Login.gov

Privacy Impact Assessment

Jan 16, 2024

POINT *of* CONTACT

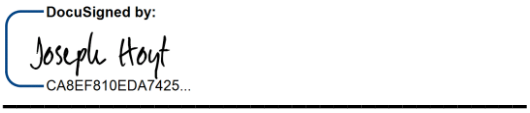
Richard Speidel

Acting Chief Privacy Officer
GSA IT

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

Signature Page

Signed:



Joseph Hoyt - IST Information System Security Manager (ISSM)

Daniel Lopez-Braus - QQ2Program Manager/System Owner

Richard Speidel - IDEChief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Table of contents

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

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?

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?

SECTION 8.0 AWARENESS AND TRAINING

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

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?

Document purpose

This document contains important details about Login.gov. In order to operate Login.gov, the General Services Administration (GSA) collects email addresses and depending on how you choose to 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.

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]

---

[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.

[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."

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 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, multi-factor method, and identity verification by verifying an individual's asserted identity on behalf of partner agencies. User authentication is the process of establishing confidence in user identities electronically presented to an information system. Identity verification is the process of verifying that a person is who they say they are. PII must be collected from a Login.gov user to verify the identity of that user at the requisite level of rigor required by a partner agency to grant access to its information, applications, programs, or records (for the purpose of this PIA, ‘‘services"). The National Institute of Standards and Technology (NIST) defines identity assurance level (IAL) as “a category that conveys the degree of confidence that the applicant’s claimed identity is their real identity.”[5] Login.gov identity verification services do not meet NIST IAL2 standards at this time but provides strong identity assurance via an identity verification process that includes:

- Document authentication
- Records check
- Address confirmation
- In person identity verification
- Fraud controls

Login.gov offers two types of services: authentication and identity verification. A user will only be asked for information necessary to achieve the type of service required by the partner agency to access their resources. Authentication provides a partner agency assurance that the account holder is, in fact, accessing that partner agency’s service or information.[6] This PIA analyzes how Login.gov works at both service levels; describes how Login.gov manages information as a strategic resource;[7] incorporates NIST's definitions of privacy risk; and describes how Login.gov

[4] *See* 6 U.S.C. § 1523(b)(1)(A)-(E): Federal cybersecurity requirements.
[5] *See* NIST Special Publication 800-63-3, “Digital Identity Guidelines”
[6] At IAL1, identity verification is not required; therefore any names in credentials and assertions are assumed to be pseudonyms. The authentication-only service 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.
[7] OMB Circular A-130.

mitigates such risks.[8] Login.gov also secures the integrity of these services by implementing fraud controls designed to detect account take-over and identity impersonation. This PIA describes the most stringent fraud controls currently in effect.

Authentication

When creating a Login.gov account, a user signs into that agency's service with an email address and password (a user account). Authentication allows a partner agency to distinguish a user account based on an email address provided by the user. Authentication 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. Per NIST guidelines, "There is no requirement to link the applicant to a specific real-life identity."[9] Login.gov authenticates a user only by validating that person is the owner of an account through a valid email address and password.

In addition to the basic requirements for authentication, Login.gov also requires multi-factor authentication (MFA) as an additional security measure for all accounts. Any user may set up multi-factor authentication using either a phone number, security key, or authentication application ("app"). In addition, federal agencies and the Department of Defense (DoD) allow employees/service members to use a personal identity verification (PIV) or common access card (CAC)[10] as an additional factor when signing into specific applications. PIV and CAC cards are only used as an additional factor beyond email and password, and by themselves cannot be used to sign into a Login.gov account.

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.

Identity verification

Identity verification provides a partner agency substantially more assurance that the same individual who created the Login.gov account is accessing that partner agency's service or

[8] *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.

[9] See NIST Special Publication 800-63-3, "Digital Identity Guidelines"

[10] 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.

information. Login.gov asks the user to provide the following PII:

- full name,
- date of birth,
- home address,
- Social Security Number,
- the type and number of the state-issued identification card (ID),
- images of the front and back of the state-issued ID card,
- and, with consent, Login.gov may use the contact phone number provided to confirm home address.

Access to an identity verified account still requires strong authentication.

Login.gov verifies a user's identity by comparing the user-provided account information to data maintained by a third-party authoritative source. Third-party identity verification services used by Login.gov may employ a variety of verification techniques, including but not limited to:

- verifying a user's self-reported personal information,
- details from a user's government-issued identification
- physical (in-person) verification

The identity verification process between the Login.gov system and third-party identity verification services takes place after the user provides the required account information. For example, Login.gov will request information about a state-issued ID type and date of issuance, and Login.gov will then relay it to the third-party identity verification service. The third-party identity verification service does not keep this information after the identity verification event has completed.

Currently, Login.gov is testing the use of a self-photograph for identity verification– to match against a user’s government issued-ID photograph. Self-photographs used for testing purposes are submitted by volunteer testers.

Table 1: Data Used for Authentication and Identity Verification

PII Category	Data Used for Authentication or ID Verification	Stored within Login.gov	Shared with Agency Partner	Shared with Third-Party Provider[11]
Email Address	Both	Yes	Yes	Yes, during ID verification only
Master Universally Unique Identifier[12] (UUID) or MBUN	Both	Yes	No[13]	No
Agency UUID	Both	Yes	Yes	No
Multi-Factor Authentication (MFA) Phone Number	Both	Yes	No[14]	Yes[15]
Short Messaging Service (SMS) Phone Number	Authentication	Yes[16]	No	No
PIV/CAC subject[17]	Both	Yes	Yes[18]	No
Contact Phone Number	ID Verification Only	Yes	Yes	Yes
Full Name	ID Verification Only	Yes	Yes	Yes
Address	ID Verification Only	Yes	Yes	Yes

[11] Each third-party identity verification service will send information back to Login.gov about its attempt to verify the identity of the user including: transaction ID; pass/fail indicator; date/time of transaction; and codes associated with the transaction data.
[12] 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.
[13] Login.gov does not share the Master UUID with third-party providers for the purpose of authentication or identity verification, but does share MBUNs with third-party fraud controls services to support fraud analytics as documented in Table 3.
[14] MFA phone number is not shared with partners for the purpose of authentication or identity verification.
[15] MFA phone number is only shared with a one-time password provider to facilitate the multi-factor authentication process.
[16] SMS phone number is used for in person proofing users who opt-in to receive alerts about account status. The phone number is deleted after 30 days.
[17] The PIV/CAC public certificate does contain the user's name in the subject. However, Login.gov uses the certificate only to verify that the PIV/CAC provided as the second factor is the correct PIV/CAC for the authenticating account
[18] The PIV/CAC certificate subject may be shared with partner agencies if requested and only if the PIV/CAC is presented during the login session.

PII Category	Data Used for Authentication or ID Verification	Stored within Login.gov	Shared with Agency Partner	Shared with Third-Party Provider[11]
Date of birth	ID Verification Only	Yes	Yes	Yes
Social Security Number	ID Verification Only	Yes	Yes	Yes
Contact Phone Number	ID Verification Only	No	Yes	Yes
State-issued ID Image	ID Verification Only	No	No	Yes
State-issued ID Type[19]	ID Verification Only	No	No	Yes
State-issued ID number	ID Verification Only	No	No	Yes
State-issued ID state of issuance	ID Verification Only	No[20]	No	Yes
Issuance data	ID Verification Only	No	No	Yes
Expiration date	ID Verification Only	No	No	Yes

Fraud controls to prevent account takeover and identity impersonation

Login.gov is employing several controls to limit account takeover and identity impersonation types of fraud.

Login.gov is leveraging third-party services to:

[19] State-issued ID type indicates the type of ID presented: driver's license, permit, or state ID.
[20] State-issued ID state of issuance is stored by Login.gov for debugging purposes.

- Confirm device integrity, characteristics, reputation and association with individual
- Validate behavioral analytics, such as usage of mouse, keyboard, and interaction with the webpage.
- Confirm Internet Protocol (IP) address and email reputation
- Protect against synthetic identities (false identities created by fraudulent actors)

These third-party services are embedded into Login.gov's authentication and identity verification services. They require collection and retention of additional information about the user and the user's device as documented in Table 2.

For more information on the privacy impact associated with Login.gov's use of LexisNexis for fraud detection and mitigation, see the LexisNexis Privacy Policy for Nonfederal Systems: (https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems).

Table 2: Data Used for Fraud Mitigation

PII Category	Account Type (Authentication or ID Verification)	Stored within Login.gov	Shared with Agency Partner	Shared with Third-Party Provider[21]
Email Address	Both	Yes	Yes	Yes, during ID verification only
Master UUID or MBUN	Both	Yes	No	Yes
Agency UUID	Both	Yes	Yes	No
MFA Phone Number	Both	Yes	No	Yes
Contact Phone Number	ID Verification Only	Yes	Yes	Yes
Full Name	ID Verification Only	Yes	Yes	Yes
Address(s)	ID Verification Only	Yes	Yes	Yes
Date of Birth	ID Verification Only	Yes	Yes	Yes

[21] Each third-party fraud service will send risk information back to Login.gov about the identity verification attempt: transaction ID; pass/fail indicator; date/time of transaction; and codes associated with the transaction data.

PII Category	Account Type (Authentication or ID Verification)	Stored within Login.gov	Shared with Agency Partner	Shared with Third-Party Provider[21]
Social Security Number	ID Verification Only	Yes	Yes	Yes
State-issued ID Image	ID Verification Only	No	No[22]	Yes
Detailed User Device Information Fingerprint I.E. (Browser, client IP address, geolocation, installed components, processor, screen resolution, user agent)	Both	No	No	Yes[23]
Additional Device information (User agent, hashed session id, user, agency partner, uuid, LG generated device fingerprint)	Both	Yes	No	No
3rd Party Javascript generated Device Fingerprint	ID Verification Only	Yes	Yes	Yes
3rd Party Biometrics Keyboard behavior Mouse behavior Touchscreen Behavior Other Device Sensors	Both	No	No	Yes[24]

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's Privacy Act notice can be found on Login.gov's public facing website (https://login.gov/policy/our-privacy-act-statement/).

[22] Once state-issued ID images have been processed for authenticity, Login.gov does not store them for the purpose of fraud mitigation.
[23] This data will be sent to LexisNexis Threatmetrix DDP for fraud analysis. This data will be sent to Google reCAPTCHA for bot detection and mitigation.
[24] During identity verification, this data is sent from the user's browser to LexisNexis's (LN) Biometric Behavioral Device Fingerprinting solution for fraud detection. During authentication, this data is sent from theuser's browser Google reCAPTCHA for bot detection and mitigation.

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, GSA/TTS-1 and the most recent modification of which was published on November 21, 2022.

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.

Yes. Information is maintained in accordance with GSA's Records Retention Schedule, GRS 03.2, System Access Records.

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:

- user profiles
- log-in files
- password files
- audit trail files and extracts
- system usage files
- cost-back files used to assess charges for system use

Exclusion 1. Excludes records relating to electronic signatures.

Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Retention:

- For systems not requiring special accountability for access: Temporary. Destroy when business use ceases.
- For systems requiring special accountability for access: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

For data retention schedules external systems to Login.gov, please refer to their specific retention record schedules. These include but are not limited to:

- USPS

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 aforementioned SORN. 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.

Links to the Login.gov Privacy Practices and Rules of Use are shown to the user before creating an account and then again when submitting information needed for identity verification. The Login.gov Privacy Practices 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. It also links to the Login.gov Privacy Act Statement (see section 1.2) Users may access the Login.gov Privacy Practices on any web page of the site. The user must agree to the Rules of Use prior to creating an account and again at the beginning of identity verification.

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 attempt 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?

Refer to table in section 1.1.

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

All users must provide an email address to create an account and additional PII is necessary for agency applications that require users to successfully verify their identity.

During account creation, the user must provide an email address and create a password. To enable multi-factor authentication as a security measure, the user can choose to receive one-time security codes via phone call or text message. If users prefer not to provide a phone number for this purpose, they can instead receive the one-time security code using an authentication application. If provided, the user's phone number is provided to a multi-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.

Additional PII is collected in order to verify a user's identity and store it on the account. Full name, date of birth and social security number are needed to match the user's identity to a single individual. The collection of state ID details, address, and phone number confirms the user has access to records associated with the identified individual. Information collected for identity verification is shared with third-party identity verification services.

Collection and storage of information about the user's device and behavior is necessary to maintain the integrity of the system (by detecting account takeover or identity impersonation).

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?

Yes, the system assigns each user a master universal unique identifier (UUID)[25] during the account creation process and then an additional agency UUID for each partner agency a 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 for analytic and debugging purposes. For example, metadata is used to identify user-interaction types, including which types of browsers access Login.gov, which multi-factor methods are used, and how many Login.gov users access each agency partner site.

[25] 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.

The system aggregates information required to protect it from unauthorized use. The system relies on a third-party service to collect information about the user's device and behavior to detect possible account takeover or identity impersonation. The third-party encrypts this information and stores it in a data store that is accessible only by Login.gov. The third-party uses the information in its encrypted form to perform fraud checks, protecting the privacy of the user information.

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

Login.gov 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, phone number) 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. Users trying to access agency applications and services that require identity verified attributes during authentication will be prompted to authorize the sharing of additional data with the partner agency.

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 multi-factor authentication service administrators, and USPS clerks.

System administrators are privileged users who can access 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 successful completion of automated unit tests, smoke tests, and security tests followed by a peer review and then signed-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 environment and generate alerts based on those queries. Security personnel only have access to the production Login.gov environment in order 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.

Multi-factor authentication service administrators are privileged users with access to the third-party tools used for sending each user a one-time security code.

USPS clerks are privileged users that can access the Name and Address of a user after the user has presented a unique enrollment 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. If provided, the user's phone number is provided to a multi-factor authentication service provider to enable multi-factor authentication as a security measure. These user actions are logged to allow auditing against any unauthorized access to the system, since it could be possible to obtain a valid one-time security code for an account via administrative access to these systems.

To facilitate identity verification, Login.gov will share the information in Table 1 received from the user with third-party providers[26] only after the user consents to that sharing.

Hashing and Asymmetric cryptography

Information transmitted to partners is encrypted in transit and is hashed, where possible..

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

Login.gov monitors users, which includes the public, and government personnel to prevent fraud. Login.gov will use the following LexisNexis services: ThreatMetrix, FraudPoint and

[26] Refer to LexisNexis PIA for information on how those third parties are required to manage PII

Emailage. These services will monitor the Login.gov users via behavioral biometrics[27] during the identity verification process to understand their behavior and to determine if a fraudulent participant is involved during this process. For more information on those monitoring services, please refer to the LexisNexis PIA (https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems). Information required from the user to conduct this inspection is listed in Table 2.

Login.gov also 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 present 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 to investigate potential incidents, diagnose problems and for related purposes. 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 access, and which methods of multi-factor authentication the user has enabled for their account. These user activity reports can be generated based on any combination of analytics attributes that are tracked. Tracked attributes are listed in Table 2: Data Used for Fraud Mitigation. User-specific fields such as email and MFA phone are not tracked directly, but a database query can reveal the UUID associated with an email or phone number, which can then be queried. Login.gov also generates aggregated data reports about overall system health.

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, and can be accessed by all privileged 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.

Login.gov uses a third-party dashboard that will enable Login.gov to revisit anti-fraud assessments. When suspected fraud occurs, a case is generated for review. This dashboard is accessible to Login.gov administrators and anti-fraud staff, who can confirm fraud or provide redress for users. Please refer to section 2.3 of the Lexis Nexis PIA (https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems) for what reports on individuals can be generated from this information.

[27] Behavioral biometrics analyzes a user's digital physical and cognitive behavior to distinguish between cybercriminal activity and legitimate use.

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 Login.gov traffic is subject to monitoring and recording to identify unauthorized attempts to change information, jeopardize the confidentiality, integrity or availability of Login.gov or otherwise cause damage. Information included in security reports may include IP addresses, master and agency UUID, and user agents that access Login.gov. The term "user agent" is a technical term which is loosely equivalent to the browser the user was on when they went to Login.gov, there is no PII associated with it.

In order to support user redress in suspected fraud, and fraud investigations, Login.gov may match information within the Login.gov system and LexisNexis to re-identify individuals. This activity is only performed to support redress in the case of potential identity theft or fraud, or in the case of an active fraud investigation. Data included and re-identified in these reports is limited to what is necessary to provide redress and support fraud investigations as permitted by the Login.gov SORN.

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, identity verification and fraud mitigation.

PII Categories	Authentication	Identity Verified	Purpose
Email Address	**Yes**	**Yes**	Establish account
Master Universally Unique Identifier (UUID) or MBUN	**Yes**	**Yes**	Assigned for account identification
Agency UUID	**Yes**	**Yes**	Assigned for account identification

Phone Number for multi-factor authentication (MFA)	**Yes**	**Yes**	Enable multi-factor authentication
Phone Number for text message alerts (SMS) - in person proofing only	**Yes**	**Yes**	Establishing account Protection against account takeover and identity impersonation.
PIV/CAC subject	**Yes**	**Yes**	Enable multi-factor authentication
Full Name	**No**	**Yes**	Identity resolution
Address	**No**	**Yes**	Identity verification
Date of Birth	**No**	**Yes**	Identity resolution
Social Security Number	**No**	**Yes**	Identity resolution
State-issued Type	**No**	**Yes**	Identity verification
State-issued ID Number	**No**	**Yes**	Identity verification
Contact Phone Number	**Only if same phone number as MFA number**	**Yes**	Verify state-issued ID address
3rd party Detailed User Device Information Fingerprint I.E. (Browser, IP address, geolocation, installed components, processor, screen resolution, User agent)	**Yes**	**Yes**	Protection against account takeover and identity impersonation. Bot detection and mitigation.
Login.gov generated additional Device information (User agent, hashed session id, user, agency partner, uuid, device fingerprint)	**Yes**	**Yes**	Protection against account takeover and identity impersonation.
3rd Party Biometrics (Keyboard behavior Mouse behavior	**Yes**	**Yes**	Protection against account takeover and identity impersonation.

Touchscreen Behavior Other Device Sensors)			Bot detection and mitigation.

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. If the partner agency requires identity verification information for users authenticating via Login.gov, then those users' self-asserted PII, including name, address, social security number, birth date and/or contact phone number could also be transmitted pursuant to the user's consent and the agreement between Login.gov and the partner agency. That 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 third-party multi-factor authentication service provider and additional information required for identity verification are also encrypted using TLS over HTTPS during transmission.

During in-person identity verification, the user's name and address will be shared with USPS over an encrypted channel. For in-person verification, users can also provide a phone number for SMS alerts about the status of their account creation and identity verification. This phone number will be encrypted and stored for 30 days and then deleted.

During identity verification and login per the table in the previous paragraph, device information and behavioral biometrics will be collected via the use of a 3rd party Javascript, and then stored in a 3rd party data store. When accessing Login.gov, the 3rd party will assess the device's risk, and its association with the user, it will not identify the user. Login.gov operators do not have access to behavioral information or personally identifying information.

To other Federal agencies or Federal entity, when GSA determines that information from this system 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.

Login.gov will share user PII to USPS if the user elects to for in person proofing. This information is sent over an encrypted channel in order for USPS to ensure the presented identity

document is the same as login.gov has validated during the validation process. The USPS PIA is located on the USPS's website.

During the identity verification process, Login.gov will share data with authoritative sources for validation, as well as LexisNexis, a third party service which is used for identity proofing and anti-fraud purposes. For additional details, please see the LexisNexis PIA (https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems). Login.gov shares this data over secure encrypted channels. Login.gov establishes agreements with third party services that limits further use of the data for commercial purposes.

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)?

During account creation and identity verification information is collected from or asserted directly by the individual. Any user information shared with a partner agency is disclosed only pursuant to user consent. Third-party providers only verify the information provided by the user and do not provide any information to partner agencies. Third-party identity identity verification services only send the following information back to Login.gov: transaction ID; pass/fail indicator; date/time of transaction; and codes associated with the transaction data.

A third-party javascript also collects information from the device and behavioral biometrics in order to validate device integrity and user behavior.

Other information is received from LexisNexis anti-fraud services, including both plain and hashed (de-identified) information about other accounts, devices and activity associated with an individual.

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?

Yes. Login.gov interacts with other systems outside of GSA in the following ways:

1. As a relying party of the Login.gov.
    a. Interaction with other systems:
        i. As mentioned in earlier section 1.1, Login.gov acts as an identity credential provider for applications that require the user to verify their identity.

ii. Before Login.gov shares any validated PII it has on a user to that relying party, Login.gov gains explicit consent from the user. The user must enter their password to provide that consent.

b. Agreements:

i. Yes, a formal Interagency Agreement is executed between Login.gov and the relying party before any information is shared.

2. As an identity verification service (government provided and commercial third-party)

a. Interaction with other systems:

i. Section 1.1 describes the interaction between Login.gov and identity verification services.

b. Agreements:

i. A formal contract always exists between Login.gov and any non-government identity verification service. This contract also specifies the strict privacy practices they must follow.

ii. A formal Interagency Agreement is executed between Login.gov and USPS for in person identity verification.

3. As a provider of anti-fraud controls to Login.gov

a. Interaction with other systems:

i. As mentioned earlier in section 1.1, Login.gov relies on 3rd parties outside of GSA to provide fraud signals and anti-fraud controls.

ii. See section 3 on how Login.gov interacts with these providers.

b. Agreements:

i. Yes, a formal contract always exists between Login.gov and any non-government (3rd party) service.

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 authentication-only account creation does not require verification (i.e. it is self-asserted and presumed pseudonymous). Login.gov ensures the accuracy and completeness of the user's email address and phone number (if provided for MFA) by requiring the user to confirm their email address and entering the one-time security code provided to them.

PII for identity-verified accounts is verified by matching the user's self-asserted information and information collected from evidence against other records to establish a level of confidence that the PII represents who the person claims to be. Login.gov will contact a number of third-party authoritative sources and identity verification services to verify the user provided PII. Each third-party identity verification service will return identity verification, risk, or resolution pass/fail information based on the user-provided data. Only after a user has been able to meet Login's identity verification standards will they be allowed to use Login.gov to connect to partner agency services that require identity verification.

Information regarding the device and user's interaction with the device are also collected to assess device integrity and risk. Please refer to the LexisNexis PIA section 4.1 for more detail on how that assessment is conducted.

In the case of a redress or fraud investigation, Login.gov may collect information from third party anti-fraud services. This may include information about other devices associated with an individual. This information is used by fraud investigators to verify the user's provided information and risk indicators to make a redress or fraud determination.

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?

Within Login.gov:

Developers, auditors, and security personnel, both employee and contractor, may access a user's email address, hashed social security number, and optional MFA phone number for system maintenance, troubleshooting and incident response purposes only. Additionally, these personnel can verify both the user's last successful authentication time and which agency partners the user's information were disclosed to. Additionally, users who use a PIV/CAC as a multi-factor method may have their PIV/CAC public certificate stored temporarily and accessed by privileged users in the event that the certificate could not be properly validated, as discussed in section 6.5. PII aside from email address, hashed SSN and optional MFA phone number is encrypted and inaccessible to the Login.gov system without the user's password and a successful authentication by the user. Login.gov systems will only keep the data unencrypted in memory during active login sessions.

Third Party Services:

Login.gov administrators and anti-fraud staff have access to the anti-fraud dashboard outlined in section 3.7.

Partners:

Certain security-significant user activity events, such as account recoveries, account lockouts, password rests, and account recovery are made available to partner agencies via the Login.gov Security Event API, https://developers.login.gov/security-events/. This API provides details that an event occurred, but does not provide PII or sensitive information to partner agencies.

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, which is designated as a FISMA "moderate" impact system and has a GSA-issued FedRAMP authority to operate (ATO) in place.

LexisNexis is also undergoing a 3rd party assessment to certify that its controls meet the NIST 800-171 standards for Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Positive preliminary assessment findings have been shared with a formal certification anticipated in 2023.

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 detailed history maintained to determine who made changes and when. By using background check

investigations for privileged users and individuals with access to user PII, Login.gov seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged access, Login.gov restricts access to the minimum required levels, decreasing the risk of unauthorized 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.

Third party services and agency partner systems that are integrated with Login.gov are also required to report any breaches / compromise of information provided by Login.gov.

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 an identity verified 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, UUID and potentially other information as required by the partner agency.

Login.gov supplements its identity verification flow with technologies that provide anti-fraud controls. Users must consent to the use of these technologies during the identity verification process. Users should reach out to the partner agency for other mechanisms to access systems integrated with Login.gov if they do not wish to consent to this collection.

Login.gov provides links to its security practices and Privacy Act Statement on the sign in and create account page for both authentication and identity verified accounts. 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 disclosing 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 email address, password, and multi-factor method.

If a user loses their password, they can reset it through access to their email and presentation of their multi-factor method. If user loses access to their multi-factor authentication method, the user can access their account using their personal key. If the user does not have access to their personal key, they can request to delete their account without signing in. When a user requests to delete their account, Login.gov sends a notification to the email and the phone number associated with the account, if provided for MFA purposes. As a security measure, the user must wait 24 hours after submitting the request before deleting the account. After 24 hours, the user will receive a second email with a link to confirm the account deletion. Completing this process will allow the user to reset their Login.gov account using the same email address. However, deleting the account removes any agency applications previously linked to the account.

Users can access information retained by LexisNexis by following the procedures listed in the published Privacy Impact Assessment on the GSA privacy page for non-federal systems (https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-for-nonfederal-systems).

Users may also access records about themselves by submitting a Privacy Act request following the instructions on GSA's Privacy Program webpage.

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 used for account authentication (email address or optional multi-factor phone number). The user is also able to view their account history as well as delete their account. To amend the additional PII that is used for identity verified/AAL2 verification, the user must delete their account, create a new account, and verify their identity. System administrators and other privileged users are not permitted to modify PII on a user's behalf. The user retains full control of their data and the means to update it.

Users can amend information retained by LexisNexis by following the procedures listed in the published Privacy Impact Assessment on the GSA.gov/privacy website.

Users seeking technical assistance signing into their account may contact the Login.gov contact center.

Users may also amend information about themselves by submitting a Privacy Act request following the instructions on GSA's Privacy Program webpage.

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.

AntiFraud staff are trained on permissible activity prior to beginning work.

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 the PIA, 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 program. 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 public source code repository, which includes a public forum for discussion of the project.

Login.gov continually monitors the security and compliance status of any third-party systems that data is shared with on a regular basis. Ensuring that these systems maintain functioning security and privacy controls and manage data according to this and vendor specific PIAs.