prosecuting, enforcing, or carrying out a statute, rule, regulation, or order, where an agency becomes aware of a violation or potential violation of civil or criminal law or regulation.

b. To an appeal, grievance, or formal complaints examiner; equal employment opportunity investigator; arbitrator; or other official engaged in investigating, or settling a grievance, complaint, or appeal filed by an individual who is the subject of the record.

c. To officials of labor organizations recognized under Public Law 95–454, when necessary to their duties of exclusive representation on personnel policies, practices, and matters affecting working conditions.

d. To another Federal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; clarifying a job; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision.

e. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Government Accountability Office (GAO) or other Federal agency when the information is required for program evaluation purposes.

f. To a Member of Congress or staff on behalf of and at the request of the individual who is the subject of the record.

g. To the National Archives and Records Administration (NARA) for records management purposes.

h. To an expert, consultant, or contractor in the performance of a Federal duty to which the information is relevant, including issuance of charge cards.

i. To GSA in the form of listings, reports, and records of all transportation related transactions, including refunds and adjustments, by the contractor to enable audits of transportation related charges to the Government.

j. To GSA contract agents assigned to participating agencies for billing of purchase expenses.

k. To agency finance offices for debt collection purposes.

l. 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 SYSTEM RECORDS:

STORAGE:

Information may be collected on paper or electronically and may be stored on paper or on electronic media, as appropriate.

RETRIEVABILITY:

Records may be retrieved by name, Social Security Number, credit card number, and/or other personal identifier or appropriate type of designation.

SAFEGUARDS:

System records are safeguarded in accordance with the requirements of the Privacy Act, the Computer Security Act, and OMB Circular A–130. Technical, administrative, and personnel security measures are implemented to ensure confidentiality and integrity of the system data stored, processed, and transmitted. Paper records are stored in secure cabinets or rooms. Electronic records are protected by passwords and other appropriate security measures.

RETENTION AND DISPOSAL:

Disposition of records is according to the National Archives and Records Administration (NARA) guidelines, as set forth in the handbook, GSA Records Maintenance and Disposition System (OAD P 1820.2A and CIO P 1820.1), authorized GSA records schedules, and by individual agencies.

SYSTEM MANAGER AND ADDRESS:

Director, Office of Commercial Acquisition (FC), General Services Administration, 1901 South Bell Street, Arlington VA 22202. Also, officials responsible for individual agency purchase card programs using the SmartPay system.

NOTIFICATION PROCEDURE:

Individuals may obtain information about their records from the purchase charge card program manager of the agency for which they transact purchases.

RECORD ACCESS PROCEDURES:

Requests from individuals for access to their records should be addressed to their agency's purchase charge card program manager or to the finance office of the agency for which the individual transacts purchases.

CONTESTING RECORD PROCEDURES:

Individuals may access their records, contest the contents, and appeal determinations according to their agency's rules.

RECORD SOURCE CATEGORIES:

Information is obtained from individuals submitting charge card applications, monthly contractor reports, purchase records, managers, other agencies, non-Federal sources such as private firms, and other agency systems containing information pertaining to the purchase charge card program.

[FR Doc. E8–8883 Filed 4–24–08; 8:45 am]

BILLING CODE 6820–34–P

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Notice of Updated Systems of Records

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: GSA reviewed its Privacy Act systems to ensure that they are relevant, necessary, accurate, up-to-date, covered by the appropriate legal or regulatory authority, and in response to OMB M–07–16. This notice is a compilation of updated Privacy Act system of record notices.

DATES: Effective May 27, 2008.

FOR FURTHER INFORMATION CONTACT: Call or e-mail the GSA Privacy Act Officer: Telephone 202–208–1317; e-mail *gsa.privacyact@gsa.gov*.

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

SUPPLEMENTARY INFORMATION: GSA undertook and completed an agency wide review of its Privacy Act systems of records. As a result of the review GSA is publishing updated Privacy Act systems of records notices. Rather than make numerous piecemeal revisions, GSA is republishing updated notices for one of its systems. Nothing in the revised system notices indicates a change in authorities or practices regarding the collection and maintenance of information. Nor do the changes impact individuals' rights to access or amend their records in the systems of records. The updated system

notices also include the new requirement from OMB Memorandum M–07–16 regarding a new routine use that allows agencies to disclose information in connection with a response and remedial efforts in the event of a data breach.

Dated: April 16, 2008.

Cheryl M. Paige,

Director, Office of Information Management.

GSA/GOVT–7

SYSTEM NAME:

Personal Identity Verification Identity Management System (PIV IDMS).

SECURITY CLASSIFICATION:

Sensitive but unclassified.

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 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 (Pub. L. 107–296, Sec. 3544); E-Government Act (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); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Services Act of 1949, as amended.

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 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.

n. 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, Suite 911, 2011 Crystal Drive, Arlington, VA 22202.

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 in person 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.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. E8–8884 Filed 4–24–08; 8:45 am]

BILLING CODE 6820–34–P

GENERAL SERVICES ADMINISTRATION

Privacy Act of 1974; Notice of Updated Systems of Records

AGENCY: General Services Administration.

ACTION: Notice.

SUMMARY: GSA reviewed its Privacy Act systems to ensure that they are relevant, necessary, accurate, up-to-date, covered by the appropriate legal or regulatory authority, and in response to OMB M–07–16. This notice is a compilation of updated Privacy Act system of record notices.

DATES: Effective May 27, 2008.

FOR FURTHER INFORMATION CONTACT: Call or e-mail the GSA Privacy Act Officer: telephone 202–208–1317; e-mail *gsa.privacyact@gsa.gov*.

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

SUPPLEMENTARY INFORMATION: GSA undertook and completed an agency wide review of its Privacy Act systems of records. As a result of the review GSA is publishing updated Privacy Act systems of records notices. Rather than make numerous piecemeal revisions, GSA is republishing updated notices for one of its systems. Nothing in the revised system notices indicates a change in authorities or practices regarding the collection and maintenance of information. Nor do the changes impact individuals' rights to access or amend their records in the systems of records. The updated system notices also includes the new requirement from OMB Memorandum M–07–16 regarding a new routine use that allows agencies to disclose information in connection with a response and remedial efforts in the event of a data breach.

Dated: April 16, 2008.

Cheryl M. Paige,

Director, Office ofInformation Management.

GSA/GOVT–5

SYSTEM NAME:

Access Certificates for Electronic Services (ACES).

SYSTEM LOCATION:

System records are maintained for the General Services Administration (GSA) by contractors at various physical locations. A complete list of locations is available from: Administrative Contracting Officer, FEDCAC, Federal Technology Service, General Services Administration, 7th and D Streets, SW., Room 5060, Washington, DC 20407; telephone (202) 708–6099.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered are persons who have applied for the issuance of a digital signature certificate under the ACES program; have had their certificates amended, renewed, replaced, suspended, revoked, or denied; have used their certificates to electronically make contact with, retrieve information from, or submit information to an automated information system of a participating agency; have requested access to ACES records under the Freedom of Information Act (FOIA) or Privacy Act; and have corresponded with GSA or its ACES contractors concerning ACES services.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information needed to establish and verify the identity of ACES users, to maintain the system, and to establish accountability and audit controls. System records include:

a. Applications for the issuance, amendment, renewal, replacement, or revocation of digital signature certificates under the ACES program, including evidence provided by applicants or proof of identity and authority, and sources used to verify an applicant's identify and authority.

b. Certificates issued.

c. Certificates denied, suspended, and revoked, including reasons for denial, suspension, and revocation.

d. A list of currently valid certificates.

e. A list of currently invalid certificates.

f. A file of individuals requesting access and those granted access to ACES information under FOIA or the Privacy Act.

g. A file of individuals requesting access and those granted access for reasons other than FOIA or the Privacy Act.

h. A record of validation transactions attempted on digital signature certificates issued by the system.

i. A record of validation transactions completed on digital signature certificates issued by the system.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 5124(b) of the Clinger-Cohen Act of 1996, 40 U.S.C. 1424, which provides authority for GSA to develop and facilitate governmentwide electronic commerce resources and services, and the Paperwork Reduction Act, 44 U.S.C. 3501, *et. seq.*, which provides authority for GSA to manage Federal information resources.

PURPOSE:

To establish and maintain an electronic system to facilitate secure, on-line communication between Federal automated information systems and the public, using digital signature technologies to authenticate and verify identity.

ROUTINE USES OF THE SYSTEM RECORDS, INCLUDING CATEGORIES OF USERS AND THEIR PURPOSES FOR USING THE SYSTEM:

Information from this system may be disclosed as a routine use:

a. To GSA ACES program contractors to compile and maintain documentation on applicants for proofing applicants' identity and their authority to access information system applications of participating agencies.

b. To GSA ACES program contractors to establish and maintain documentation on information sources for verifying applicants' identities.

c. To Federal agencies participating in the ACES program to determine the validity of applicants' digital signature certificates in an on-line, near real time environment.

d. To GSA, participating Federal agencies, and ACES contractors, for ensuring proper management, ensuring data accuracy, and evaluation of the system.

e. To Federal, State, local or foreign agencies responsible for investigating,