Privacy Impact Assessment for Login.gov LOA1

March 29, 2017

1. Overview

Login.gov is an authentication platform that makes the public's online interactions with the U.S. government simpler, more efficient and intuitive. The system is a single, secure platform owned and operated by GSA through which members of the public can log in and access information and services from participating federal agencies ("partner agencies"). Login.gov reduces the burden of operations, maintenance and security oversight for partner agencies.[1]

GSA has developed Login.gov as a single sign-on trusted identity platform for individuals accessing any public website of any partner agency that requires user authentication.[2] However, federal agencies are not required to use Login.gov.

This Privacy Impact Assessment (PIA) analyzes how Login.gov works at level of assurance 1 (LOA1).[3] In addition to the basic requirements for LOA1, Login.gov also requires multi-factor authentication for all accounts. The National Institute of Standards and Technology (NIST) defines "assurance" as the degree of confidence in the vetting process used to establish the identity of an individual to whom a credential[4] is issued, and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.[5]

LOA1 provides a partner agency very limited assurance that the same individual who created the Login.gov account is in fact accessing that partner agency's service or information.[6] This PIA also assesses how Login.gov manages information as a strategic resource[7] and includes NIST's definitions of privacy risk, for example related to "data actions" and "PII processing."[8]

---

[1] Each partner agency is a "relying party" on Login.gov under NIST's definition of that term: "An entity that relies upon the Subscriber's token and credentials or a Verifier's assertion of a Claimant's identity, typically to process a transaction or grant access to information or a system."

[2] *See* 6 U.S.C. § 1523(b)(1)(A)-(E): Federal cybersecurity requirements.

[3] See OMB M-04-04, "E-Authentication Guidance for Federal Agencies" There are four levels of assurance, 1 to 4, with each increasing level representing in terms of the consequences of authentication errors and misuse of credentials.

[4] *See* NIST Special Publication 800-63-2, "Electronic Authentication Guideline" which defines "credential" as "an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber." In this instance, a Login.gov user is a "subscriber" and their credential is the combination of their email address and UUID.

[5] *See* NIST Special Publication 800-63-2, "Electronic Authentication Guideline."

[6] At Level 1, identity proofing is not required so names in credentials and assertions are assumed to be pseudonyms. LOA1 allows a partner agency to distinguish a user account based on the email address provided by the user and the Universally Unique Identification Number (UUID) assigned by Login.gov to that user. Each UUID is a 128-bit number used to identify other pieces of stored information.

[7] OMB CIrcular A-130

[8] *See* NISTIR 8062, "An Introduction to Privacy Engineering and Risk Management in Federal Systems."

2. Data Collected and Stored Within the System

2.1. What information will be collected, used, disseminated or maintained in the system?

Login.gov collects or generates the following PII about the user in order to create and maintain that user's LOA1 account:

PII Categories	Is collected or generated and stored by Login.gov	With user's consent, may be shared with and stored by partner agencies	Is shared with a third party provider
Email Address	**Yes**	**Yes**	
UUIDs[9]	**Yes**	**Yes**	
Phone Number	**Yes**		**Yes**[10]

As a security measure, Login.gov requires each user to provide a phone number at account creation to enable two-factor authentication (2FA).The user's phone number is only sent to the one-time password service provider, not any of the partner agencies.

The system also assigns each user a universal unique identifier (UUID)[11] during the account creation process and then an additional UUID for each partner agency that user accesses via Login.gov. The UUID is stored during each of the user's sessions so that each partner agency can use it to locate a user's profile within their own systems. For example, if an individual accesses two different agencies' information or services through Login.gov, that user will be assigned two different UUIDs. However, each agency will only be provided the user's UUID related to the user's visit to that agency's site.

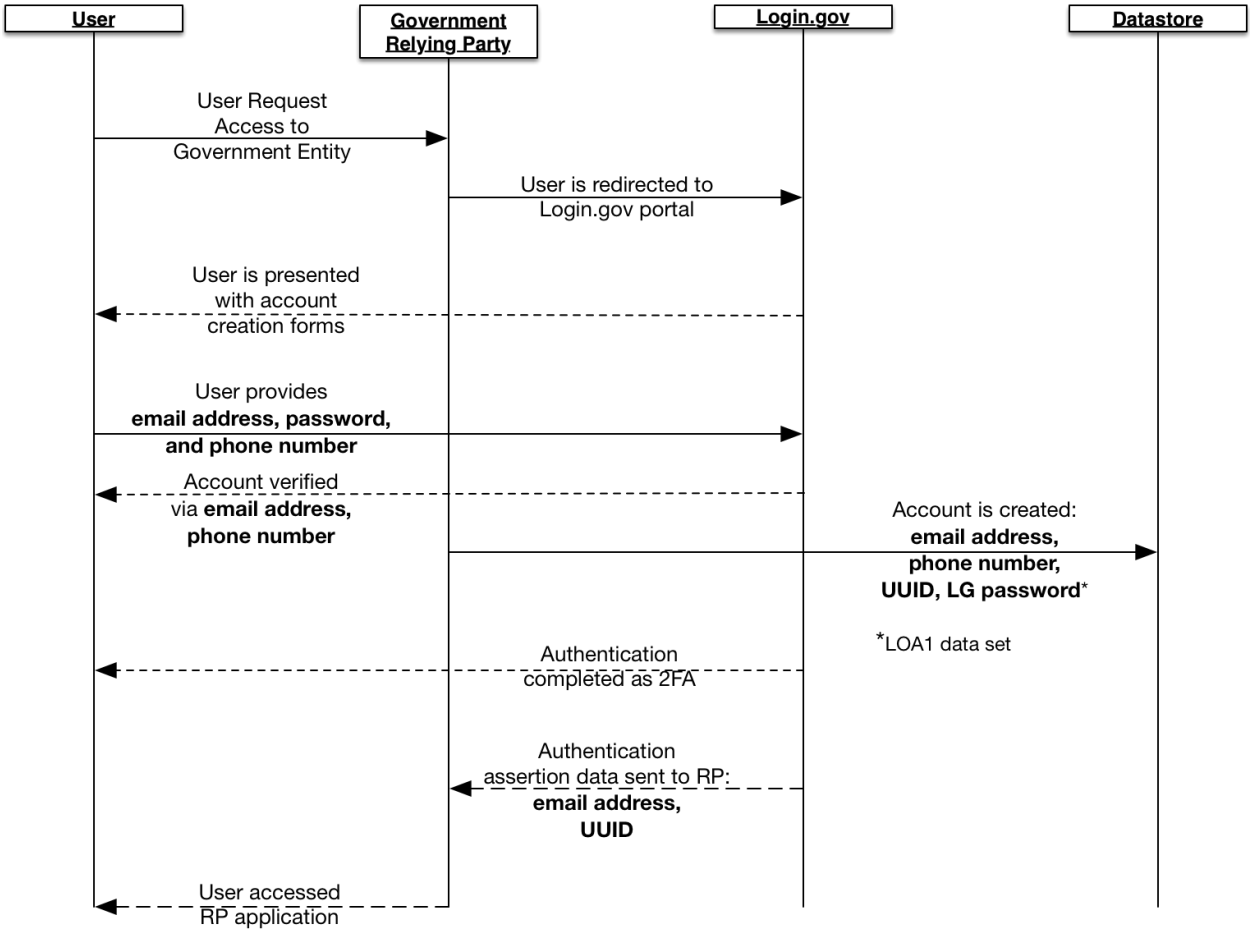
Data actions are any system operations that process PII. PII processing includes, but is not limited to, the collection, retention, logging, merging, disclosure, transfer, and disposal of PII.

[9] Multiple 'Universally Unique Identification' numbers are generated. Login.gov creates a UUID for each user in Login.gov, and additional UUIDs to send to each agency that a user visits.

[10] Phone numbers are transmitted by Login.gov to a one-time password service provider, Twilio. Twilio sends text messages and places phone calls as specified by the Login.gov system during the user's two-factor authentication process.

[11] The login.gov system uses UUID v4 strings which are composed of 128-bit numbers. Each user is assigned one UUID per partner agency that the user accesses via Login.gov.

User account creation



2.2. What will be the sources of the information in the system?

The user is the source of all of the PII collected by the system. To create an account, Login.gov collects an email address and password[12] from each user, and then collects a phone number to provide two-factor authentication. However, only the user's email address and the system-generated UUID are used to achieve LOA1.

2.3. Why will the information be collected, used, disseminated or maintained?

Login.gov shares the minimum information necessary with a partner agency to enable that user's LOA1 access to that agency's information or services.

[12] At account creation, the user is provided with recovery codes that can be used to access Login.gov if the user forgets or loses the password.

To enable two-factor authentication as a security measure, the user must provide a phone number during account creation. The user's phone number is only provided to Twilio so that it can send one-time passwords via text or phone call to that user's phone.

2.4. What specific legal authorities authorize the collection of the information?

GSA developed Login.gov pursuant to 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501.

3. Data and Records Retention

3.1. For what period of time will data collected by this system be maintained and in what form will the data be retained?

All records are stored electronically in a database in GSA's Amazon Web Services (AWS) environment. User account information is encrypted in transit (i.e., when it is shared with partner agencies) and at rest. Users can modify, or amend, any of their user account information (i.e. their email address or phone number) by accessing it in their account. That information will be maintained for at least 6 years in accordance with National Archives and Records Administration (NARA) guidance. However, GSA is authorized to maintain the information for longer if it is required for business use. Login.gov must be able to provide users access to information and services at partner agencies and therefore may have a business need to retain the information longer than the six year retention period.

3.2. What are the plans for destruction and/or disposition of the information?

System records will be disposed of in accordance with NARA's General Records Schedule (GRS) Transmittal 26, section 3.2 "System access records," which covers user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges to partner agencies for usage of Login.gov.

4. Access to and Sharing of the Data

4.1. Who will have access to the information in the system (internal and external parties), and with whom will the data be shared?

Login.gov only supports two user roles: the public user and system administrators. The public user role allows each user to make changes to their profile information after logging into the system. Each user must authorize the sharing of their email address with a partner agency in order to access that agency's services and information and to enable that agency to recognize that user on subsequent visits.

System administrators are privileged users who can gain access to Login.gov from the GSA network or via Amazon Web Services. System administrators use their elevated privileges in support of account management and to check system logs to ensure proper operation of the system and to detect potential malicious activity.

As discussed above, Login.gov will share the user's email address and UUID with partner agencies only after the user consents to that sharing. The user's phone number is provided to Twilio to enable two-factor authentication as a security measure.

4.2. If the data will be shared outside the Agency's network, how will the data be transferred or shared?

With the user's consent, the user's email address and UUID will be shared with partner agencies. That information is encrypted during transit using Transport Layer Security over Hypertext Transfer Protocol Secure (TLS over HTTPS). The user's phone number is also encrypted using TLS over HTTPS during transmission to Twilio.

4.3. If the data will be released to the public, consultants, researchers or other third parties, will it be aggregated or otherwise de-identified (i.e. anonymized)?

No, Login.gov does not release information to the public, consultants, researchers or other third parties.

4.4. Describe how GSA will track disclosures of personally identifiable information that will be shared with outside entities. The Privacy Act requires that GSA record the date, nature, and purpose of each disclosure of a record to any person or to another agency.

GSA will log the transfer of email addresses and UUIDs to partner agencies including the date and purpose for each transfer. The reason Login.gov shares users' email addresses and UUIDs with partner agencies, with user consent, is to give those agencies limited assurance that the individual who is accessing their information or services is the individual to whom the credential was issued. The reason the system provides the user's phone number to Twilio is to enable additional security via two factor authentication.

4.5. Do other systems share the information or have access to the information in this system?

No. Other systems do not have access to the information in the system. Information is shared only when a user authorizes the system to transmit information to a partner agency.

The information also may be shared in accordance with the applicable Privacy Act System of Records Notice, GSA/TTS-1, Login.gov, 82 FR 6552, January 19, 2017.

5. Notice, Consent and Access for Individuals

5.1. What notice will be provided to individuals about the collection, use, sharing and other processing of their personal data?

Each user is provided Login.gov's Privacy Policy and Terms of Use before creating an account and submitting information. The Login.gov Privacy Policy describes, among other things, what information is collected and stored automatically; how submitted information may be shared; security; and the purposes of the information collection. Users may access the Login.gov Privacy Policy on any web page of the site. In addition, this PIA is available at https://www.GSA.gov/privacy.

5.2. What opportunities will exist for an individual to decline to provide information or to consent to particular uses of the information? If opportunities exist, how will this notice be given to the individual and how will an individual grant consent?

A user must opt in to share any information with each partner agency. For example, when a user navigates to a partner agency's website and access it via Login.gov, that user is provided an opportunity to consent to that partner agency's use of the user's email address and UUID.

An email address is required to create an account. The email address the user selects to create a Login.gov account is the account through which partner agencies will share information with that user. Therefore, the user should choose an email address through which he or she would like to receive correspondence from any partner agency whose services or information he or she might access. A user can change the email address associated with his or her Login.gov account at any time, but changing that address will redirect all email correspondence with any partner agency.

The user's phone number is required to enable two-factor authentication, a security measure. If it is not provided, the user will not be able to create an account. The user should choose the number of a phone that they will have access to in order to receive and respond with the one-time password.

5.3. What procedures will exist to allow individuals to gain access to their information and request amendment/correction, and how will individuals be notified of these procedures?

An individual can access their email address and phone number to update it at any time, however updating the email address in the user account will change the address to which partner agencies send user emails and updating the phone number will change the number to which the one-time passwords are sent for two-factor authentication purposes.

6. Maintenance of Controls

6.1. What controls will be in place to prevent the misuse of the information by those having authorized access and to prevent unauthorized access, use or disclosure of the information?

The information in Login.gov is protected from misuse and unauthorized access through various administrative, technical and physical security measures. Technical security measures within GSA's AWS systems include restrictions on remote computer access to authorized individuals who hold a second factor of authentication (such as a government-issued personal identity verification (PIV) card), required use of strong passwords that are frequently changed and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals. System administrators regularly review Login.gov audit records for indications of inappropriate or unusual activity.

6.2. While the information is retained in the system, what will the requirements be for determining if the information is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

As part of the two-factor log-in process, Login.gov either calls or sends a text message to the user's phone number stored in the system every time a user attempts to sign in. That process helps to ensure that the phone number in Login.gov is accurate. Every time the user resets their password, they receive a confirmation email which serves to validate that the email address on record is accurate.

6.3. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No, the system does not provide the capability to locate an individual in real-time or monitor an individual. LOA1 only provides limited assurance that the individual accessing a partner agency's services or information is the person who initially created the Login.gov account. Each user's UUID is specific to only one agency, thereby decreasing the risk that a third party could re-identify the user across visits to different agencies.

6.4 Does this system comply with FISMA requirements to help ensure that information is appropriately secured?

Yes. GSA follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure that user email addresses, phone numbers, passwords and recovery codes[13] are appropriately secured.

The Login.gov system resides in the Amazon Web Services (AWS) East/West commercial cloud

[13] Each user is provided a recovery code when they create their Login.gov account. The code can be used to access the account if the user forgets or mistypes the password.

environment, a Federal Risk and Authorization Management Program (FedRAMP) authorized cloud infrastructure which is categorized as a moderate system under Federal Information Processing Standards (FIPS) 199. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Login.gov is comprised of web forms hosted on a web application server and a database that stores users' account information. All connections to partner agencies are protected with TLS over HTTPS using FIPS 140-2 approved algorithms.

In addition, all of the Login.gov source code is available at GitHub for public review, and the Login.gov team encourages anyone who may be interested to examine it.

6.5. Describe the privacy training provided to users either generally or specifically relevant to the program or system.

All GSA personnel are trained on how to identify and safeguard PII. In addition, each must complete annual privacy and security training. Many staff receive additional training focused on their specific job duties. For example, those who need to access, use, or share PII as part of their regular responsibilities complete additional role-based training.

7. Privacy Act

7.1. Will the data in the system be retrieved by a personal identifier in the normal course of business? If yes, explain. If not, can it be retrieved by a personal identifier?

Yes, Login.gov retrieves information by searching against stored email addresses. For example, when a user provides their email address and password in order to log into the system, Login.gov searches against all the stored email addresses in the system to find that user's account information.

7.2 Is the system covered by an existing Privacy Act System of Records Notice ("SORN")? Provide the name of the system and its SORN number, if applicable.

Yes, GSA's Technology Transformation Service (TTS) published a SORN for Login.gov on January 19, 2017, number GSA/TTS-1:
https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-a-new-system-of-records

8. Privacy Policy

8.1. Confirm that the collection, use and disclosure of the information in this system have been reviewed to ensure consistency with GSA's Privacy Policy on **www.GSA.gov**.

Login.gov will only collect, use or disclose information with the user's consent or as authorized by the system of records notice: https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-a-new-system-of-records The system's collection, use and disclosure of information comport with GSA's privacy policy and Login.gov does not make data actions (e.g. sharing a user's email address and UUID with a partner agency) without the user's consent.

9. Privacy Risks and Mitigation

Risk associated with the collection, use, dissemination and maintenance of the data

Potential Privacy Risk: Could a user's PII be accessible to individuals who do not have a need to know it?

Mitigation: To decrease the risk of the problematic data action for the user described above, the system does not retrieve a user's account information unless that user provides either their password or recovery code. See section 4.1, above. One copy of each user's account information is encrypted using their password and a second copy is encrypted using their recovery code.

When a user creates a Login.gov account, the system combines the user's password, a server-controlled random string of characters, and a hardware security module (HSM) from the AWS environment to create an encryption key. The same process occurs with the user's recovery code. The system is designed to deny access to the user's unencrypted information without that user's password or security code.

Both the user's password and security code are one-way hashed within the system. Hashing is a process of transforming strings of characters (i.e. the user's password and security code) into fixed-length values that represent the original string, but can be very difficult to reverse.

Risk associated with why the information is collected

Potential Privacy Risk: A user may not recognize the Login.gov interface when trying to access a partner agency's services or understand why the system is asking for the information it does.

Mitigation: Login.gov designers have conducted usability testing to decrease the risk that users don't have adequate prompts and explanations for what is happening. See section 5, above. The web-based interface provides visual cues and instructions while links to the Privacy Policy

and this PIA explain the overall purpose of the system.

Risk related to sources of information

Potential Privacy Risk: Why is each user required to provide a phone number to create an account?

Mitigation: LogIn.gov requires a phone number in order to allow for two-factor authentication, which is another security measure for each account. See section 2, above. However, Login.gov only provides that information to Twilio for the purpose of sending the user a one-time password. Login.gov does not provide your phone number to partner agencies.

Methodology References:
http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf