GENERAL SERVICES ADMINISTRATION

[Notice-2015-ISP-2015-02; Docket No. 2015-0002; Sequence 2]

Privacy Act of 1974; Notice of an Updated System of Records

AGENCY: Office of the Chief Information Officer; General Services Administration.

ACTION: Updated Notice.

SUMMARY: GSA proposes to update a system of records subject to the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

DATES: Effective: **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: GSA Privacy Act Officer (ISP), General Services Administration, 1800 F Street NW, Washington, DC 20405.

FOR FURTHER INFORMATION CONTACT: Call the GSA Privacy Act Officer at 202-368-1852 or email gsa.privacyact@gsa.gov.

SUPPLEMENTARY INFORMATION: GSA is updating a system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. The notice provides updated information. Nothing in the notice will impact individuals' rights to access or amend their records in the systems of records.

DATED: October 16, 2015.

David A. Shive,
Chief Information Officer,
Office of GSA IT (I).

[Billing Code: 6820-38]

GSA/GOVT-7

SYSTEM NAME: HSPD-12 USAccess.

SYSTEM LOCATION: Records covered by this system are maintained by a contractor at the contractor's site.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The Personal Identity Verification Identity Management System (PIV IDMS) records will cover all participating agency employees, contractors and their employees, consultants, and volunteers who require routine, long-term access to federal facilities, information technology systems, and networks. The system also includes individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.). At their discretion, participating Federal agencies may include short-term employees and contractors in the PIV program and, therefore, inclusion in the PIV IDMS. Federal agencies shall make risk-based decisions to determine whether to issue PIV cards and require prerequisite background checks for short-term employees and contractors. The system does not apply to occasional visitors or short-term guests. GSA and participating agencies will issue temporary identification and credentials for this purpose.

CATEGORIES OF RECORDS IN THE SYSTEM: Enrollment records maintained in the PIV IDMS on individuals applying for the PIV program and a PIV credential through the GSA HSPD-12 managed service include the following data fields: Full name; Social Security Number; Applicant ID number, date of birth; current address; digital color photograph; fingerprints; biometric template (two fingerprints); organization/office of assignment; employee affiliation; work e-mail address; work telephone number(s); office address; copies of identity source documents; employee status; military status; foreign national status; federal emergency response official status; law enforcement official status; results of background check; Government agency code; and PIV card issuance location. Records in the PIV IDMS needed for credential management for enrolled individuals in the PIV program include: PIV card serial number; digital certificate(s) serial number; PIV card issuance and expiration dates; PIV card PIN; Cardholder Unique Identifier (CHUID); and card management keys. Agencies may also choose to collect the following data at PIV enrollment which would also be maintained in the PIV IDMS: Physical characteristics (e.g., height, weight, and eye and hair color). Individuals

enrolled in the PIV managed service will be issued a PIV card. The PIV card contains the following mandatory visual personally identifiable information: Name, photograph, employee affiliation, organizational affiliation, PIV card expiration date, agency card serial number, and color-coding for employee affiliation. Agencies may choose to have the following optional personally identifiable information printed on the card: Cardholder physical characteristics (height, weight, and eye and hair color). The card also contains an integrated circuit chip which is encoded with the following mandatory data elements which comprise the standard data model for PIV logical credentials: PIV card PIN, cardholder unique identifier (CHUID), PIV authentication digital certificate, and two fingerprint biometric templates. The PIV data model may be optionally extended by agencies to include the following logical credentials: Digital certificate for digital signature, digital certificate for key management, card authentication keys, and card management system keys. All PIV logical credentials can only be read by machine.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554); E-Government Act of 2002 (Pub. L. 107-347, Sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note); Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004;

PURPOSES: The primary purposes of the system are: To ensure the safety and security of Federal facilities, systems, or information, and of facility occupants and users; to provide for interoperability and trust in allowing physical access to individuals entering Federal facilities; and to allow logical access to Federal information systems, networks, and resources on a government-wide basis.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice (DOJ) when: (1) The agency or any component thereof; or (2) any employee of the agency in his or her official capacity; (3) any

employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (4) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ and is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.

b. To a court or adjudicative body in a proceeding when: (1) The agency or any component thereof; (2) any employee of the agency in his or her official capacity; (3) any employee of the agency in his or her individual capacity where the agency or the Department of Justice has agreed to represent the employee; or (4) the United States Government is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records and is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

c. Except as noted on Forms SF 85, SF 85-P, and SF 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.

d. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.

e. To the National Archives and Records Administration (NARA) or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.

f. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract, service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a, the Federal Information Security Management Act (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration.

g. To a Federal agency, State, local, foreign, or tribal or other public authority, on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.

h. To the Office of Management and Budget (OMB) when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.

i. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended; the CIA Act of 1949, as amended; Executive Order 12333 or any successor order; and applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders, or Directives.

j. To designated agency personnel for controlled access to specific records for the purposes of performing authorized audit or authorized oversight and administrative functions. All access is controlled systematically through authentication using PIV credentials based on access and authorization rules for specific audit and administrative functions.

k. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Government Accountability Office (GAO), or other Federal agency in accordance with the agency's responsibility for evaluation of Federal personnel management.

l. To the Federal Bureau of Investigation for the FBI National Criminal History check.

m. To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: Records are stored in electronic media and in paper files.

RETRIEVABILITY: Records may be retrieved by name of the individual, Cardholder Unique Identification Number, Applicant ID, Social Security Number, and/or by any other unique individual identifier.

SAFEGUARDS: Consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration, the GSA HSPD-12 managed service office protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards. Access is restricted on a “need to know" basis, utilization of PIV Card access, secure VPN for Web access, and locks on doors and approved storage containers. Buildings have security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include: Indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; biometric access screening. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All

data is encrypted in transit. While it is not contemplated, any system records stored on mobile computers or mobile devices will be encrypted. GSA maintains an audit trail and performs random periodic reviews to identify unauthorized access. Persons given roles in the PIV process must be approved by the Government and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.

RETENTION AND DISPOSAL: Disposition of records will be according to NARA disposition authority N1-269-06-1 (pending).

SYSTEM MANAGER AND ADDRESS: Director, HSPD-12 Managed Service Office, Federal Acquisition Service (FAS), General Services Administration, 1800 F Street, NW, 4th Floor, Washington, DC 20405.

NOTIFICATION PROCEDURE: A request for access to records in this system may be made by writing to the System Manager. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date of birth, agency name, and work location. An individual requesting notification of records must provide identity documents sufficient to satisfy the custodian of the records that the requester is entitled to access, such as a government-issued photo ID.

RECORD ACCESS PROCEDURES: Same as Notification Procedure above.

CONTESTING RECORD PROCEDURES: Same as Notification Procedure above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES: Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other Federal agencies; contract employer; former employer.

[FR Doc. 2015-26940 Filed: 10/22/2015 08:45 am; Publication Date: 10/23/2015]