GENERAL SERVICES ADMINISTRATION

[Notice-ISP-2016-02; Docket 2016-0002; Sequence 22]

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

AGENCY: General Services Administration (GSA).

ACTION: Notice; New System.

SUMMARY: GSA proposes a new 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 or e-mail the GSA Privacy Act Officer: telephone 571-388-6570; e-mail gsa.privacyact@gsa.gov.

SUPPLEMENTARY INFORMATION: GSA proposes to establish a new system of records subject to the Privacy Act of 1974, 5 U.S.C. 552a. The system is a citizen-centric platform for delivering government services through a centralized single sign-on platform. The platform will leverage personal information to provide identity proofing to partner agencies, as well as data and resources associated with the user's account. Based on a successful user login and identity proofing, the partner agency will grant access to the user.

In order to facilitate access, information must be collected to authenticate an individual's identity at the requisite level of assurance for the purpose of obtaining a credential or electronically authorizing access to an agency application or service. Identity proofing is the process by which an identity service provider collects and verifies personally identifiable information (PII) about an individual for the purpose of issuing credentials to that individual.

Third-party identity service providers used by Login.gov use a variety of verification techniques. Users will be authenticated and proofed at the level required by the partner agency for accessing specific services and records. When a user attempts to access an agency service or record, the individual will be directed to Login.gov. The information requested by the system and asserted back to the agency will be only what is necessary to establish Level of Access (LOA)1 or LOA3 as appropriate. For access to services or records that require LOA1, the user will be asked for email, password, and phone number.

For access to services or records that require LOA3, the user will be asked for PII that will be used for identity proofing, and then maintained in the system. Attributes requested for the proofing process are full

name, date of birth, address, phone number, and social security number (SSN). The identity proofer will also ask the user credit and financial related questions. Login.gov does not have access to or retain the commercial identity verification information, questions asked of a user or the responses provided thereto.

Once proofed, the attribute bundle will be given a meaningless, but unique identifier number (MBUN) to identify the user in the system. The MBUN and attribute bundle will be asserted to the partner agency. The partner agency is granted access to user information only when the user logs in or specifically gives permission to transmit their information. The information in the system is contributed voluntarily by the user and cannot be accessed by the government without explicit consent of the user, except as provided in this notice.

Information is not shared between government agencies, except when the user gives explicit consent to share his or her information, except as provided in this notice.

Pranjali Desai,
Director,
Office of Information Management,
General Services Administration.

[BILLING CODE: 6820-34]

GSA/GOVT-10

SYSTEM NAME: Login.gov.

SYSTEM LOCATION: The system is maintained for GSA under contract. Contact the System Manager for additional information.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Anyone is able to create an account.

CATEGORIES OF RECORDS IN THE SYSTEM: Records may include, but are not limited to: biographical data such as name, address, email, password, phone number, birth date, social security number. Use of the system, and contribution of personal information, is completely voluntary.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. 3501 note)

PURPOSES: To enable users to control how government interacts with them and their personal information, and to aid and assist users in interacting with the government. Users interacting with local, state, or federal agency developed applications may be asked to authorize the application to access system resources, such as their personal profile information. If a user authorizes use of his or her information, the agency application will be given programmatic access to the user's account resources. Profile, usage, and system information may be accessed by

system managers, technical support and designated analysts in the course of their official duties.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

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

a. In any legal proceeding, where pertinent, to which GSA, a GSA employee, or the United States is a party before a court or administrative body.

b. To a Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when GSA becomes aware of a violation or potential violation of civil or criminal law or regulation.

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

d. To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), and the Government Accountability Office (GAO) in accordance their responsibilities for evaluating Federal programs.

e. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant.

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

g. To a Federal agency in connection with the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation; 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.

h. 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.

i. To federal, state, or local government agencies or entities for purposes of complying with any legally authorized order or request of such an entity that is made in carrying out the entity's official responsibilities.

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

STORAGE: All records are stored electronically in a database. Personally Identifiable Information (PII) is encrypted.

RETRIEVABILITY: Records are retrieved using an authorization protocol. A user of the system grants explicit authorization to an application or government agency to access his or her profile.

SAFEGUARDS: Access to the database is maintained behind a firewall certified in accordance with National Institute of Standards and Technology standards and information in the database is encrypted.

Records access is limited to authorized individuals and protected with two-factor authentication, and databases are behind a firewall. PII is encrypted at rest, and all transmissions of any information over external networks are encrypted. All passwords, encryption algorithms and

firewalls are compliant with National Institute of Standards and Technology standards.

RETENTION AND DISPOSAL: System records are retained and disposed of according to GSA records maintenance and disposition schedules and the requirements of the National Archives and Records Administration. The initial implementation of this has a limited scope of users. The option for users to delete their own information will be functional in a future version of the application. Physical records are disposed of by cross-cut shredding or burning as scheduled in the handbook, GSA Records Maintenance and Disposition System (CIO P. 1820.1).

SYSTEM MANAGER AND ADDRESS: Director, Login.gov, General Services Administration, 1800 F Street, NW, Washington, DC 20405; ATTN: https://www.login.gov.

NOTIFICATION PROCEDURE: Individuals or users maintain their own information. Inquires can be made via the web site at https://login.gov/ or at the above address under 'System Manager and Address'.

RECORD ACCESS PROCEDURES: Individuals or users wishing to access their own records may do so by password or by contacting the system administrator at the above address.

CONTESTING RECORD PROCEDURES: Individuals or users of the system may amend their own records online.

RECORD SOURCE CATEGORIES: The sources for information in the system are the individuals (or system users) for whom the records are maintained, and third-party applications which the user has authorized to contribute information to his or her account.

[FR Doc. 2016-20191 Filed: 8/23/2016 8:45 am; Publication Date: 8/24/2016]