



This document is scheduled to be published in the Federal Register on 07/05/2013 and available online at <http://federalregister.gov/a/2013-16124>, and on FDsys.gov

GENERAL SERVICES ADMINISTRATION

[Notice-CIB-2013-05; Docket 2013-0002; Sequence 18]

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

AGENCY: U.S. General Services Administration (GSA).

ACTION: 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 date: [Insert date 30 days after publication in the Federal Register].

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, 1275 First Street, NE, Washington, DC 20417.

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 provides an account to users that gives them control over how government agencies interact with them and their personal information. Agencies can build applications on top of the MyUSA platform that will streamline and improve citizen interactions with government. Applications will leverage data and resources associated with the user's account, including personal

information. The information in the system is contributed voluntarily by the user and cannot be accessed by 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.

Dated: June 28, 2013

James Atwater,
Acting Director,
Office of Information Management,
General Services Administration.

[BILLING CODE: 6820-34]

GSA/OCSIT-1

SYSTEM NAME: MyUSA.

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: (1) biographical data such as name, address, email, phone number, birth date, and basic demographic information such as whether or not the individual is married, a veteran, a small business owner, a parent or a student; (2) information stored by third-party applications that have been authorized by the user to access their account using one or more of MyUSA's programmatic interfaces, such as notifications, tasks, or events; (3) a history of third-party applications interactions with a user's account so the user can monitor how their account is being accessed by third-parties. 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 USC § 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 government.

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

Users interacting with third-party applications, such as those developed by government agencies, may be asked to authorize the third-party application to access their system resources, such as their personal profile information. If a user authorizes use of his or her information, the third-party application will be given programmatic access to the user's account resources. All interactions with a user's account, such as reading personal profile information, are logged and are auditable by the user. Users can revoke a third-party application's authorization to access their account resources at any time. System information may be accessed by system managers, technical support and designated analysts in the course of their official duties. 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.

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 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. The system generates

a unique token that authorizes only that application or agency to access the user's account. The system correlates the unique token, ensures that both the agency and the user involved are correct, and returns the information to the agency.

SAFEGUARDS: System records are safeguarded in accordance with the requirements of the Privacy Act. Access to physical infrastructure is limited to authorized individuals with passwords; 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 are safeguarded in accordance with Privacy Act requirements. Access is limited to authorized individuals and protected with two-factor authentication, databases are behind a firewall. Personally Identifiable Information 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. Users may delete their own information from the system at any time.

SYSTEM MANAGER AND ADDRESS: Director, MyUSA, General Services Administration, 1800 F Street, NW, Washington, DC 20405. <https://my.usa.gov/>

NOTIFICATION PROCEDURE: Individuals or users maintain their own information. Inquires can be made via the web site at <https://my.usa.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.

CONTESTING RECORD PROCEDURES: Individuals or users of the system may amend or delete 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. 2013-16124 Filed 07/03/2013 at 8:45 am;

Publication Date: 07/05/2013]