

INFORMATION CONTACT section of this document for alternate instructions.

Instructions: Please submit comments only and cite Information Collection 3090–0310, Nondiscrimination in Federal Financial Assistance Programs, GSA 3702, in all correspondence related to this collection. Comments received generally will be posted without change to <http://www.regulations.gov>, including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two-to-three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Stephanie Stoltzfus Treier, Deputy Associate Administrator, Office of Civil Rights, at telephone 202–501–0767 or via email to civilrights@gsa.gov.

SUPPLEMENTARY INFORMATION:

A. Purpose

GSA has mission responsibilities related to monitoring and enforcing compliance with Federal civil rights laws and regulations that apply to Federal financial assistance programs administered by GSA. Specifically, those laws provide that no person on the ground of race, color, national origin, disability, sex or age shall be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program in connection with which Federal financial assistance is extended under laws administered in whole, or in part, by GSA.

These mission responsibilities generate the requirement to request and obtain certain data from recipients of Federal surplus property for the purpose of determining compliance, such as the number of individuals that speak non-English languages encountered by the recipient's program(s) and how the recipient is addressing meaningful access for individuals that are Limited English Proficient; whether the recipients provide disability access in compliance with applicable laws and standards; whether there has been complaints or lawsuits filed against the recipient based on prohibited discrimination; whether there has been any findings of discrimination; and whether the recipient's facilities are accessible to qualified individuals with disabilities.

B. Annual Reporting Burden

Respondents: 1,200.
Responses per Respondent: 1.
Total Responses: 1,200.
Hours per Response: 2.
Total Burden Hours: 2,400.

C. Public Comments

Public comments are particularly invited on: Whether this collection of information will have practical utility; whether our estimate of the public burden of this collection of information is accurate, and based on valid assumptions and methodology; ways to enhance the quality, utility, and clarity of the information to be collected; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

Obtaining Copies of Proposals: Requesters may obtain a copy of the information collection documents from the GSA Regulatory Secretariat Division by calling 202–501–4755 or emailing GSARegSec@gsa.gov. Please cite OMB Control No. 3090–0310, Nondiscrimination in Federal Financial Assistance Programs, GSA 3702, in all correspondence.

Beth Anne Killoran,
Deputy Chief Information Officer.
 [FR Doc. 2022–25277 Filed 11–18–22; 8:45 am]
BILLING CODE 6820–34–P

**GENERAL SERVICES
ADMINISTRATION**

[Notice–ID–2022–02; Docket No. 2022–0002; Sequence No. 29]

**Privacy Act of 1974; Notice of a
Modified System of Records**

AGENCY: Office of the Chief Privacy Officer, General Services Administration (GSA).

ACTION: Notice of a modified system of records.

SUMMARY: GSA proposes to modify a system of records subject to the Privacy Act of 1974, as amended. *Login.gov* is a secure sign-in service with the capability to authenticate and identity proof users before the user is granted access to participating government websites or applications. GSA is modifying the categories of records in the system, the policies and practices for retrieval and routine uses of records, and removing outdated references to National Institute of Standards and Technology (NIST) technical standards. This modification is intended to revise and replace all notices previously describing this system of records.

DATES: Submit comments on or before: December 21, 2022.

ADDRESSES: Submit comments identified by “Notice–ID–2022–02,

Notice of Modified System of Records” via. Submit comments via <https://www.regulations.gov>, the Federal eRulemaking portal, by searching for Notice–ID–2022–02, Notice of Modified System of Records. Select the link “Comment Now” that corresponds with “Notice–ID–2022–02, Notice of Modified System of Records.” Follow the instructions provided on the screen. Please include your name, company name (if any), and “Notice–ID–2022–02, Notice of Modified System of Records” on your attached document.

FOR FURTHER INFORMATION CONTACT: Richard Speidel, Chief Privacy Officer, GSA, by email at gsa.privacyact@gsa.gov or by phone at 202–969–5830.

SUPPLEMENTARY INFORMATION: GSA proposes to alter language in this system of records to remove an outdated NIST technical standard, and instead use plain language to describe the system's authentication and identity proofing process.

In 2019, the Office of Management and Budget (OMB) published Memorandum 2019–17 (M–19–17), which withdrew Memorandum 2004–04 (M–04–04) and specified the most recent version of NIST SP 800–63 as authoritative for defining levels associated with the rigor of various digital identity related functions. OMB directed agencies to transition from the prior use of Levels of Assurance (LOAs) from M–04–04 in favor of Authentication Assurance Levels (AALs), Identity Assurance Levels (IALs), and Federation Assurance Levels (FALs).

To prevent future potential misalignment between Federal guidance and this system of record notice (SORN), this revision removes references to NIST standards and instead uses plain language descriptions of *Login.gov*'s authentication and identity proofing process. This revision also adds categories of records and two new routine uses related to research studies and fraud prevention operations, and details the records management practices for those new records.

Specifically:

- references to Level of Assurance (LOA) are removed because that is an outdated NIST technical standard and *Login.gov* instead uses plain language descriptions of its authentication and identity proofing process;
- use of records to increase coverage and access to authentication and identity proofing services to the public, including studies evaluating impacts to equitable access by identity verification.
- use of records to support fraud prevention operations to preserve

integrity of the authentication and identity proofing system.

Richard Speidel,

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

SYSTEM NAME AND NUMBER:

GSA/TTS-1 (*Login.gov*)

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

General Services Administration owns *Login.gov*, which is housed in secure data centers in the continental United States. Contact the System Manager listed below for additional information.

SYSTEM MANAGER(S):

Daniel Lopez-Braus, Director, *Login.gov*, TTS, Office of Solutions, 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 (Pub. L. 107-347, 44 U.S.C. 3501 note), 6 U.S.C. 1523 (b)(1)(A)–(E), and 40 U.S.C. 501.

PURPOSES(S) OF THE SYSTEM:

The purposes of the system are:

- to provide a secure sign-in service with the capability to authenticate and identity proof users before the user is granted access to participating government websites or applications;
- to prevent fraud and to protect the integrity of the *Login.gov* system; and
- to conduct studies into enhancements to the secure sign-in service, including demographic studies of the equitable performance of new technologies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by this system of records include members of the public seeking electronic access to a website or application from a federal, state, or local agency that has integrated with *Login.gov* (“partner agency”) and participants in studies commissioned by GSA to evaluate equitable performance of new identity verification and fraud prevention technologies.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains information provided by individuals who create and use *Login.gov* accounts. There are two types of accounts in the *Login.gov* system: records related to the process of authenticating a *Login.gov* user’s account, and records related to the process in which an individual’s identity is verified.

For accounts for which *Login.gov* is authenticating the user, the system collects and maintains:

- email address,
- password,
- and phone number (optionally).

For accounts that require a verified identity, the system collects and maintains:

- photographs of their government-issued ID, to include all personal information and images on the ID. Photographs are stored in an encrypted format, and are only accessed to investigate suspected or confirmed fraud;

- Social Security Number (SSN); and
- phone number or postal address.

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
- status 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.

To protect the public and the integrity of the system, *Login.gov* needs to detect and prevent fraud while providing redress to users who were unable to complete identity verification. To that end, *Login.gov* will also obtain a collection of information about the device (a “Device ID”) including, for example browser type and internet protocol (IP) address) and usage patterns (e.g., keyboard, mouse, or touchscreen behavior) used to access their *Login.gov* account. The Device ID and usage patterns are assessed by a third-party fraud prevention service along with the other information collected by *Login.gov*. The third-party fraud prevention services provide *Login.gov* risk scores for all of the information assessed, and also provide other identifying attributes that have been associated with that same Device ID in the past. Those identifying attributes include, but are not limited to, names, addresses, phone numbers, and SSNs that have been associated with the Device ID.

Separate from *Login.gov*’s active sign-on service, GSA may also conduct studies in which it temporarily collects information from voluntary participants to evaluate the equitable performance of new technologies and guide service improvements. In addition to the categories of records previously described, collection of information for studies could include, but is not limited to:

- demographic information such as race, ethnicity, gender, income, age, and education; and
- biometric information to verify that the applicant matches the identity documents (e.g., a photograph or video of the user).

RECORD SOURCE CATEGORIES:

The sources for information in the system include individual *Login.gov* users, participants in GSA-commissioned studies, third-party identity-proofing services, partner agencies, and third-party fraud prevention services. Individual users and research participants provide information needed to authenticate themselves, verify their identity, or voluntarily respond to research surveys. Each third-party identity proofing service provides transaction details about their attempt to identity proof a user. Partner agencies may provide their own unique identifier to that user’s account information. Third party fraud prevention services provide risk scores and identity attributes associated with a user’s Device ID.

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 third parties providing remote or in-person authentication and identity proofing services, inclusive of other federal agencies providing such services, as necessary to authenticate and/or identity proof an individual for access to a participating government website or application;

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), Office of Inspector General (OIG), 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.

j. To the Government Publishing Office (GPO), when *Login.gov* needs to mail a user an address confirmation form or if a user requests mailed notifications of account changes or of proofing attempts.

k. To other federal agencies and third-party fraud prevention services as

necessary to detect and investigate suspected fraud, including providing redress to users.

l. To third-party identity proofing services and fraud prevention services when participating in studies commissioned by the GSA to evaluate the equitable performance of new technologies and guide service improvements.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

All records are stored electronically in databases. User account information is encrypted in transit and at rest.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records retrieval practices vary based on the type or category of record in the system.

a. When a user logs in, *Login.gov* retrieves their email and phone number (if provided) to send the user a one-time passcode.

b. When a user accesses a participating government website or application that requires the user's identity attributes, the following retrieval practice occurs:

i. The user successfully logs into their account (enabling decryption and retrieval of certain records);

ii. *Login.gov* decrypts and retrieves the user's verified personal information (full name, date of birth, postal address, and Social Security Number); and

iii. *Login.gov* requests that the user provide consent to share the personal information requested by the participating government site.

c. When a user with verified identity is recovering access to their account, the following retrieval practice occurs:

i. The user successfully authenticates their account when requesting to reset their *Login.gov* password;

ii. The user provides their personal recovery code (enabling decryption and retrieval of the records) and selects a new password;

iii. *Login.gov* retrieves the user's verified personal information (full name, date of birth, postal address, and Social Security Number);

iv. These attributes are then encrypted with the user's new password.

d. When *Login.gov* is performing fraud investigation and redress, the following retrieval practices occur:

i. Only trained *Login.gov* fraud operations personnel have access to records maintained specifically for fraud prevention purposes. This includes Device IDs and usage patterns associated with personal identifiers and risk scores as described in the Categories of Records in the System.

ii. *Login.gov* fraud operations personnel retrieve personal information (full name, date of birth, postal address and Social Security Number) from third-party identity proofing services while completing a manual review of a user's identity proofing transaction.

e. When GSA is conducting studies into enhancements to the secure sign-in service, data from voluntary participants' surveys and identity-proofing transactions are retrieved by GSA and third-party contractors to conduct statistical analysis of the performance of new technologies. Data from *Login.gov*'s active service is not retrieved during these studies.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Retention and disposal policies and practices vary based on the type or category of record in the system.

a. Records related to active user authentication and validated user identities will be retained and disposed of in accordance with NARA's General Records Schedule (GRS) 3.2 (Transmittal 26), item 31 "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."

b. Records related to identity verification attempts (photographs of government IDs, personal information entered by the user) may be retained by *Login.gov* to aid in fraud investigation, redress, or product improvement.

c. Records related to fraud prevention operations, such as Device IDs and user behaviors with associated identity attributes and risk scores, are maintained by a third party on behalf of GSA for up to three years.

d. For studies commissioned by GSA, third-party proofing services will discard any information collected within 24 hours of collection. GSA will maintain the information for the duration of the study after which it will be preserved for 6 years as required by the GSA's retention schedule for Customer Research and Reporting Records.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in the system are protected from unauthorized access and misuse through a combination of administrative, technical, and physical security measures. Administrative measures include but are not limited to

policies that limit system access to individuals within an agency with a legitimate business need, and regular review of security procedures and best practices to enhance security. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of passphrases 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, other than email address, neither the system nor the system operators can retrieve the user's personal account information without the user supplying a password or recovery code. Trained and cleared *Login.gov* fraud operations personnel are able to cross-reference personal information used by third party or federal agency identity proofing services to validate a user's identity attributes as part of a manual review of identity proofing transactions. Records related to studies are kept separate from records related to *Login.gov*'s active users.

RECORD ACCESS PROCEDURES:

Requests for access to records should be directed to the system manager. Individuals seeking access to their records in this system of records may submit a request by following the instructions provided in 41 CFR part 105–64, subpart 105–64.2.

CONTESTING RECORD PROCEDURES:

During identity proofing, an individual can use the *Login.gov* fraud operations redress mechanism to contest records used by third party identity proofing services. After identity proofing or participating in a study, individuals wishing to contest the content of records about themselves contained in this system of records should contact the system manager at the address above. See 41 CFR part 105–64, subpart 105–64.4 for full details on what to include in a Privacy Act amendment request.

NOTIFICATION PROCEDURES:

Individuals seeking notification of any records about themselves contained in this system of records should contact the system manager at the address above. Follow the procedures on accessing records in 41 CFR part 105–64, subpart 105–64.2 to request such notification.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

82 FR 6552; 82 FR 37451
[FR Doc. 2022–25420 Filed 11–18–22; 8:45 am]
BILLING CODE 6820–34–P

DEPARTMENT OF DEFENSE

GENERAL SERVICES ADMINISTRATION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[OMB Control No. 9000–0024; Docket No. 2022–0053; Sequence No. 22]

Submission for OMB Review; Buy American, Trade Agreements, and Duty-Free Entry

AGENCY: Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA).

ACTION: Notice.

SUMMARY: Under the provisions of the Paperwork Reduction Act, the Regulatory Secretariat Division has submitted to the Office of Management and Budget (OMB) a request to review and approve a revision of a previously approved information collection requirement regarding Buy American, associated with implementation of Federal Acquisition Regulation (FAR) rule 2021–008, Amendments to the FAR Buy American Act Requirements.

DATES: Submit comments on or before December 21, 2022.

ADDRESSES: Written comments and recommendations for this information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting “Currently under Review—Open for Public Comments” or by using the search function.

Additionally, submit a copy to GSA through <https://www.regulations.gov> and follow the instructions on the site. This website provides the ability to type short comments directly into the comment field or attach a file for lengthier comments.

Instructions: All items submitted must cite OMB Control No. 9000–0024, Buy American, Trade Agreements, and Duty-Free Entry. Comments received generally will be posted without change to <https://www.regulations.gov>, including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two-to-three days after submission to verify posting. If there are difficulties submitting comments,

contact the GSA Regulatory Secretariat Division at 202–501–4755 or GSARegSec@gsa.gov.

FOR FURTHER INFORMATION CONTACT: Ms. Mahruba Uddowla, Procurement Analyst, at telephone 703–605–2868, or mahruba.uddowla@gsa.gov.

SUPPLEMENTARY INFORMATION:

A. OMB Control Number, Title, and Any Associated Form(s)

9000–0024, Buy American, Trade Agreements, and Duty-Free Entry.

B. Needs and Uses

This clearance covers the information that an offeror must submit in response to the requirements of the provisions and clauses in Federal Acquisition Regulation (FAR) part 25 that relate to the following:

- * The Buy American statute (41 U.S.C. chapter 83) and Executive Orders (E.O.s) 10582 and 14005.

- * The Trade Agreements Act (19 U.S.C. 2501–2515), including the World Trade Organization Government Procurement Agreement and various free trade agreements.

- * The American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5) (Recovery Act).

- * Subchapters VIII and X of Chapter 98 of the Harmonized Tariff Schedule of the United States (19 U.S.C. 1202).

a. 52.225–2, Buy American Certificate. This provision requires the offeror to identify in its proposal supplies that do not meet the definition of domestic end product and whether those supplies exceed 55% domestic content. This provision also requires offerors to identify in its proposal domestic end products that contain a critical component.

b. 52.225–4, Buy American—Free Trade Agreements—Israeli Trade Act Certificate. This provision requires a separate list of foreign products that are eligible under a trade agreement, and a list of all other foreign end products and whether those supplies exceed 55% domestic content. This provision also requires offerors to identify in its proposal domestic end products that contain a critical component.

c. 52.225–6, Trade Agreements Certificate. This provision requires the offeror to certify that all end products are either U.S.-made or designated country end products, except as listed in paragraph (b) of the provision. Offerors are not allowed to provide other than a U.S.-made or designated country end product, unless the requirement is waived.

d. 52.225–8, Duty-Free Entry. This clause requires contractors to notify the