

General Services Administration

[Notice-ID-2016-03; Docket 2016-0002; Sequence No. 29]

Privacy Act of 1974; Notice of a New System of Records

AGENCY: General Services Administration (GSA).

ACTION: Notice of a New System of Records.

SUMMARY: GSA proposes to establish a new system of records subject to the Privacy Act of 1974. The proposed system is a single sign-on platform to facilitate access to government services.

DATES: The system of records notice is effective upon its publication in today's Federal Register, with the exception of the routine uses which are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Comments on the routine uses or other aspects of the system of records notice must be submitted by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Submit comments identified by "Notice-ID-2016-03, Notice of New System of Records" by any of the following methods:

- Regulations.gov: <http://www.regulations.gov>.

Submit comments via the Federal eRulemaking portal by searching for Notice-ID-2016-03, Notice of New System

of Records. Select the link "Comment Now" that corresponds with "Notice-ID-2016-03, Notice of New System of Records." Follow the instructions provided on the screen. Please include your name, company name (if any), and "Notice-ID-2016-03, Notice of New System of Records" on your attached document.

- Mail: General Services Administration, Regulatory Secretariat Division (MVCB), 1800 F Street, NW, Washington, DC 20405. ATTN: Ms. Flowers/ Notice-ID-2016-03, Notice of New System of Records.

FOR FURTHER INFORMATION CONTACT: Call the GSA Chief Privacy Officer at telephone 202-322-8246; or 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 proposed system is a single sign-on platform to facilitate access to government services. The previously published notice, at 81 FR 57912, on August 24, 2016, is being replaced. The system is a single, secure platform through which members of the public can log-in and access services from participating federal agencies (partner agencies). All federal agencies are eligible to participate, and those that do will be listed on the

Login.gov information page. The platform will use information given by the user to identity proof them including email address, password, name, date of birth, address, phone number, and social security number.

Identity proofing is the process of verifying that a person is who they say they are. Personally Identifiable Information (PII) must be collected from a Login.gov user to identity proof that user and then authenticate that user's identity at a Level of Assurance (LOA) required by a partner agency to grant access to its information, applications, programs, or records (for the purpose of this notice, "services"). Login.gov authenticates a user by validating that person is the owner of an account through a valid username, password, and the completion of the multi-factor authentication step, for example by providing the one-time password they receive by phone.

Login.gov operates at two levels of assurance: Level of Assurance 1 (LOA1) and Level of Assurance 3 (LOA3). A user will only be asked for information based on the LOA required by the partner agency to access a given service. For example, in order to access a service that requires LOA1, the user will only be asked to provide an email address, password and phone number, because that

information suffices for LOA1. To access a service that requires LOA3, the user will be asked to provide the above information as well as full name, date of birth, home address and Social Security Number. These two sets of PII comprise the user's LOA1 or LOA3 "account information," respectively.

Login.gov will collect and maintain a user's LOA1 account information, and if required, LOA3 account information. Login.gov will verify a user's identity at LOA3 by providing the user's LOA3 account information to a third party identity proofing service. Third party identity proofing services used by Login.gov may employ a variety of verification techniques, including, but not limited to, verifying a user's financial information or information from a user's government-issued identification.

The identity proofing process between Login.gov and a third party identity proofing service takes place within Login.gov after the user provides the information required by that third party identity proofing service. However, Login.gov does not retain a user's response(s) to any question(s) posed by a third party identity proofing service during the proofing process.

Once a user is proofed at LOA1, that user's account information will be assigned a meaningless, but unique, number (MBUN) to identify the user in Login.gov. The user's MBUN (and the minimum set of user account information needed to allow access to the partner agency's service) will be provided to the partner agency only after the user gives permission to send that information.

The information in Login.gov is contributed voluntarily by the user and cannot be accessed, used, or disclosed by GSA without consent of the user, except as provided in this notice. A partner agency may add its own unique identifier to the user's Login.gov account information for the purpose of identifying the user on subsequent attempts to access that agency's services.

Login.gov follows National Institute of Standards and Technology (NIST) Special Publication 800-63-2, "Electronic Authentication Guideline" and will employ third party identity proofing services, proofing using government data sources, including government-issued identification.

Richard Speidel, J.D., CIPP/G
Chief Privacy Officer,

Office of the Deputy Chief Information Officer,
General Services Administration.

SYSTEM NAME AND NUMBER: Login.gov, GSA/TTS-1.

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: The system is owned and maintained by GSA, housed in secure datacenters in continental United States. Contact the System Manager listed below for additional information.

SYSTEM MANAGER: Joel Minton, Director, Login.gov, General Services Administration, 1800 F Street, NW, Washington, DC 20405. <https://www.Login.gov>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: E-Government Act of 2002 (P.L. 107-347, 44 U.S.C. 3501 note), 6 U.S.C. 1523 (b) (1) (A)-(E), and 40 U.S.C. 501.

PURPOSE(S) OF THE SYSTEM: The purpose of the system is to provide a single, secure platform through which members of the public can log-in and access services from partner agencies, and to increase user security by facilitating identity proofing and authentication as necessary in order to access specific government services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Anyone with an email account and access to a phone is able to

create an account at any time. Individuals in this system of records are members of the public seeking electronic access to a service from a participating Federal agency (partner agency), including anyone attempting to authenticate and/or identity proof for the purpose of obtaining a credential to electronically access a partner agency's services. All federal agencies are eligible to participate, and those that do will be listed on the Login.gov information page.

CATEGORIES OF RECORDS IN THE SYSTEM: The information collected by Login.gov is necessary to perform identity proofing at the partner agency's required level of assurance (LOA). A user's account information is only retained as necessary to manage the user's credential. The only information a user must provide to identity proof at LOA1 is an email address, password and phone number. For LOA3 identity proofing, the above information is collected, as well as the user's name, address, birth date, Social Security number.

If a third party identity proofing service is unable to proof the user based on the user's LOA3 account information, Login.gov may request additional information from the user. However, any additional questions from the

third party identity proofing service and the user's responses will not be retained by Login.gov after the user logs off.

Each third party identity proofing service will send information back to Login.gov about its attempt to identity proof the user including: transaction ID; pass/fail indicator; date/time of transaction; and codes associated with the transaction data.

Each partner agency whose services the user accesses via Login.gov may add its own unique identifier to that user's account information.

RECORD SOURCE CATEGORIES: The sources for information in the system are the individual Login.gov users. Each third party identity proofing service will provide transaction details about its attempt to identity proof a user and each partner agency whose services the user accesses via Login.gov may provide its own unique identifier to that user's account information.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may

be disclosed to authorized entities, as is determined to be relevant and necessary, outside GSA as a routine use pursuant to 5 U.S.C. 552a(b) (3) as follows:

a. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) GSA or any component thereof, or (b) any employee of GSA in his/her official capacity, or (c) any employee of GSA in his/her individual capacity where DOJ or GSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and GSA determines that the records are both relevant and necessary to the litigation.

b. To NIST-compliant third party identity proofing services, as necessary to identity proof an individual for access to a service at the required level of assurance.

c. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record,

either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

d. To a Member of Congress or his or her staff in response to a request made on behalf of and at the request of the individual who is the subject of the record.

e. To the Office of Management and Budget (OMB) and the Government Accountability Office (GAO) in accordance with their responsibilities for evaluation or oversight of Federal programs.

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

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

h. To appropriate agencies, entities, and persons when (1) GSA suspects or has confirmed that there has been a breach of the system of records; (2) GSA has determined that as a result of the suspected or

confirmed breach there is a risk of harm to individuals, GSA (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 GSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

i. To another Federal agency or Federal entity, when GSA 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: All records are stored electronically in a database. User account information is encrypted in transit and at rest.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The user's email address and phone number, which are part of LOA1

account information, can be retrieved using Login.gov developed software with system access. When the user provides their password or recovery code, the system retrieves that user's LOA1 account information (email, password, and phone number) or LOA3 account information (full name, date of birth, home address and Social Security Number) using a search of the email addresses in the system. However, each user's LOA3 account information is encrypted such that neither the system nor system operators can retrieve it without the user providing their password or recovery code.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF

RECORDS: System records will be retained and disposed of in accordance with NARA's General Records Schedule (GRS) Transmittal 26, section 3.2 "System access records" covering user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges for system use. The guidance instructs, "Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use."

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records in the system are protected from unauthorized access and

misuse through various administrative, technical and physical security measures. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed and regular review of security procedures and best practices to enhance security. Access to the Login.gov database is maintained behind an industry-standard firewall and information in the database is encrypted. As noted above, neither the system nor the system operators can retrieve the user's LOA3 account information without the user supplying a password or recovery code.

RECORD ACCESS PROCEDURES: Individuals or users wishing to access their own records may do so by providing their email address, password, and a multi-factor authentication token (e.g. a one-time password or code sent to the user's phone) to Login.gov, or by contacting the system administrator at the above address.

CONTESTING RECORD PROCEDURES: Users can modify, or amend, any of their user account information by accessing it in their account. Users that want access to partner agency records, or to contest the contents of those records, need to make a request with that agency.

NOTIFICATION PROCEDURE: Users create their account information and, thereafter, access it by providing their email address, password, and a multi-factor authentication token (e.g. a one-time password or code sent to the user's phone). Inquiries can be made via the web site at <https://Login.gov/> or at the above address under 'System Manager and Address'.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None

HISTORY: This notice replaces the previously published notice at 81 FR 57912, on August 24, 2016.

[FR Doc. 2017-01174 Filed: 1/18/2017 8:45 am; Publication Date: 1/19/2017]