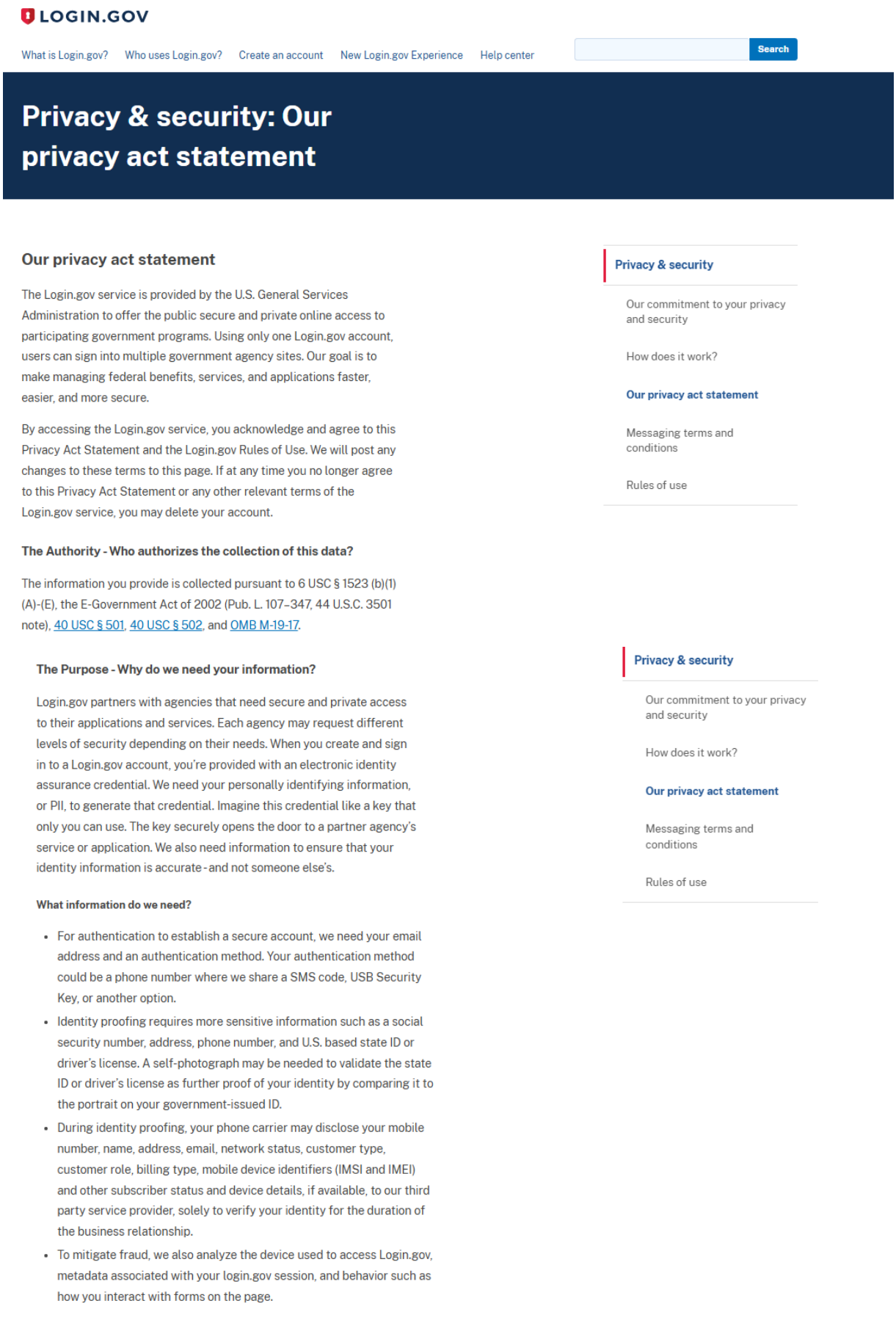
Appendix X—Login.gov Privacy Act Statement



LOGIN.GOV

What is Login.gov? Who uses Login.gov? Create an account New Login.gov Experience Help center Search

Privacy & security: Our privacy act statement

Our privacy act statement

The Login.gov service is provided by the U.S. General Services Administration to offer the public secure and private online access to participating government programs. Using only one Login.gov account, users can sign into multiple government agency sites. Our goal is to make managing federal benefits, services, and applications faster, easier, and more secure.

By accessing the Login.gov service, you acknowledge and agree to this Privacy Act Statement and the Login.gov Rules of Use. We will post any changes to these terms to this page. If at any time you no longer agree to this Privacy Act Statement or any other relevant terms of the Login.gov service, you may delete your account.

The Authority - Who authorizes the collection of this data?

The information you provide is collected pursuant to 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (Pub. L. 107–347, 44 U.S.C. 3501 note), 40 USC § 501, 40 USC § 502, and OMB M-19-17.

The Purpose - Why do we need your information?

Login.gov partners with agencies that need secure and private access to their applications and services. Each agency may request different levels of security depending on their needs. When you create and sign in to a Login.gov account, you're provided with an electronic identity assurance credential. We need your personally identifying information, or PII, to generate that credential. Imagine this credential like a key that only you can use. The key securely opens the door to a partner agency's service or application. We also need information to ensure that your identity information is accurate - and not someone else's.

What information do we need?

- For authentication to establish a secure account, we need your email address and an authentication method. Your authentication method could be a phone number where we share a SMS code, USB Security Key, or another option.
- Identity proofing requires more sensitive information such as a social security number, address, phone number, and U.S. based state ID or driver's license. A self-photograph may be needed to validate the state ID or driver's license as further proof of your identity by comparing it to the portrait on your government-issued ID.
- During identity proofing, your phone carrier may disclose your mobile number, name, address, email, network status, customer type, customer role, billing type, mobile device identifiers (IMSI and IMEI) and other subscriber status and device details, if available, to our third party service provider, solely to verify your identity for the duration of the business relationship.
- To mitigate fraud, we also analyze the device used to access Login.gov, metadata associated with your login.gov session, and behavior such as how you interact with forms on the page.

Privacy & security

Our commitment to your privacy and security

How does it work?

Our privacy act statement

Messaging terms and conditions

Rules of use

Privacy & security

Our commitment to your privacy and security

How does it work?

Our privacy act statement

Messaging terms and conditions

Rules of use

Routine Uses - With whom is the information routinely shared?

- To third parties providing remote or in-person authentication and identity proofing services, including other federal agencies providing such services, as necessary to authenticate or identity proof you for access to a participating government website or application.
- To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant.
- To the Government Publishing Office (GPO), when Login.gov needs to mail you an address confirmation form or if you request mailed notifications of account changes or of proofing attempts.
- To other federal agencies and third-party fraud prevention services as necessary to detect and investigate suspected fraud, including providing you with redress.

This list is not comprehensive. Please see system of records notice GSA/TTS-1 for all entities and individuals.

What happens to the information you share?

All records are stored electronically in a database in GSA's Amazon Web Services (AWS) environment. Login.gov's vendors also store personal information for 90 days for the purpose of detecting and mitigating fraud in the system. Vendors may retain data longer than 90 days if needed to investigate or prevent suspected fraud or if otherwise required by law. You can modify, or amend, either your email address or phone number on your account page.

Your personal information, including profiles, log-in files, password files, audit trail files and extracts, system usage records, and agency billing data used to assess charges for system use, will be maintained for as long as you have an active account, unless longer retention is required for business use, such as for law enforcement matters or other legal actions in accordance with National Archives and Records Administration (NARA) guidance. This personal information is necessary to provide users access to information and services at partner agencies.

There may be circumstances where we are required to share certain data. Please refer to the "routine uses" section of the system of records notice linked above for more information on those circumstances.

Consent - How can you control what information is shared?

You decide if you want to share personal information with any agency and you can revoke consent at any time. You can modify, or amend, either your email address or phone number on your account page.

However, failure to provide complete and accurate information may delay access to the partner agency. Login.gov does not make any eligibility or suitability determinations; that is the responsibility of the government websites that use the Login.gov service.

Other than as specified in this Privacy Act Statement and our Rules of Use, we will never share your information without your consent. Your validated personal data is encrypted and the only way to share it with a partner agency is if you, the authorized user, enter your password and explicitly grant consent to share the information.

When you create an account or visit a new partner agency website after you have created your account, you will see the option to consent to share your information with the partner agency. You are required to give consent yearly for each agency.

Remember you can update your personal information, revoke consent, or delete your account entirely at any time through your account page.

Fraud mitigation - How do we stop bad actors?

Identity fraud is someone pretending to be you and attempting to access a partner agency using your Login.gov information. Login.gov protects your data from bad actors. Our product works with trusted third-party vendors to make sure it is you - and not someone pretending to be you - accessing your account. These vendors look for changes and risks in user behavior that might indicate a fraud attempt.

Privacy & security

Our commitment to your privacy and security

How does it work?

Our privacy act statement

Messaging terms and conditions

Rules of use

Fraud mitigation - How do we stop bad actors?

Identity fraud is someone pretending to be you and attempting to access a partner agency using your Login.gov information. Login.gov protects your data from bad actors. Our product works with trusted third-party vendors to make sure it is you - and not someone pretending to be you - accessing your account. These vendors look for changes and risks in user behavior that might indicate a fraud attempt.

Records - Where can you find more information?

Please see the Login.gov system of records notice (GSA/TTS–1).

Website Analytics – Other data we collect

Other data, like the pages you visit and the length of your session, are aggregated into reports to help us better understand how the site is being used and how we can make it more helpful. The data is anonymized. No personally identifying user information is tied to this data and it is only shared anonymously with the Login.gov team.

We collect device information and behavioral analytics to assess for risk of misuse. This information is stored in an obfuscated manner. Login.gov is able to assess device and behavioral risk from this obscured data store, but neither Login.gov nor its providers can read the information.

Privacy Impact Assessment

View our privacy impact assessment at www.gsa.gov/PIA for further details on how Login.gov collects, uses, secures, and destroys information in ways that protect privacy.

Back to top

Our commitment to your privacy and security

How does it work?

Our privacy act statement

Messaging terms and conditions

Rules of use