Privacy Impact Assessment for Login.gov LOA1

March XX, 2017

1. Overview

Login.gov is an authentication platform to make the public's online interactions with the U.S. government simpler, more efficient and intuitive. The system is a single, secure platform owned and operated by GSA through which members of the public can log-in and access services from participating federal agencies (partner agencies), including GSA. Login.gov will reduce the burden of operations, maintenance and security oversight for GSA's partner agencies within the Federal government.

Federal agencies are not required to use Login.gov to authenticate members of the public who seek access to information or services. GSA's role is to "implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication,"[1] and each federal agency is free to select the authentication platform(s) and/or service(s) that best meet its needs.

This Privacy Impact Assessment only analyzes Login.gov's mode of operation at level of assurance 1 (LOA1) because Login.gov currently provides only LOA1. 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 is the individual to whom the credential was issued.[2] For example, at LOA1 no identity proofing is required – all an individual must provide is an email address. In order to add a layer of increased security, Login.gov asks for a phone number which is used to enable two-factor authentication (2FA).

LOA1 provides limited assurance that the same individual who created the Login.gov account is in fact accessing the partner agency's service or information. In turn, LOA1 allows a partner agency to distinguish a user account based on the email address provided by the user and a UUID assigned by Login.gov to that user.

Login.gov is hosted in the Amazon Web Services (AWS) East/West commercial cloud environment, a Federal Risk and Authorization Management Program, or FedRAMP, authorized cloud infrastructure. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The Login.gov system is managed day-to-day by GSA staff.

[1] *See* 6 USC 1523(b)(1)(A)-(E): Federal cybersecurity requirements.

[2] *See* NIST Special Publication 800-63-2, "Electronic Authentication Guideline." 800-63-3 will include mapping… In addition, Office of Management and Budget M-04-04, "E-Authentication Guidance for Federal Agencies" defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of credentials.

The system is a cloud based architecture operating on Amazon Web Services. Login.gov is comprised of web forms based web application server, workers servers to service transactions from a service queue forms and a database that stores users' account information. All connections to partner agencies are protected with via HTTPS using FIPS 140-2 approved algorithms. Access with Login.gov is restricted with configurations based on their SAML/OIDC signing certificates and their application URL….   In addition, all of the Login.gov source code is available at github for community review and is continuously inspected for vulnerabilities by the Login.gov team….

This PIA covers the nature and purpose of the information being collected by Login.gov in the context of its mission to provide appropriate usability, security, and privacy to members of the public seeking access to federal agencies' services and information. The framework used for the assessment focuses not only on managing Login.gov information as a strategic resource, but also encompasses definitions of privacy risk found in NISTIR 8062 related to "data actions," and "PII processing."[3]

2. Data Collected and Stored Within the System

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

User account data, as defined above will be collected, used, disseminated, or maintained:

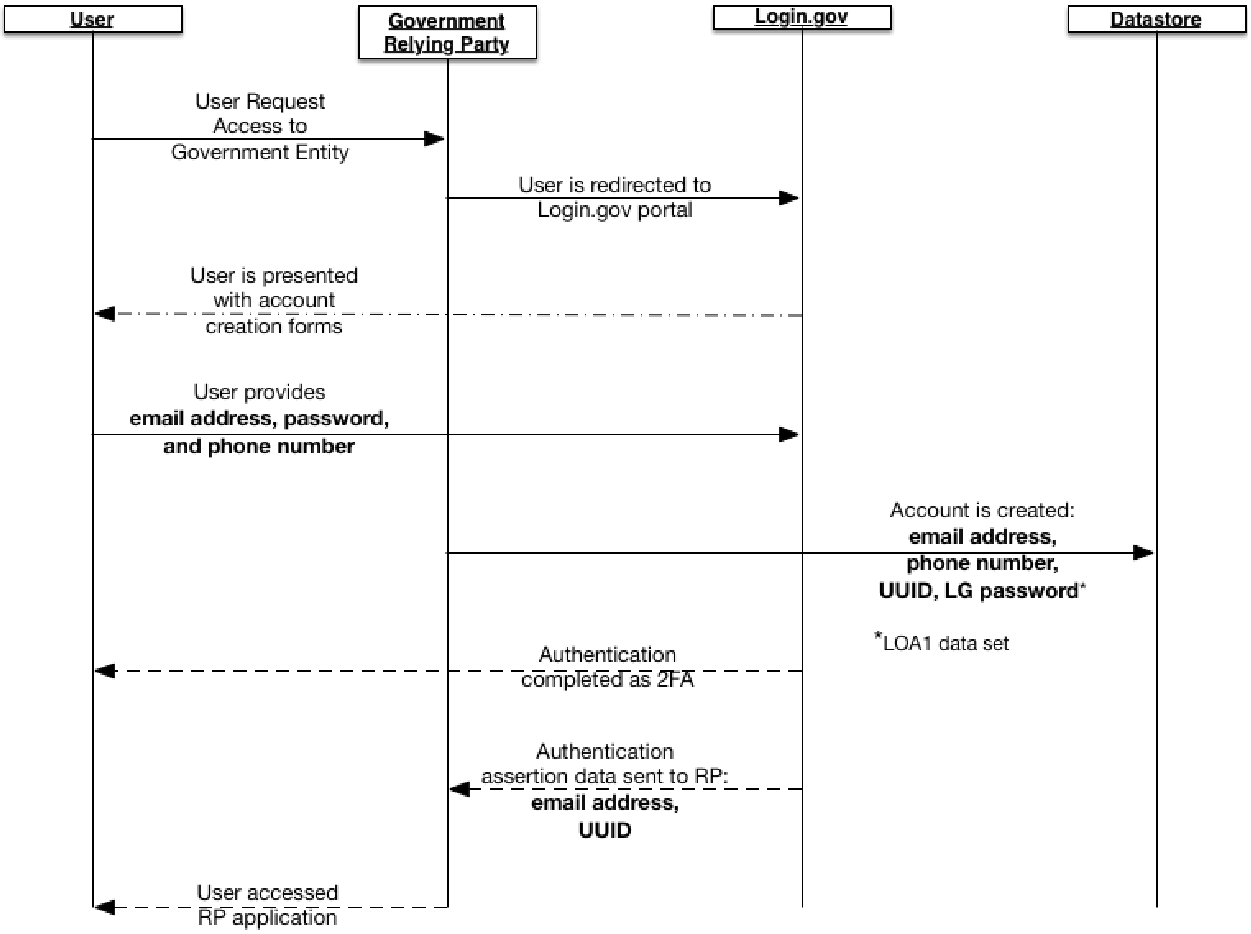
Login.gov collects the following PII from the user in order to create and maintain that user's LOA1 account:

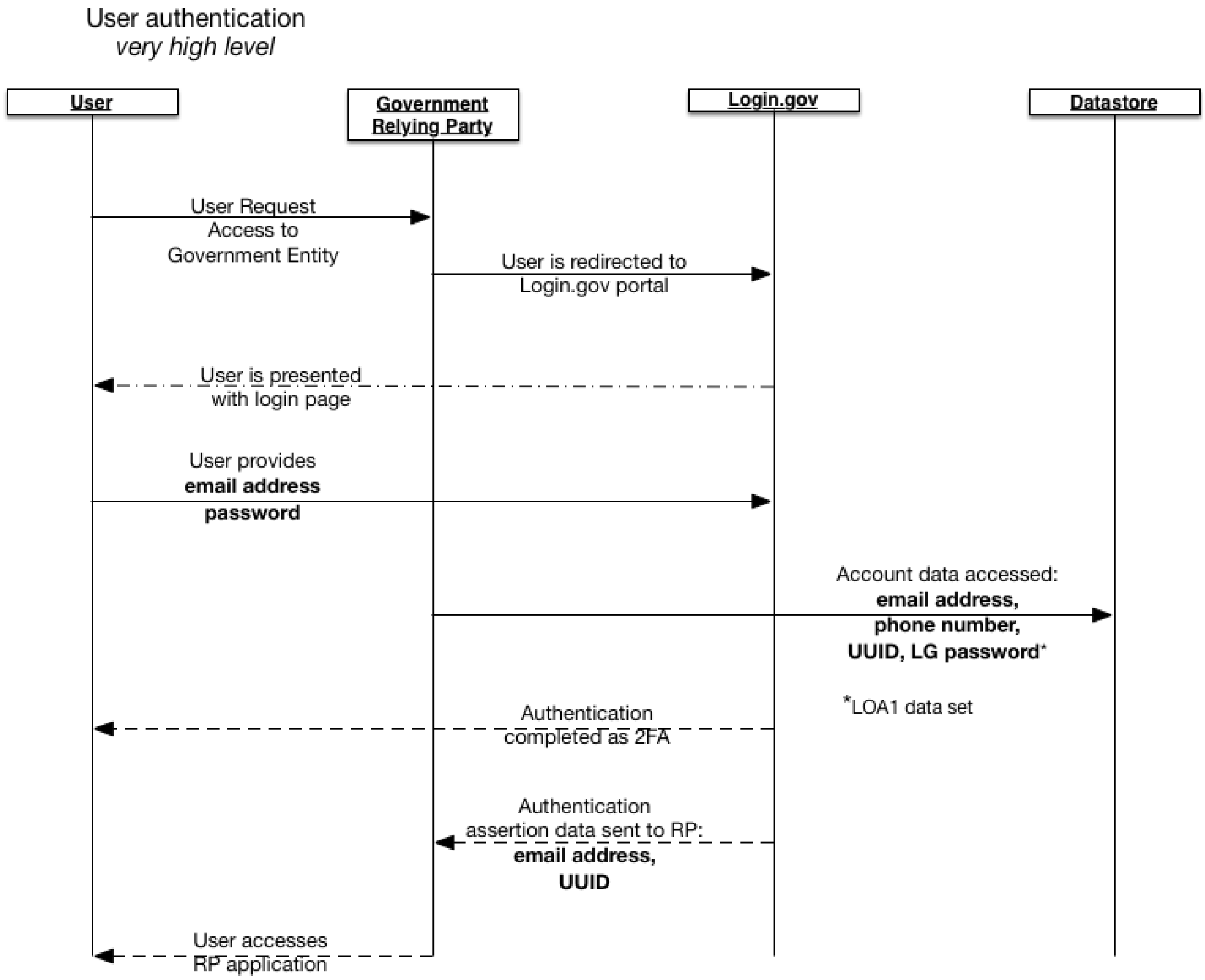
PII Categories	Is collected and stored by Login.gov	With user's consent, may be shared with and stored by partner agencies
Email Address	**Yes**	**Yes**
Phone Number	**Yes**	
2 Factor Authentication Metadata	**Yes**	
UUIDs[4]	**Yes**	**Yes**

[3] *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.

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

User account creation
very high level


User
Government Relying Party
Login.gov
Datastore
User Request Access to Government Entity
User is redirected to Login.gov portal
User is presented with account creation forms
User provides **email address, password, and phone number**
Account is created: **email address, phone number, UUID, LG password***
*LOA1 data set
Authentication completed as 2FA
Authentication assertion data sent to RP: **email address, UUID**
User accessed RP application


User authentication
very high level
User
Government Relying Party
Login.gov
Datastore
User Request Access to Government Entity
User is redirected to Login.gov portal
User is presented with login page
User provides email address password
Account data accessed: email address, phone number, UUID, LG password*
*LOA1 data set
Authentication completed as 2FA
Authentication assertion data sent to RP: email address, UUID
User accesses RP application

The system assigns each user a unique user identification (UUID),[5] and additional UUIDs for each partner agency that user accesses via Login.gov. The UUID is stored during each of the user's sessions so that each partner agency can use it to locate a user's profile within their own systems. For example, if an individual accesses GSA's information or services and another partner agency's services or information through Login.gov, that user will be assigned two different UUIDs. GSA will only be provided the user's UUID related to the GSA site visit and the other partner agency will be sent only the second UUID. Each partner agency may also assign each Login.gov user its own unique identifier, which will be sent back to the system and stored as part of the user's account information, along with the UUID.

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

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

[5] 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.

generated UUID are used to achieve LOA1. Web-based interfaces guide the user through the data entry process via the public internet.

2.3. Why will the information be collected, used, disseminated or maintained?
Login.gov uses the minimum information necessary to enable LOA1 access to partner agency services (i.e. email address paired with the user's UUID). To enable two-factor authentication for added security, the user must provide a phone number. The user's phone number will only be shared with Twilio to provide codes via text or phone call to enable additional security via two-factor authentication.

In order to access a service that requires LOA1, the user will only be asked to provide an email address and password because that information suffices for LOA1.

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

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

3. Data and Records Retention

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

All records are stored electronically in a database in GSA's Amazon Web Services (AWS) environment. User account information is encrypted in transit and at rest. Users can modify, or amend, any of their user account information (i.e. their email address or phone number) by accessing it in their account. It will be maintained for 6 years in accordance with NARA guidance. However, in order to maintain access to participating government services, neither the system nor the system operators will delete or expire user records.

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

System records will be retained and disposed of in accordance with NARA's General Records Schedule (GRS) Transmittal 26, section 3.2 "System access records" covering user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges for system use. The guidance instructs, "Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use." Login.gov must provide access to participating government services and therefore may have business need to retain the information longer than the 6 year retention period.

4. Access to and Sharing of the Data

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

(FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

Login.gov only supports a single role: the public user. The public user role only allows that user permission to make changes to that profile information after successful authentication. During the authentication process, data exchanged with a Service Provider relying on login.gov application only shares the user’s email address and UUID so that they can make authorization decisions to provide access to services and information and recognize the user on subsequent visits. The user’s phone number is transmitted to Twilio to enable additional security via two-factor authentication.

Authorized users with elevated privileges may perform an export at the infrastructure layer; however there is a separation of duties, auditing, etc.

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

With the user’s consent, the user’s email address and UUID will be shared with partner agencies. The user’s email address is shared via encrypted transport (TLS/HTTPS), and depending on the authentication protocol (SAML or OpenID), is contained within a text payload encrypted and signed with asymmetric public key encryption (PKE). The user’s phone number is encrypted during transmission to Twilio.

4.3. If the data will be released to the public, consultants, researchers or other third parties, will it be aggregated or otherwise de-identified (i.e. anonymized)? If yes, please also explain the steps that GSA will take to aggregate or de-identify the data.

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

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

GSA will log the transfer of PII to partner agencies and third party providers, including the date and purpose for each disclosure. The reason Login.gov shares users’ email addresses and UUIDs with partner agencies, with user consent, is to provide confidence that the individual who uses the Login.gov credential is the individual to whom the credential was issued. The reason the system provides Twilio with the user’s phone number is to enable additional security via two factor authentication.

4.5. Do other systems share the information or have access to the information in this system? If yes, explain who will be responsible for protecting the privacy rights of the individuals affected by the interface (e.g., System Administrators, System Developers, System Managers)?

No. Other systems do not have access to the information in the system. Information is shared when a user authorizes the system to transmit information to a partner agency. A partner agency is not be able to access information unless the user authorizes the sharing.

As determined by the GSA procurement office/OGC, the contract between GSA and AWS .contains the Federal Acquisition Regulation (FAR) provisions necessary to protect and secure information to which it has access. The information also may be shared in accordance with the applicable Privacy Act System of Records Notice, GSA/TTS-1, Login.gov, 82 FR 6552, January 19, 2017.

5. Notice, Consent and Access for Individuals

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

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

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

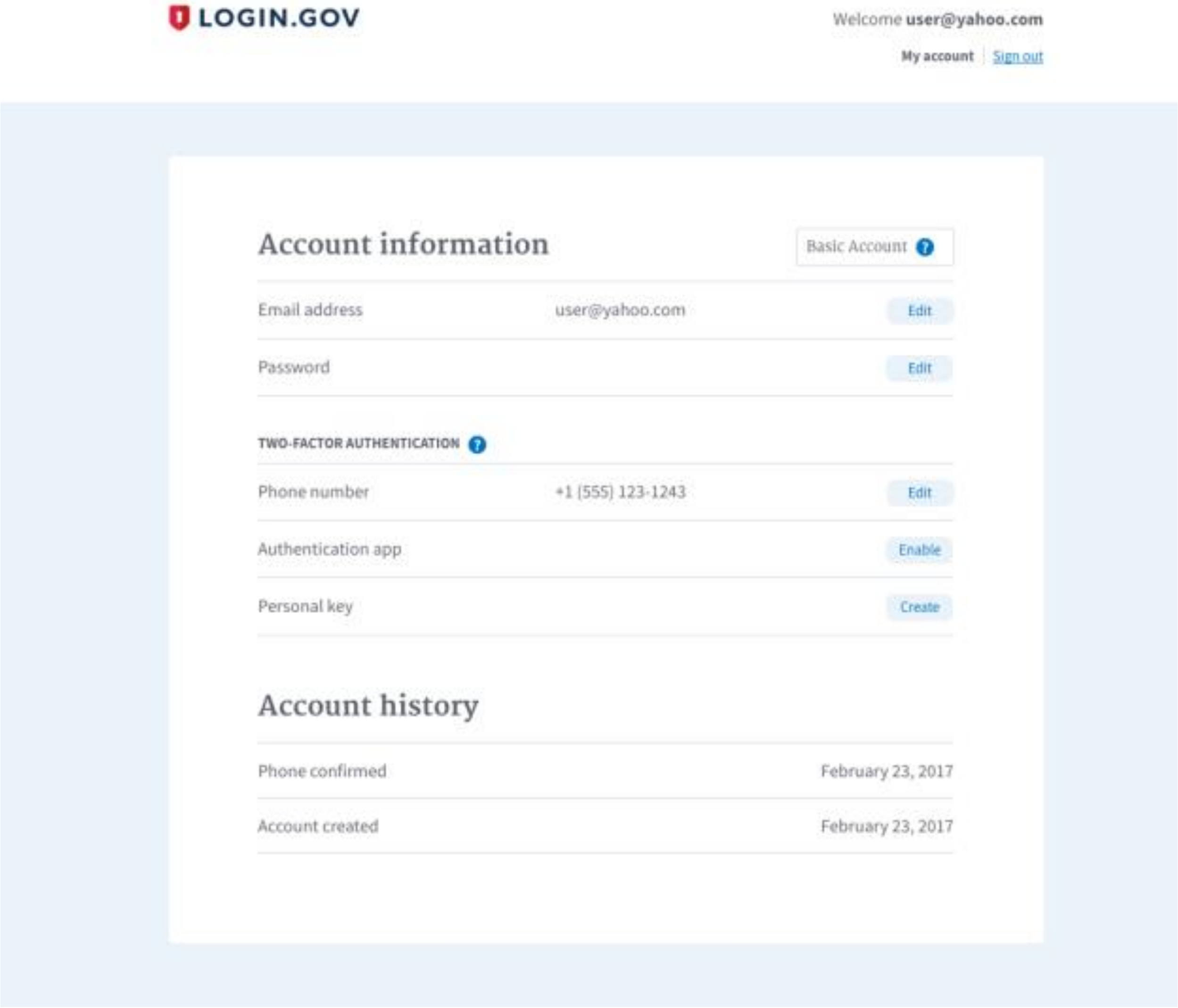
A user must opt-in to share any information with each partner agency. For example, if a user navigates to a partner agency's website and access it via Login.gov, that user will be provided notice and an opportunity to consent to that partner agency's use of the user's LOA1 credential.

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

The user's phone number is required to enable two-factor authentication. If it is not provided, the user will not be able to create an account.

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

An individual can access their email address and phone number to change it at any time, however changing the email address in the user account will change the address to which partner agencies send user emails.



LOGIN.GOV

Welcome user@yahoo.com

My account | Sign out

Account information

Basic Account

Email address user@yahoo.com

Password

TWO-FACTOR AUTHENTICATION

Phone number +1 (555) 123-1243

Authentication app

Personal key

Account history

Phone confirmed February 23, 2017

Account created February 23, 2017

6. Maintenance of Controls

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

Access to the Login.gov system is authorized only via possession of private SSH keys available via a physical PIV card. PIV card holders must be pre-authorized to access the system.

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

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

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

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

No, the system does not provide the capability to locate an individual in real-time or monitor an individual. LOA1 does not involve any identity proofing; therefore, the system only provides limited assurance that the individual accessing a partner agency’s services or information is the person who was initially provided the credential.

Assigning a user a different UUID for each partner agency that individual accesses decreases the risk that...
6.4 Does this system comply with FISMA requirements to help ensure that information is appropriately secured?

Yes. GSA follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure that user email addresses, phone numbers, passwords and recovery codes[6] are appropriately secured. The Login.gov system resides on Amazon Web Services (AWS) which is categorized as a moderate system under Federal Information Processing Standards (FIPS) 199.

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

All GSA personnel are subject to GSA agency-wide procedures for safeguarding PII and receive annual privacy and security training. Many staff receive additional training focused on their

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

specific job duties, for example, those who need to access, use or share PII complete additional role-based training.

7. Privacy Act

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

Yes, the system retrieves information by searching against stored email addresses.

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

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

8. Privacy Policy

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

Login.gov will only collect, use or disclose information with the user's consent or as authorized by the system of records notice: https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-a-new-system-of-records The system's collection, use and disclosure of information comport with GSA's privacy policy and Login.gov does not make data actions with the user's consent.

9. Privacy Risks and Mitigation

9.1. What privacy risks are associated with the collection, use, dissemination and maintenance of the data? How have those risks been mitigated?

Privacy Risk: A user's PII may be accessible to individuals who do not have a need to know it, resulting in a problematic data action for the user.

Mitigation: The system will not retrieve the user's account information unless the user provides either their password or recovery code. See section X, above.

All PII in Login.gov is encrypted at rest and in transit. One copy of each user's account information is encrypted using their password and a second copy is encrypted using their security code. The system is designed to deny access to the user's unencrypted information without that user's password or security code. Both the user's password and security code are one-way hashed within the system. Hashing is a process of transforming of a string of characters (i.e. a password or security code) into a fixed-length value that represents the original string.

When a user creates a Login.gov account, the system combines the user's password, a server-controlled random string, and a hardware security module (HSM) from the AWS environment to create an encryption key. The same process occurs with the user's recovery code.

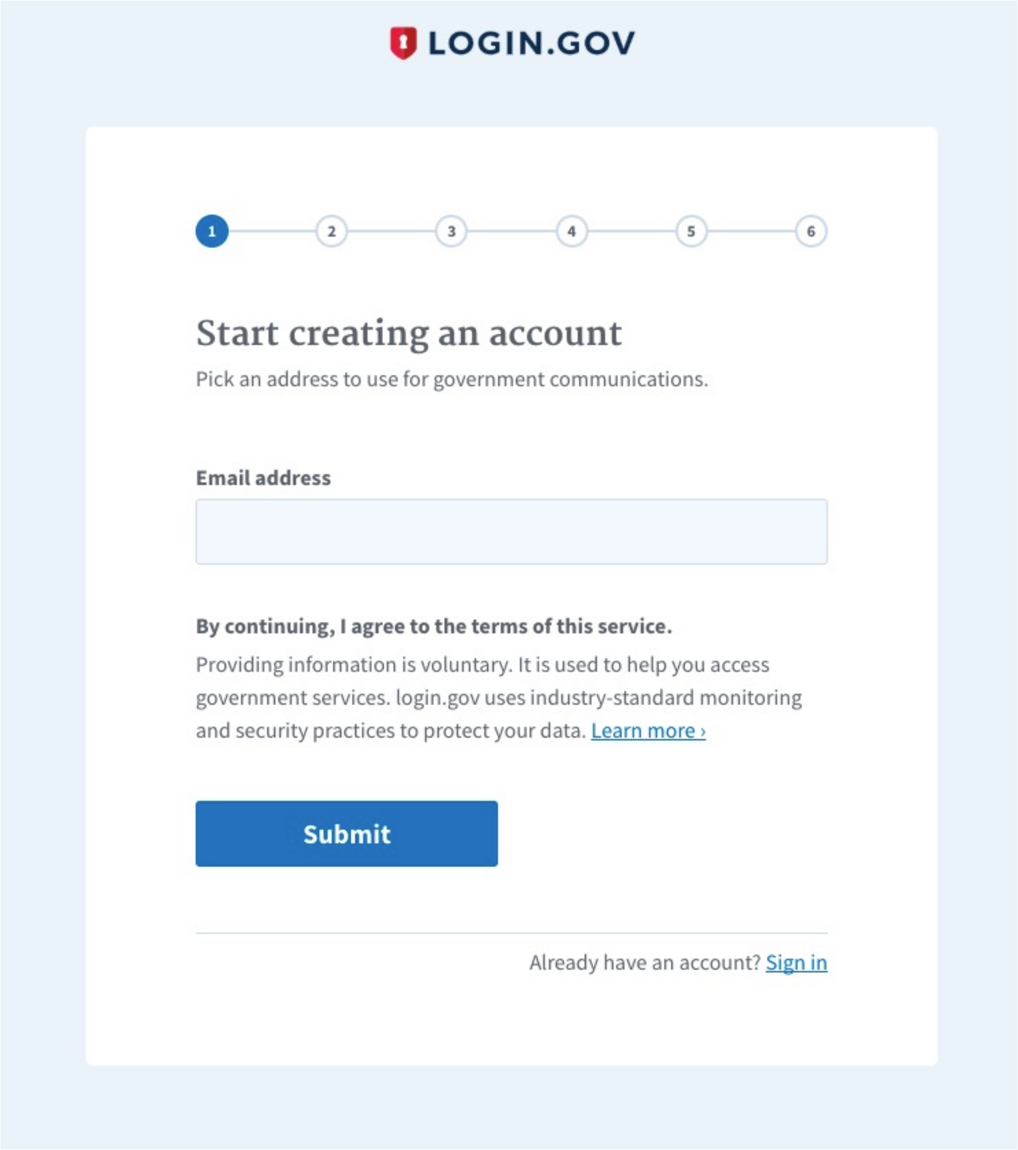
Privacy Risk: Metadata (information that provides information about other data) about how the user accesses a partner service may be used to track individual behavior, resulting in a problematic data action for the user.

Mitigation: The encryption of a user's account information means that information cannot be associated with other types of behavioral information to unmask a user. See section Y, above.

Privacy Impact Analysis: Risks Related to Why the information is collected

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 may not understanding what is happening. See section Z, above. Additionally, the interface provides visual prompts and explains the purpose of the system:



Start creating an account

Pick an address to use for government communications.

Email address

By continuing, I agree to the terms of this service.

Providing information is voluntary. It is used to help you access government services. login.gov uses industry-standard monitoring and security practices to protect your data. Learn more ›

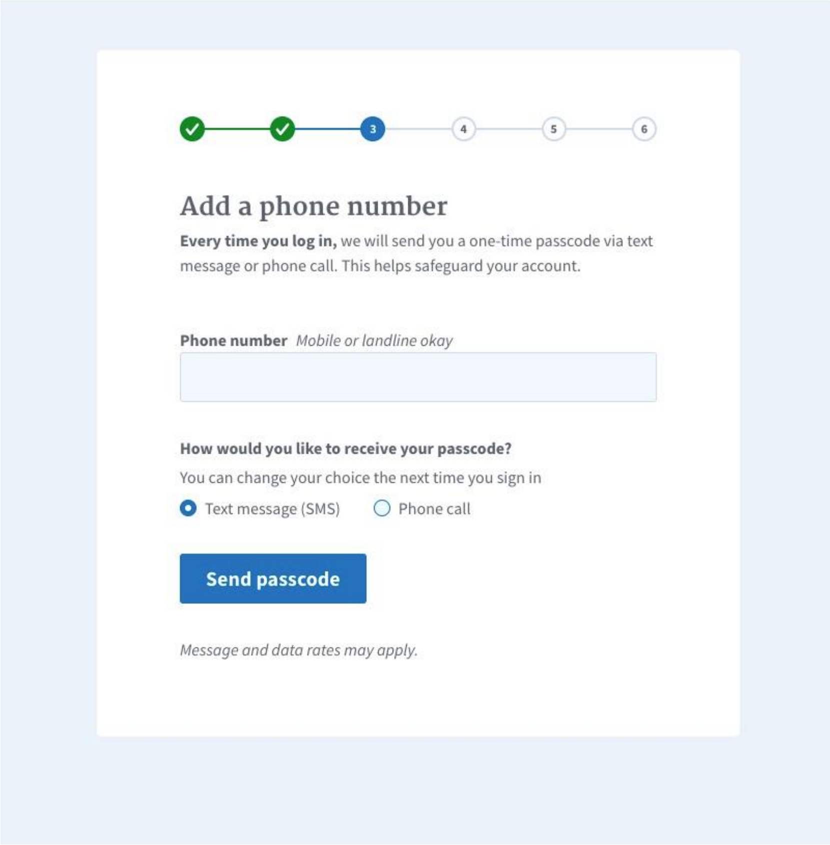
Already have an account? Sign in

Privacy Impact Analysis: Risks Related to Sources of Information in the System

Privacy Risk: Identity thieves may try to access Login.gov accounts using stolen email accounts, thereby preventing individuals from being able to access the system and create a problematic data action.

Mitigation: Two factor authentication is required to initiate each session and helps ensure that a stolen email account is not enough to access an individual's account. The user's account password is required and during the log-in process the user must type in a code that is sent to their phone either via a phone call or text message:

LOGIN.GOV



Add a phone number

Every time you log in, we will send you a one-time passcode via text message or phone call. This helps safeguard your account.

Phone number *Mobile or landline okay*

How would you like to receive your passcode?

You can change your choice the next time you sign in

● Text message (SMS) ○ Phone call

Message and data rates may apply.

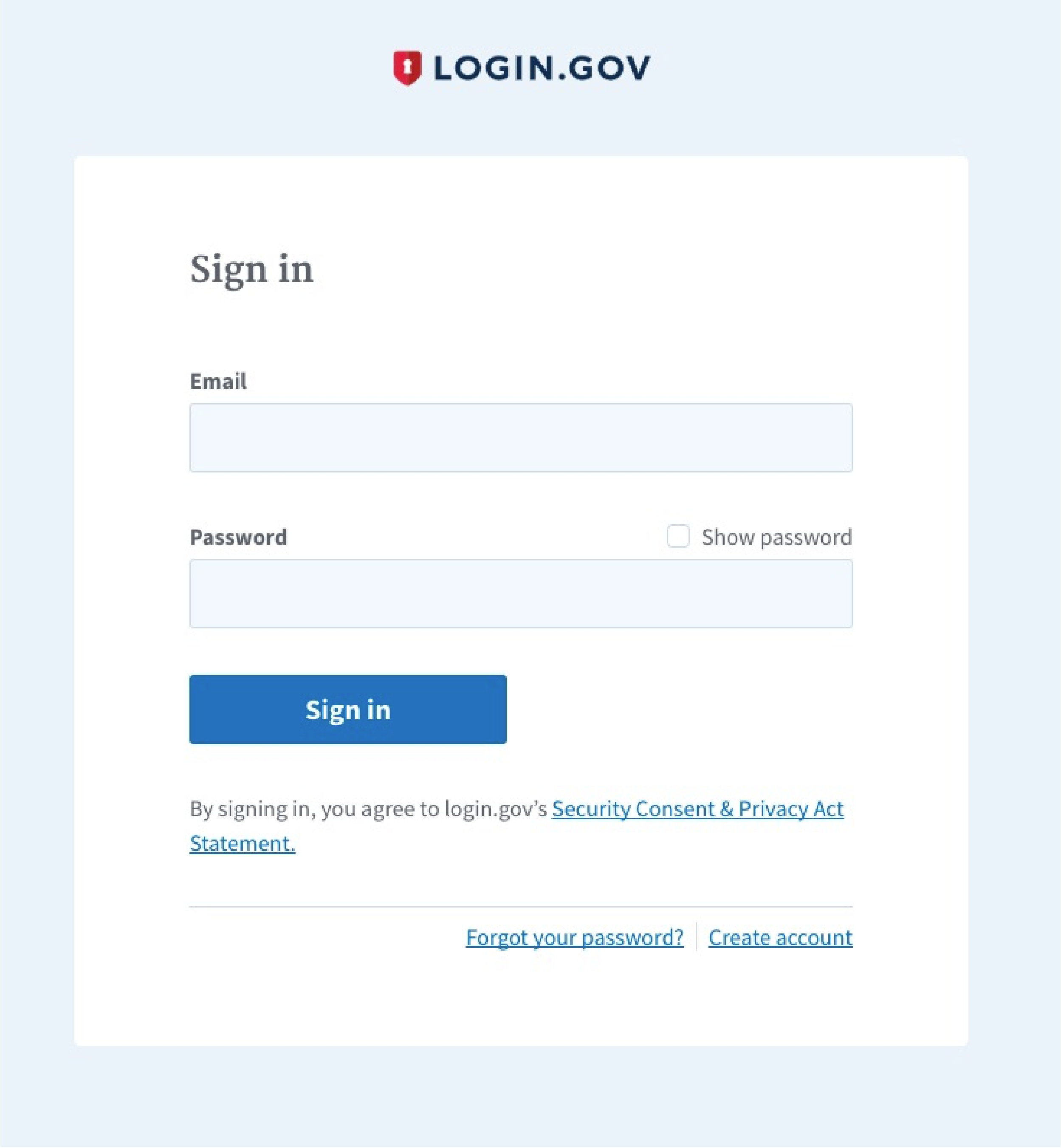
Why does LogIn.gov collect my phone number when I initially create my account?
LogIn.gov requires a phone number in order to allow 2FA, which provides additional security for your account. Login.gov does not use your phone number to identity proof you at LOA1, just as an added security measure, which is consistent w best practices...provide examples, etc.

What if I forget my password and lose my recovery code?
Each user can reset their password via email.

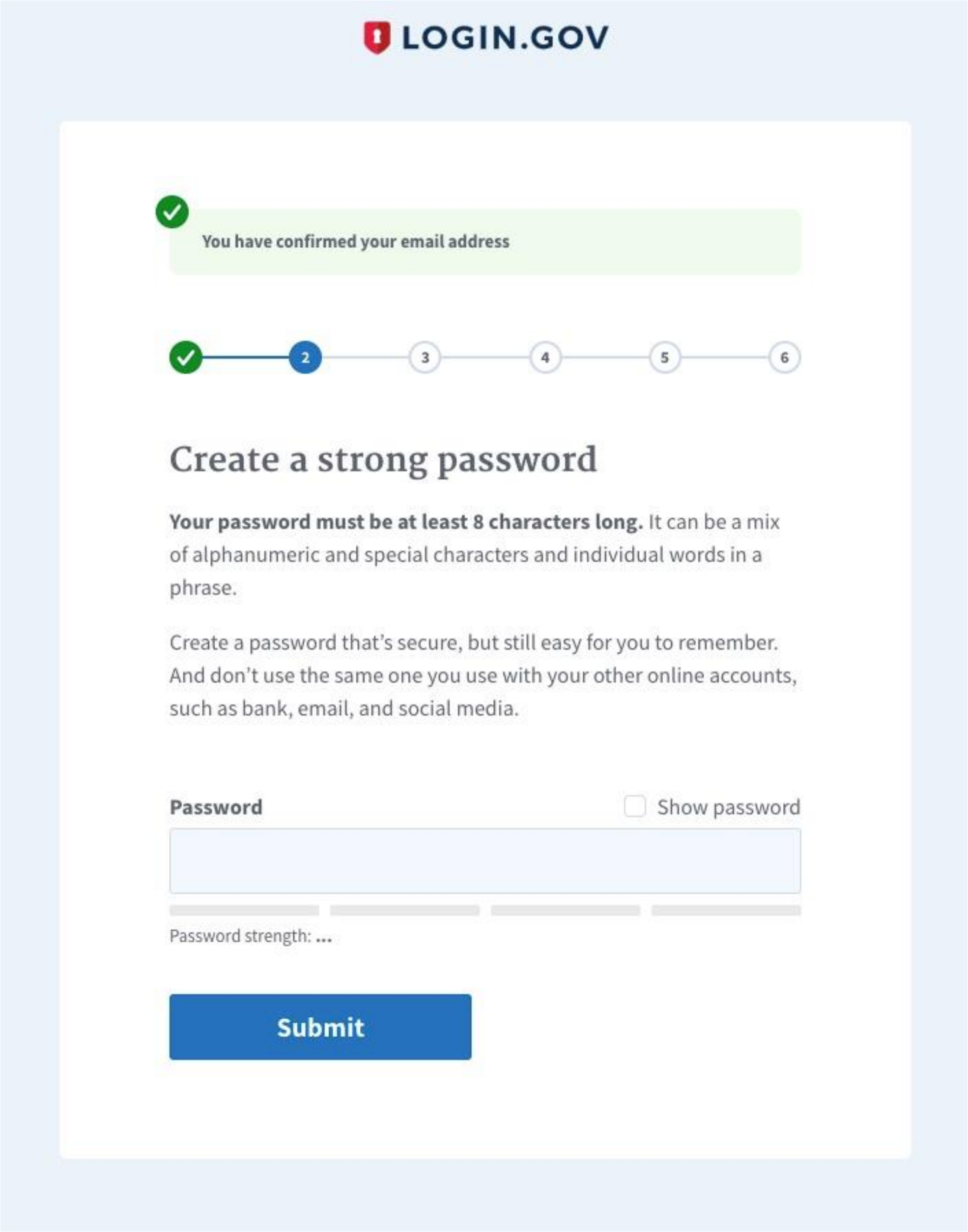
Will different partner agencies be able to tell which services I have accessed? No, Login.gov provides a unique identifier to each partner agency whose services you access. Partner agencies do not have access to other information about a user’s activities not associated with their agency

What is my meaningless but unique number (MBUN)? Who is provided this information?
The MBUN is associated with a specific user and a specific agency service provider. The MBUN is persistent across sessions, so that a relying agency can use it to locate a user’s profile within their own systems. The MBUN is unique to one service provider. Currently the login.gov system uses UUID v4 strings as MBUN values.

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



By signing in, you agree to login.gov's Security Consent & Privacy Act Statement.



✓ You have confirmed your email address

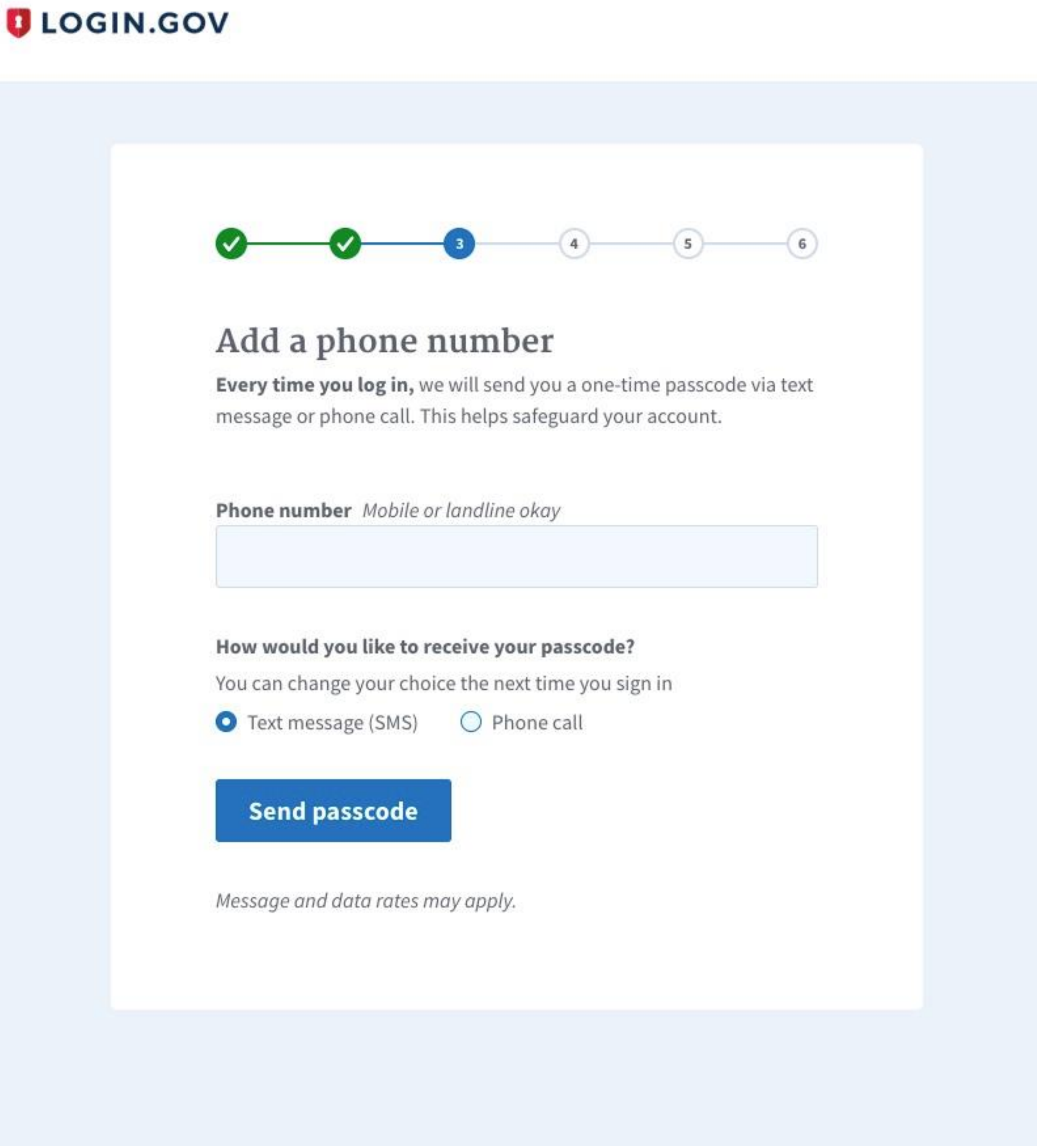
Create a strong password

Your password must be at least 8 characters long. It can be a mix of alphanumeric and special characters and individual words in a phrase.

Create a password that's secure, but still easy for you to remember. And don't use the same one you use with your other online accounts, such as bank, email, and social media.

Password □ Show password

Password strength: **...**



Add a phone number

Every time you log in, we will send you a one-time passcode via text message or phone call. This helps safeguard your account.

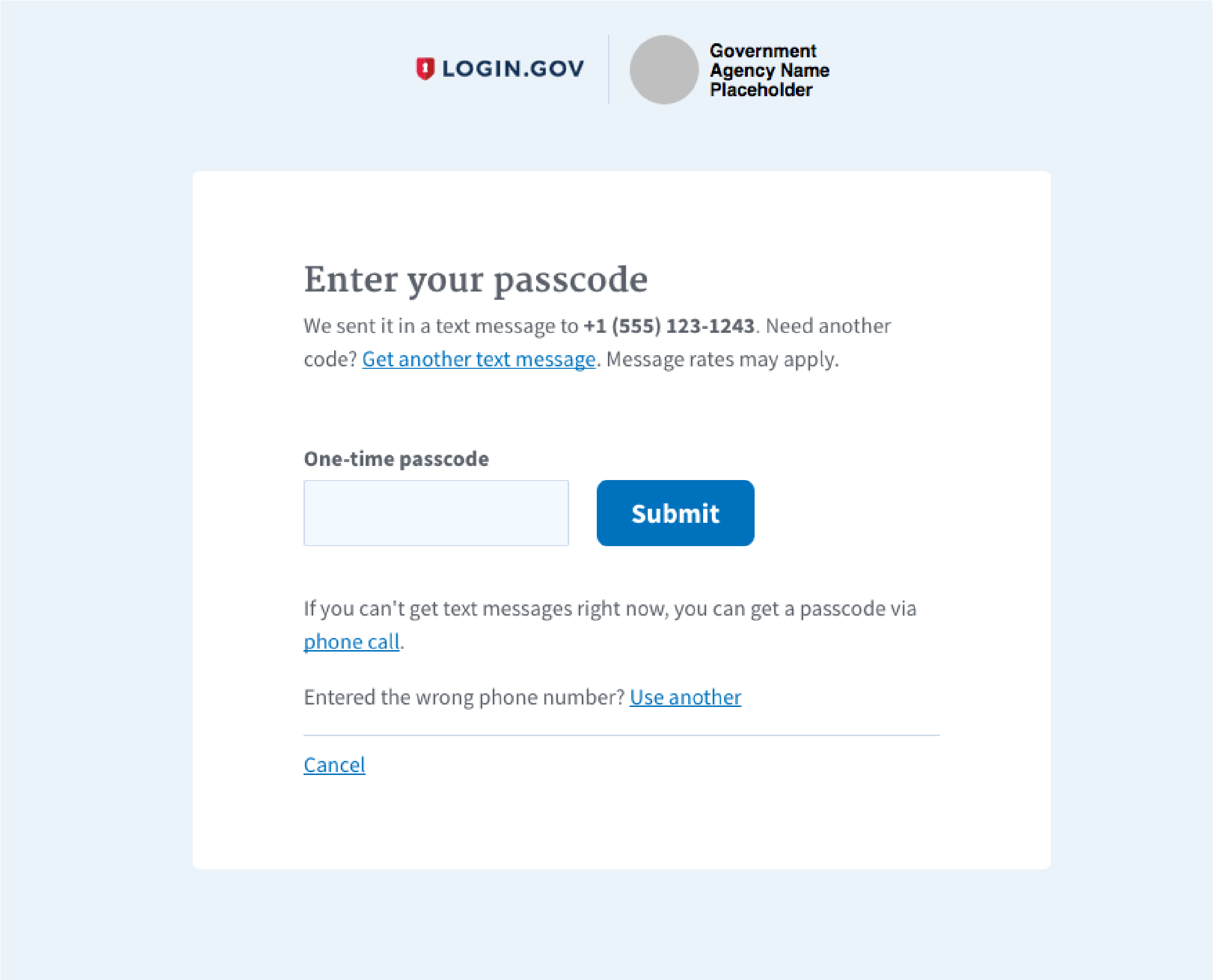
Phone number *Mobile or landline okay*

How would you like to receive your passcode?

You can change your choice the next time you sign in

● Text message (SMS) ○ Phone call

Message and data rates may apply.



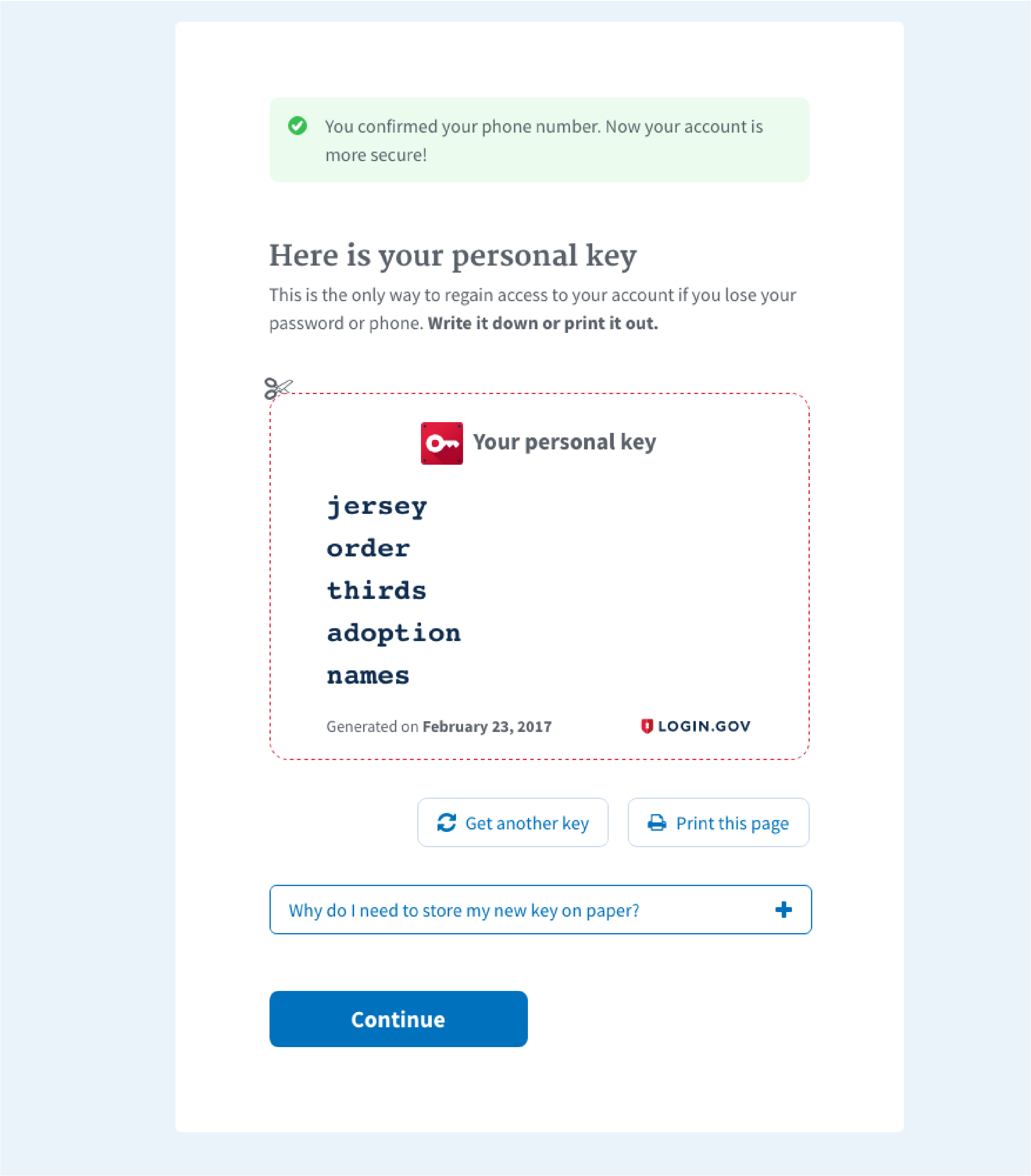
Enter your passcode

We sent it in a text message to **+1 (555) 123-1243**. Need another code? Get another text message. Message rates may apply.

If you can't get text messages right now, you can get a passcode via phone call.

Entered the wrong phone number? Use another

Cancel



You confirmed your phone number. Now your account is more secure!

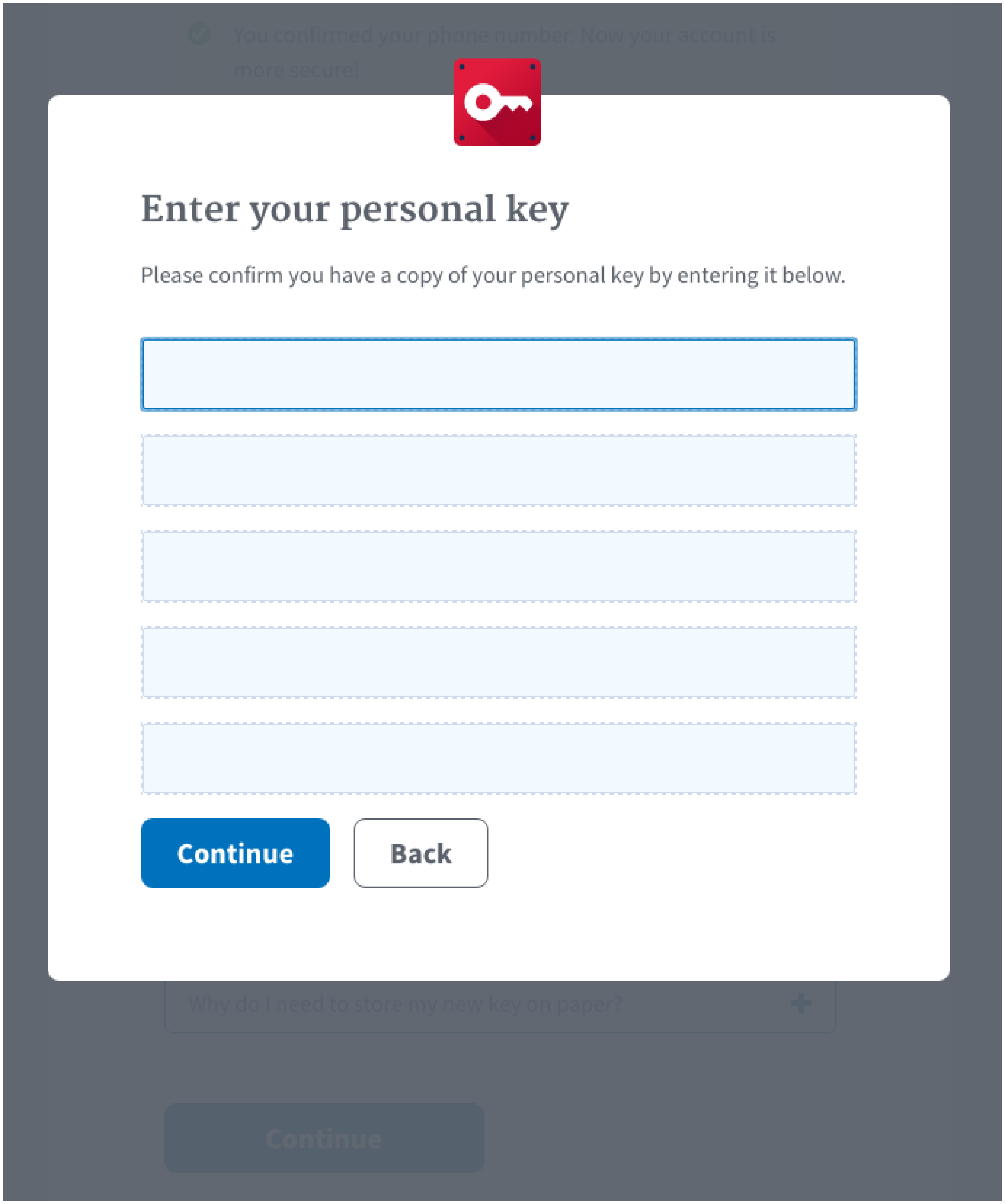
Here is your personal key

This is the only way to regain access to your account if you lose your password or phone. **Write it down or print it out.**

Your personal key

```
jersey
order
thirds
adoption
names
```

Generated on **February 23, 2017**

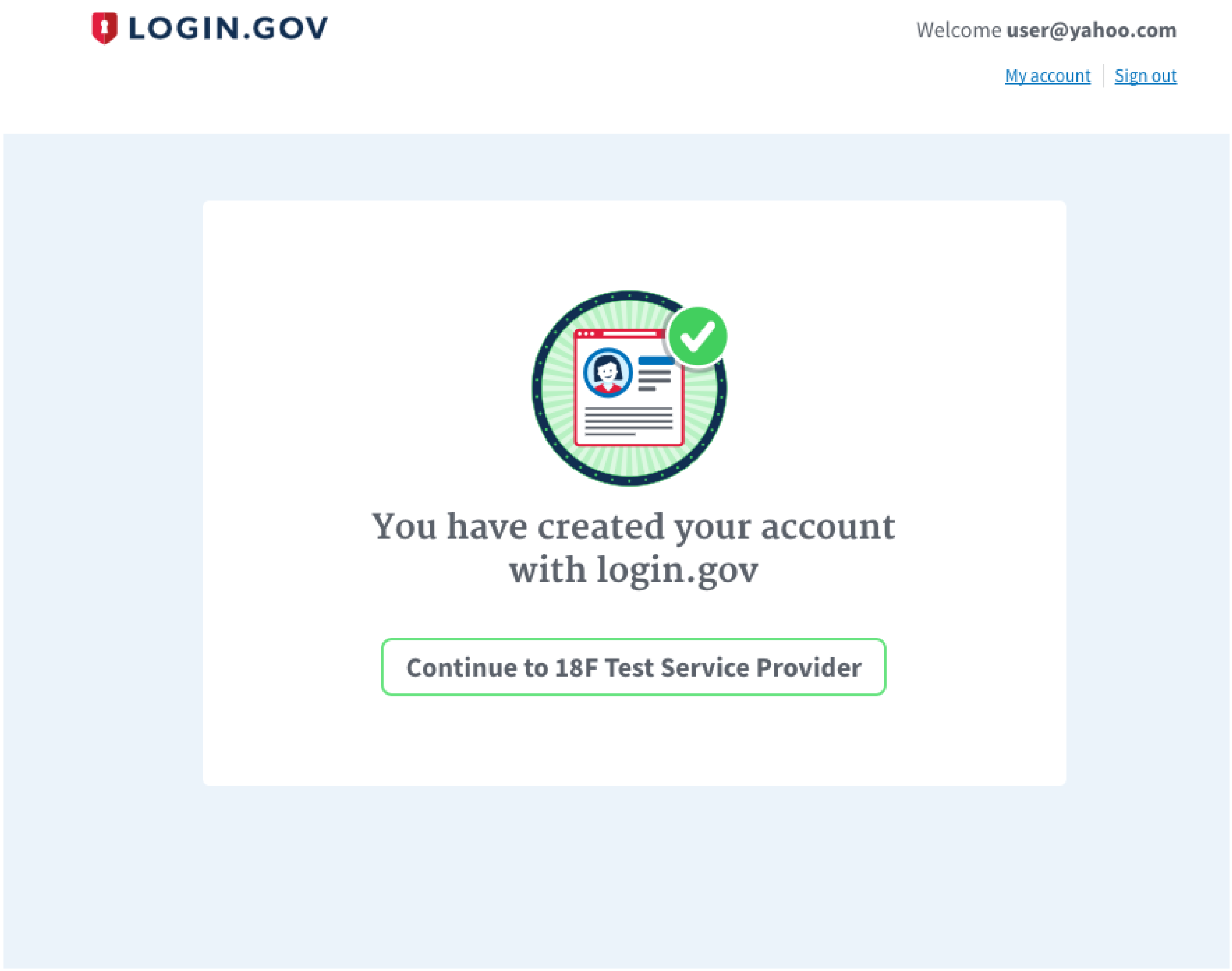


You confirmed your phone number. Now your account is more secure!

Enter your personal key

Please confirm you have a copy of your personal key by entering it below.

Why do I need to store my new key on paper?



Welcome **user@yahoo.com**

You have created your account with login.gov

Key terms and concepts that are used throughout this document:

Assurance
Authentication
ID proofing
Credential
Two-factor authentication
Etc.