transfer to the new SORN for PSS 2.0. Details regarding the system of records are contained in this Federal Register Notice. The PSS 2.0 assists the Security Management Division (SMD) 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. Access to the system is restricted to authorized users and will be maintained in a secure, password protected computer system, in secure areas and buildings with physical access controls and environmental controls. In the performance of their official duties, EPA federal personnel must input and manage Sensitive Personally Identifiable Information (such as SSN) and Personally Identifiable Information (such as home address and email address). The data is required in the system to start the onboarding process and to manage personnel through lifecycle activity at EPA (such as background investigations).

System Name and Number: Personnel Security System (PSS) 2.0 – EPA-83

Security Classification: Unclassified

System Location: National Computer Center (NCC), 109 TW Alexander Drive, Research Triangle Park, Durham, NC 27711.

System Manager (s): Jon Ross, Security Management Division, Environmental Protection Agency, William Jefferson Clinton North Building, Mailcode 3206A, 1200 Pennsylvania Avenue, N.W., Washington, DC 20460; telephone number, (202) 564-6153; e-mail address, Ross.Jon@epa.gov.

Authority for Maintenance of the System: 5 U.S.C. 301; 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); and the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); Federal Property and Administrative Act of 1949, as amended.

Purpose of the System: The purpose of the Personnel Security System is to assist the members of the Security Management Division with tracking the documentation associated with background investigations for potential and current Federal and non-Federal personnel working for EPA.

Categories of Individuals Covered by the System: Individuals who require access to EPA-controlled facilities, information technology systems, or information classified in the interest of national security, including applicants for employment or to work on a contract, grant etc. Federal employees, contractors, grantees, students, interns, volunteers, other non-Federal employees and individuals formerly in any of these positions. The system does not apply to occasional visitors or short-term guests to whom the Agency will issue temporary identification.

Categories of Records in the System: Employee name, social security number (SSN), 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, foreign bank accounts and arrests in foreign countries.

Record Source Categories: The sources of data within PSS 2.0 are from internal EPA systems such as the Human Resources Line of Business (HRLoB) and the General Service Administration (GSA) external system, USAccess, and from external sources such as vendors, applicants and onboard personnel. The HRLoB SORN is EPA-1 and the USAccess SORN is GSA/GOVT-7.

Routine Uses of Records Maintained in the System, including Categories of Users and Purposes of Such Uses: The following routine uses 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, and K apply to this system (73 Fed Reg 2245). In addition, the two routine uses below (L and M) are required by M-17-12.

L. Disclosure to Persons or Entities in Response to an Actual or Suspected Breach of Personally Identifiable Information. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that there has been a breach of the system of records, (2) the Agency has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Agency (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Agency's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

M. Disclosure to assist another agency in its efforts to respond to a breach. To another Federal agency or Federal entity, when the Agency determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Policies and Practices for Storage of Records: The information collected within PSS 2.0 is maintained and stored in the database located at NCC. These records are maintained electronically on computer storage devices such as computer tapes and disks. Backup will be

maintained at a disaster recovery site. Computer records are maintained in a secure password protected environment. Access to computer records is limited to those who have a need to know. Permission level assignments will allow users access only to those functions for which they are authorized. All records are maintained in secure, access-controlled areas or buildings.

Policies and Practices for Retrieval of Records: Personal information will be retrieved by SSN, name, date of birth, email address, personal identification number or background investigation case number.

Policies and Practices for Retention and Disposal of Records: Records are retained and disposed of in accordance with NARA records retention schedules appropriate to the retention of background investigation related data, as well as EPA's Records Schedule 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, "Recommended Security Controls for Federal Information Systems," Revision 4.

Administrative Safeguards: Access to PSS 2.0 requires two-factor authentication accomplished by using Personal Identity Verification (PIV) cards that are issued to all personnel based on the requirements of Homeland Security Presidential Directive 12 (HSPD 12).

When a user is logged into PSS 2.0, they are asked by the system to confirm that they still want to remain logged in. If there is no response, or after 15 minutes of inactivity, the user is automatically logged out of the system. Personnel are instructed to lock their computer when they leave their desks. Personnel receive annual Privacy Act awareness training and are regularly reminded about appropriate SPII and PII handling procedures.

In addition to the agency's Rules of Behavior and Privacy Act training that personnel undergo, PSS users are required to sign a PSS-specific Rules of Behavior document prior to their access being granted to the system.

Contracting Officer's Representatives (CORs) will be receiving SPII / PII as a normal part of their operations. The COR's user guide provides confirmation of how SPII / PII should be handled, and the following is an excerpt of that guide:

> "BE AWARE THAT YOU ARE HANDLING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (SPII) and need to do so under the following guidelines, which will help prevent privacy breaches by ensuring the COR, who has a need to know the information, is the only individual to see the PII/SPII:
>
> - The COR will instruct the vendor to send the requested information (name, email address, SSN) by email with the COR as the only EPA email recipient.
> - The COR will enter the information into PSS 2.0 and will then delete the email.
> - To properly delete the email, press the Shift key and the Delete key at the same time – this will fully remove the email, so it isn't even in the Deleted Items folder.
> - If the COR replies to the email, the COR will ensure that all SPII and PII in their email response is removed prior to hitting Send.
> - The COR will not save or print the email in any form.
> - The COR will not forward the email to others."

Technical Safeguards: Access to the data is strictly controlled and is limited to those with an operational need to access the information. 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 requires multi-factor authentication.

Physical Safeguards: 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 any information. Entry to the EPA facility and within the facility to specific spaces at the NCC is achieved using HSPD-12 PIV cards on door readers. PIV cards are only issued to personnel who have met EPA's initial security screening requirements. Security Guards at all entrances confirm that the PIV card is valid, unexpired and reflects the identity of the card holder. Entry to the server rooms is only available to personnel using their PIV cards on door readers, where those personnel have been approved for elevated access (meaning they have undergone a more rigorous security screening). The NCC maintains an Access Control List to ensure access to server rooms is limited to approved personnel only.

Record Access Procedures: Any individual who wants access to his or her record, should make a written request to the EPA Attn: Privacy Officer, MC2831T, 1200 Pennsylvania Avenue, N.W., Washington, DC 20460.

Contesting Record Procedures: 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.

Notification Procedure: 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 EPA, Attn: Privacy Officer, MC2831T, 1200 Pennsylvania Avenue, NW., Washington, DC 20460.

Exemptions Promulgated for the System: Under 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), the Personnel Security System is 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)(2),

(d)(3), and (d)(4); (e)(1), and (f)(2) through (5). Although the Personnel Security System has been exempted, 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.

History: The security files were previously covered under Office of Administrative Services Information System (OASIS) EPA 41 Federal Register (FR) Volume 71, Number 169, FR DOC No: 06-7319 until 2019 and is being transferred to this existing PSS 2.0 SORN to include all exemptions and provisions.

Vaughn Noga,

Senior Agency Official for Privacy.

[FR Doc. 2020-11356 Filed: 5/28/2020 8:45 am; Publication Date: 5/29/2020]