login.gov

Privacy Impact Assessment

July 13, 2018

POINT *of* CONTACT

Richard Speidel
Chief Privacy Officer
GSA IT

1800 F Street, NW
Washington, DC 20405
richard.speidel@gsa.gov

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about login.gov. In order to operate login.gov, the General Services Administration (GSA) collects emails and phone numbers, and depending on how you use login.gov, may collect and use additional personally identifiable information ("PII"). PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is divided into sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

Project

login.gov

Project/system includes information about

Any member of the public can use login.gov to sign in to multiple government agencies. The goal of the system is to make managing federal benefits, services, and applications easier and more secure.

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

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 sign 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.[3]

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

GSA has developed login.gov as a single sign-on identity platform for members of the public to access government services online that require user authentication.[4] login.gov is a shared service that federal agencies that can use and integrate with online applications; however, agencies are not required to use login.gov.

login.gov manages user authentication by allowing users to sign in with an email address, password, and a second factor on behalf of partner agencies. User authentication is the process of establishing confidence in user identities electronically presented to an information system. 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 is issued and the degree of confidence that the individual who uses the credential[5] is issued and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.[67] 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.[8] This PIA assesses how login.gov manages information as a

---

[3] Each agency partner 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."

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

[5] 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.

[6] 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.

[7] See NIST Special Publication 800-63-2, "Electronic Authentication Guideline."
5. Id.http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[8] At LOA1, identity proofing is not required; therefore any 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

strategic resource[9] and incorporates NIST's definitions of privacy risk.[10]

LOA1

When creating a login.gov account, a user signs into that agency's service with an email address and password (a user account). LOA1 allows a partner agency to distinguish a user account based on the user's self-asserted email address. LOA1 provides a partner agency minimal assurance that the same individual who created the login.gov account is accessing that partner agency's service or information.[11] LOA1 provides no information about a user's identity beyond an email address. login.gov authenticates a user only by validating that person is the owner of an account through a valid username and password.

In addition to the basic requirements for LOA1, login.gov also requires multi-factor authentication as an additional security measure. Any user may set up multi-factor authentication using either a phone number or authentication application ("app"). In addition, Federal agencies and the Department of Defense (DoD) allow employees/service members to sign in to specific applications using a personal identity verification (PIV) or common access card (CAC).[12]

Once a user creates an account, that user's account information is assigned a master universal unique identifier (UUID; also known as a "meaningless but unique number" or "MBUN") to identify the user in login.gov. This master UUID is only used within the login.gov system. The user is assigned an additional agency-specific UUID for each agency the user accesses. The user's agency UUID and the minimum set of user account information that a partner agency identifies as needed to allow access to its service is provided only after the user consents to send that information.

---

the user and the Universally Unique Identification Number (UUID) assigned by Login.gov to that user. Each UUID is a 128-bit number.

[9] OMB Circular A-130

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

[11] 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 agency-specific (UUID) assigned by login.gov to that user. Each UUID is a 128-bit number used to identify other pieces of stored information.

[12] PIV (Personal Identity Verification) cards are standardized by the NIST publication Federal Information Processing Standard (FIPS) 201, and mandated for use by executive branch agencies by Homeland Security Presidential Directive 12 (HSPD-12). Within the Department of Defense, the Common Access Card (CAC) is functionally equivalent.

PII Categories	LOA 1: stored and shared with agency partner	LOA 1: Shared with third-party provider
Email Address	**Yes**	**No**
Master Universally Unique Identifier (UUID) or MBUN[13]	**Stored within login.gov but not shared with agency partner**	**No**
Agency UUID	**Yes**	**No**
Phone Number for two-factor authentication	**Stored within login.gov but not shared with agency partner**	**Yes[14]**
PIV/CAC subject[15]	**Not stored within login.gov but may be shared with agency partner**	**No**

1.2 What legal authority and/or agreements allow GSA to collect 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. login.gov presents the following Privacy Act notice to the user when creating an account or signing in using login.gov:

Privacy Act Notice for LOA1:

GSA is asking for your email address and a phone number in order to create your account and enable two-factor authentication. You are not required to provide these; however, if you do not, you won't be able to create a login.gov account.

[13] Multiple 'Universally Unique Identification' numbers are generated. login.gov creates a master UUID for each user in login.gov, and an additional UUID to each agency that a user visits.

[14] Two-factor phone number is only shared with a one-time password provider to facilitate the two-factor authentication process.

[15] The PIV/CAC public certificate does contain the user's name in the subject. However, login.gov uses the certificate only to verify that that the PIV/CAC provided as the second factor is the correct PIV/CAC for the authenticating account. The PIV/CAC subject may be shared with partner agencies if requested and only if the PIV/CAC is presented during the login session.

This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA may use this information pursuant to its published Privacy Act system of records notice, GSA/TTS-1.

1.3 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

Yes, GSA's Technology Transformation Service (TTS) published a SORN for login.gov on January 19, 2017, number GSA/TTS-1 and modified it on August 10, 2017.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

System records will be disposed of in accordance with NARA's General Records Schedule (GRS) Transmittal 29, 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.

1.5. Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

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. The web-based interface provides visual cues and instructions while links to the Privacy Policy, Privacy Act Notice, and this PIA explain the overall purpose of the system. Additionally, login.gov designers conduct regular usability testing for functional upgrades to decrease the risk that users don't understand why they are being asked to provide personal information.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about them? If not, please explain.

Yes. login.gov only collects, uses or discloses information with the user's consent or as authorized by the system of records notice. The system's collection, use, and disclosure of information comport with GSA's adoption of the Fair Information Practice Principles ("FIPPs"), and login.gov does not make data actions (e.g., sharing a user's information with a partner agency) without the user's consent. Information is shared with a partner agency only after the user gives consent.

Each user is provided a Privacy Act Notice (see section 1.2) with links to the login.gov 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 to share submitted information; security practices; and the purpose of the information collection. Users may access the login.gov Privacy Policy on any web page of the site.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

Potential Privacy Risk: In the event a government employee uses a PIV/CAC card as a second factor, the public certificate from the card will be transmitted to login.gov as part of the login process. While this does not cause a direct risk to the government employee, the public key transmission does create a "fingerprint" which could be uniquely tracked if it were intercepted en route to login.gov.

Mitigation: login.gov mitigates this via implementation of Transport-Layer Security (TLS), which creates a cryptographically secure channel between the party with the key and login.gov's PIV/CAC service pool. The public certificate contains government employee information in the form of the "subject" of the public key containing the "Canonical Name" (i.e. full name), "Organization", and "Organization Unit" (corresponding to the card holder's full name, "U.S. Government", and top-level department name). login.gov generally does not store the public certificate.[16] Instead the PIV/CAC service pool stores a one-way hash of the public certificate, to be able to perform a lookup against a list of the hashes which correspond to a separate UUID (a MBUN) for the PIV/CAC service. That PIV/CAC

[16] login.gov temporarily stores the public certificate only if it cannot verify the validity of the certificate. For example, if login.gov does not have the signing certificate in its reference library, the certificate is expired, or the certificate is revoked, then the system will temporarily store it for further review and maintenance purposes.

UUID is then passed to the login.gov IdP service, as the unique identifier to allow for correlating a specific PIV/CAC for validation with the IdP service as a registered MFA method for that account.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

Members of the public who choose to create a login.gov account and Federal employees/DoD service members who need access to specific applications using PIV/CAC.

3.2 What PII will the system, application or project include?

PII Categories	LOA 1, stored and shared with agency partner
Email Address	**Yes**
UUIDs[17]	**Yes**
2FA Phone Number	**Stored only**
PIV/CAC Subject[18]	**Not stored within login.gov but may be shared with agency partner**

3.3 Why is the collection and use of the PII necessary to the system, application or project?

All users must provide PII to create an LOA1 account. During account creation, the user must provide an email address. To enable two-factor authentication as a security measure, the user can choose to receive one-time security codes via phone call or text message. The user can bypass providing a phone number by instead receiving the one-time security code using an authentication application. The phone number is only provided to a two-factor authentication service so that it can send one-time passwords via text or phone call to that user's phone. Each user must authorize the sharing of their email address with a partner agency to access that agency's services and information and to enable that agency to recognize that user on subsequent visits.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

[17] Multiple 'Universally Unique Identification' numbers are generated. login.gov creates a UUID for each user in login.gov, and an additional UUID to each agency that a user visits.

[18] While the PIV/CAC certificate is publishable without impacting the cryptographic use of the certificate, the public certificate does contain the user's name in the subject.

Yes, the system assigns each user a master universal unique identifier (UUID)[19] during the account creation process and then an additional agency UUID for each partner agency that user accesses via login.gov. The agency UUID is stored during each of the user's sessions so that each partner agency can use it to locate that user's profile within their systems. For example, if an individual accesses two different agencies' information or services through login.gov, that user is assigned two different agency UUIDs. However, each agency is only provided the user's agency UUID related to the user's visit to that agency's site. The system also keeps de-identified metadata related to the user's account and transactional data as described in the SORN for analytic purposes.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

login.gov only supports two types of user roles: the public user and privileged users.

Public User:
The public user role allows each user to make changes to their profile information (e.g. email address or phone number changes) 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.

Privileged Users:

Privileged users are login.gov employees and contractors that have access to login.gov systems, which require additional safeguards and controls around their actions. All privileged users have their access reviewed on a quarterly basis. Current login.gov categories of privileged users are: system administrators, developers, security personnel, auditors, and two-factor authentication service administrators.

System administrators are privileged users who can gain access to login.gov from the GSA network or via cloud 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 potentially malicious activity. All system administrator functions require multi-factor authentication.

Developers are privileged users who have some access to login.gov from the GSA network, or via cloud services. Developers use their permissions to promote new versions of the login.gov software from one environment to another (e.g. from testing to production). All developer actions taken are logged and reported and all developer functions that interact with the production environments require multi-factor authentication. All code submissions require peer review and sign-off before they can be merged into the code-base for inclusion in future versions of the software.

Security personnel are privileged users who have access to the logs generated from login.gov from the GSA network or via cloud services. Security personnel can create queries on logs from the production

[19] 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.

environment and generate alerts based on those queries. Security personnel only have access to the production login.gov environment to perform emergency shutdown procedures. All security personnel functions that interact with production systems require multi-factor authentication.

Auditors are privileged users who have access to "read" but not alter the state and data of login.gov systems. Auditors can query machines in the production environment, and report data from those queries. All auditor actions in production systems require multi-factor authentication. All auditor actions are logged and reported upon.

Two-factor authentication service administrators are privileged users with access to the 3rd party tools used for sending login.gov each user a one-time security code.

As discussed above, login.gov only shares the user's email address and agency UUID with partner agencies after the user consents to that sharing. The user's phone number is provided to a two-factor authentication service provider to enable two-factor authentication as a security measure. These user actions are logged to allow auditing against any unauthorized access to the system, since it would be possible to obtain a valid one-time security code for an account via administrative access to these systems.

3.6 Will the system, application or project monitor the public, GSA employees or contractors?

login.gov will not be used to monitor the public. login.gov has an analytics dashboard that tracks aggregate user activity. This dashboard is used to monitor business metrics and overall performance of the login.gov application but does not have access to user metadata or PII. All privileged users' actions on the system are monitored, logged, and reviewed as described in section 3.5.

3.7 What kinds of report(s) can be produced on individuals?

System administrators and security personnel can generate reports on an individual. For example, a privileged user can generate a report on user activity, such as a user's most recent sign-in, or which agencies a user has used login.gov to communicate with, and which methods of MFA the user has enabled for their account. login.gov only generates aggregated data reports about overall system health and does not monitor the individual user.

The login.gov analytics dashboard generates reports and logs on population activity such as the percentage of successful sign-ins or the total number of users. These reports do not include any metadata or PII. login.gov provides agency partners with access to similar types of reports for their application user population.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

All logn.gov traffic is subject to monitoring and recording to identify unauthorized attempts to change information, or otherwise cause damage. Information included in security reports may include IP addresses that access login.gov but will not contain other user information, for example email address and phone number.

3.9 Are there any privacy risks for this system, application or project that relate to data minimization? If so, how will GSA mitigate these risks?

Each set of data is collected solely to create an account and enable multi-factor authentication.

Potential Privacy Risk: Will login.gov collect additional sensitive PII from a user's PIV/CAC?

Mitigation: login.gov will only use a PIV/CAC as a second-factor authentication method and will not use it for authorization or identification. To verify that the PIV/CAC provided as the second factor is the correct PIV/CAC, login.gov will store a SHA-512 hash of the PIV/CAC certificate subject to be validated against the transmitted public certificate. No additional PII will be collected or stored from the PIV/CAC.[20]

[20] As discussed in section 2.2 above, login.gov temporarily stores the public certificate only if it cannot verify the validity of the certificate. For example, if login.gov does not have the signing certificate in its reference library, the certificate is expired, or the certificate is revoked, then the system will temporarily store it for further review and maintenance purposes.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Yes, PII collected is only for the purpose of account creation.

PII Categories	LOA1	Purpose
Email Address	**Yes**	Establish account
UUIDs	**Yes**	(Assigned for account identification)
2FA Phone Number	**Yes**	Enable multi-factor authentication
PIV/CAC	**Yes**	Enable multi-factor authentication

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

With the user's consent, the user's email address and agency UUID will be shared with a partner agency. The information is encrypted during transit using Transport Layer Security over Hypertext Transfer Protocol Secure (TLS over HTTPS) and inside either a Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) signed payload. The user's phone number for calls or text messages from the 3rd party two-factor authentication service provider is also encrypted using TLS over HTTPS during transmission.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The information is collected directly from the individual. Any information on a user shared with another agency is disclosed pursuant to user consent.

4.4 Will the project interact with other systems, either within or outside of GSA? If so, what is the other system(s)? If so, how? If so, is a formal agreement(s) in place?

No. Other systems do not have access to the information in the system. login.gov only shares information when a user authorizes the system to transmit information to a partner agency or third-party provider.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will GSA mitigate these risks?

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, below. 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. Additionally, login.gov designers plan on conducting regular usability testing for functional upgrades to ensure that users are clear.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

The source of the PII is the individual. PII collected for LOA1 account creation does not require verification (i.e. it is self-asserted and presumed pseudonymous). LOA1 accounts ensure the accuracy and completeness of the email address and phone number by requiring the user to confirm their email address and entering the one-time security code sent to their phone.

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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 as a security measure. See section 2, above. login.gov provides the user's phone number to a one-time password provider for the purpose of sending the user a one-time password.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the system, application or project? What is the authorization process for access to the project?

Developers, auditors and security personnel, both federal and contractor, may access user's email and phone numbers for system maintenance and troubleshooting purposes only. Additionally, they can verify both the user's last successful authentication time and which agency partners the user's credentials were disclosed to. This data is only accessed to diagnose system issues, and only if other attempts at remediating the issue have failed.

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

Yes. GSA has completed a system security plan for login.gov and has a "moderate" impact system authority to operate (ATO) in place. That ATO was granted based on GSA's internal Lightweight ATO ("LATO" process) and login.goiv is working toward a Federal Risk and Authorization Management Program (FedRAMP) Moderate authorization.

6.3 How will the system, application or project be secured from a physical, technological, and managerial perspective?

login.gov's physical security is provided by its cloud service provider. login.gov's cloud service provider is FedRAMP authorized, and has provided login.gov with a set of virtual private clouds to separate it from other physical assets.

login.gov manages technological security via a defense-in-depth approach, minimizing access at every level, with strong encryption of data both in transit and at rest. By maintaining strict control over the flow of information at every step within the system, login.gov is able to provide robust technical security. Additionally, other services run on top of login.gov to further detect any compromised systems, atypical system behavior, and/or data disclosure.

login.gov manages security from three aspects of control: auditing of access, vetting of privileged users, and enforcing principles of least-privileged access. By keeping all audit logs for any action taken as a privileged user on login.gov systems, there is a robust history maintained to determine who made any changes, and when. By using background check investigations for privileged users, login.gov seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged

access, login.gov will both restrict access to the minimum possible levels, restricting the chance of any disclosure or abuse. Additionally, all of these managerial controls are subject to regular review.

6.4 Are there mechanisms in place to identify security incidents and breaches of PII? If so, what are they?

Yes, login.gov has an incident response plan and conducts incident and breach response exercises. Additionally, the system uses tools from the cloud service provider that heuristically detect both security incidents and potential breaches of PII. These tools both offer additional insight on avenues of breach that may not be alarmed directly, and provide real-time insight about trends and flows of data to further enhance responsiveness.

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

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 only allows privileged, vetted users to access email addresses, phone numbers or PIV/CAC public certificates for maintenance and trouble-shooting purposes. All such access is logged and audited.

Both the user's password and recovery codes are one-way hashed within the system. Hashing is a process of transforming strings of characters (i.e. the user's password and recovery codes) into fixed-length values that represent the original, but can be very difficult to reverse.[21]

[21] To hash passwords and recovery codes, login.gov builds a consumer encryption key from an SCrypt digest of the password and a random value encrypted on an hardware security module (HSM). The stored hash is the result of the taking a SHA256 digest of the consumer encryption key.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of the project? If no opportunities exist to consent, decline or opt out, please explain.

login.gov only gathers PII directly from the user during account creation or when the user is modifying their information. A user must also opt in to share any information with each partner agency. For example, when a user navigates to a partner agency's website to 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.

login.gov provides a Privacy Notice with links to its security practices and Privacy Act statement on the sign in and create account page. Partner agency branding is also included throughout the sign in and create account process to ensure the user knows which agency login.gov they are disclosinging information to.

7.2 What procedures allow individuals to access their information?

Individuals with a login.gov account can sign into their account at any time to access their information when they present their username, password, and 2FA method.

If a user loses their password, they can reset it through access to their email and presentation of their 2FA method. If a user loses access to their two-factor authentication method, the user can access their account using their personal key. If they do not have access to their personal key, they will be unable to access their account and must create a new one.

7.3 Can individuals amend information about themselves in the system? If so, how?

The login.gov account page allows a user to update or amend any PII in the system. The user is also able to view their account history as well as delete their account.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

System administrators and other privileged users have no access to sensitive personally identifiable information. The user retains full control of their data and the means to update it.

Potential Privacy Risk: Can users easily navigate to their login.gov account page to amend PII or delete information?

Mitigation: Yes, users are presented with their account page immediately upon logging in. However, users might change PII on a partner agency application and mistakenly think they have amended their login.gov data. Potential confusion could be the result of login.gov having a separate sign in page to access a user's account page. Login.gov uses branding to clarify the difference between login.gov and the partner agency application's functionality.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

Potential Privacy Risk: Is the required training for GSA personnel adequate and effective in terms of content and structure?

Mitigation: In addition to the training required by GSA, login.gov limits the use of access to user PII through strict permission sets and maintaining audit logs of employee and contractor activity. This is applied to data stored on the login.gov platform as well as PII data gathered from customers across customer service channels. All employees and contractors are also trained to immediately report suspected or confirmed IT security incidents and PII breaches and any inappropriate use of GSA systems to the GSA IT Service Desk.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's privacy program is designed to make the agency accountable for complying with these principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

login.gov regularly reviews its operations to ensure that they meet the requirements outlined in this PIA. Program leaders and developers are held accountable for adhering to privacy best practices related to data minimization, transparency, and timely, effective notice. For example, login.gov has created a transparent system built upon an open-source platform so that interested parties can advise the development team and so that the system owner remains accountable to the public and partners across the government. Further, login.gov is building a system that tells users what it does with their information to create accountability and build trust. It engages developers and other interested parties through a GitHub repository and provides other public forums where people can discuss the work.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

As discussed above, login.gov has adopted a privacy by design model and works closely with security and privacy advisors to ensure that it identifies potential privacy risks early and mitigates them in a timely, efficient fashion. login.gov recognizes that the success of the project requires maintaining the public trust. That's why it has adopted modern privacy practices and a transparent, open-source development platform.