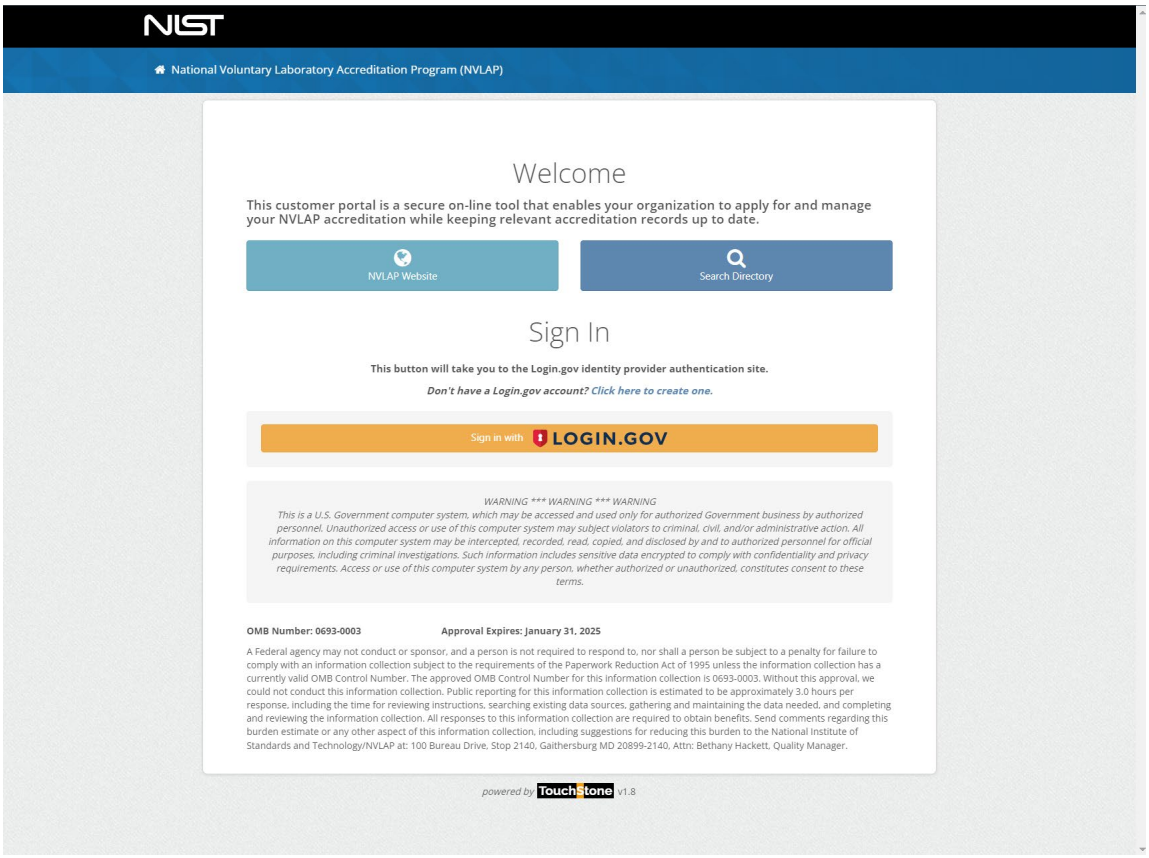
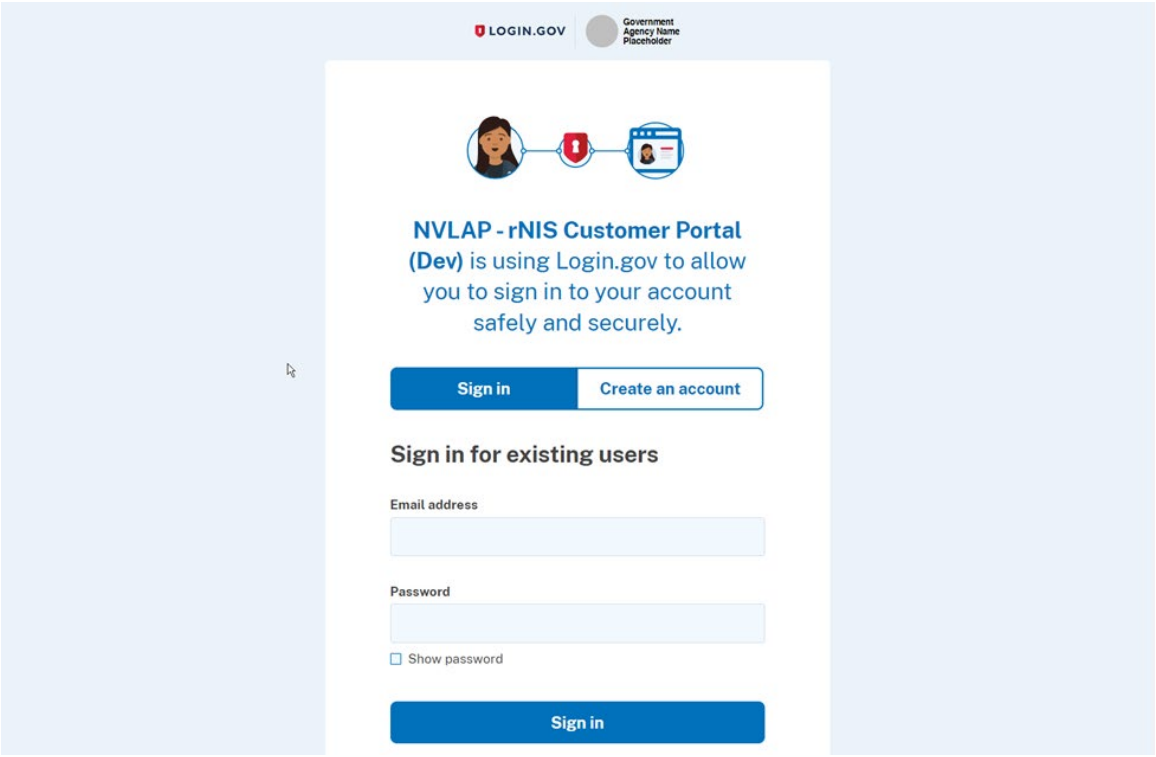
Accessing NIWS Lab or Assessor portal once a Login.gov account has been created

1. Click the Login bar. This will forward you to Login.gov.



2. Log into your Login.gov account. This will redirect you to the NIWS home page once logged in.



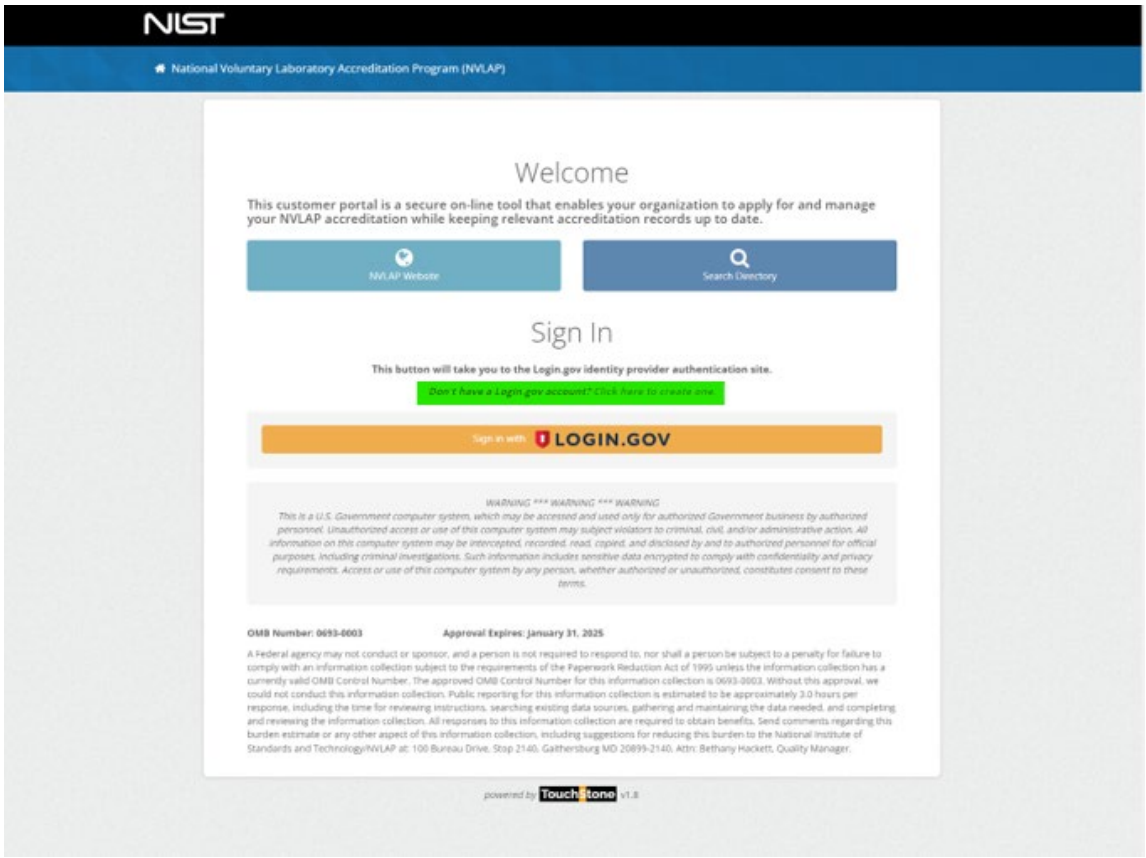
3. Now you are on the NIWS home page!

Registering for Login.gov from the NIWS portal

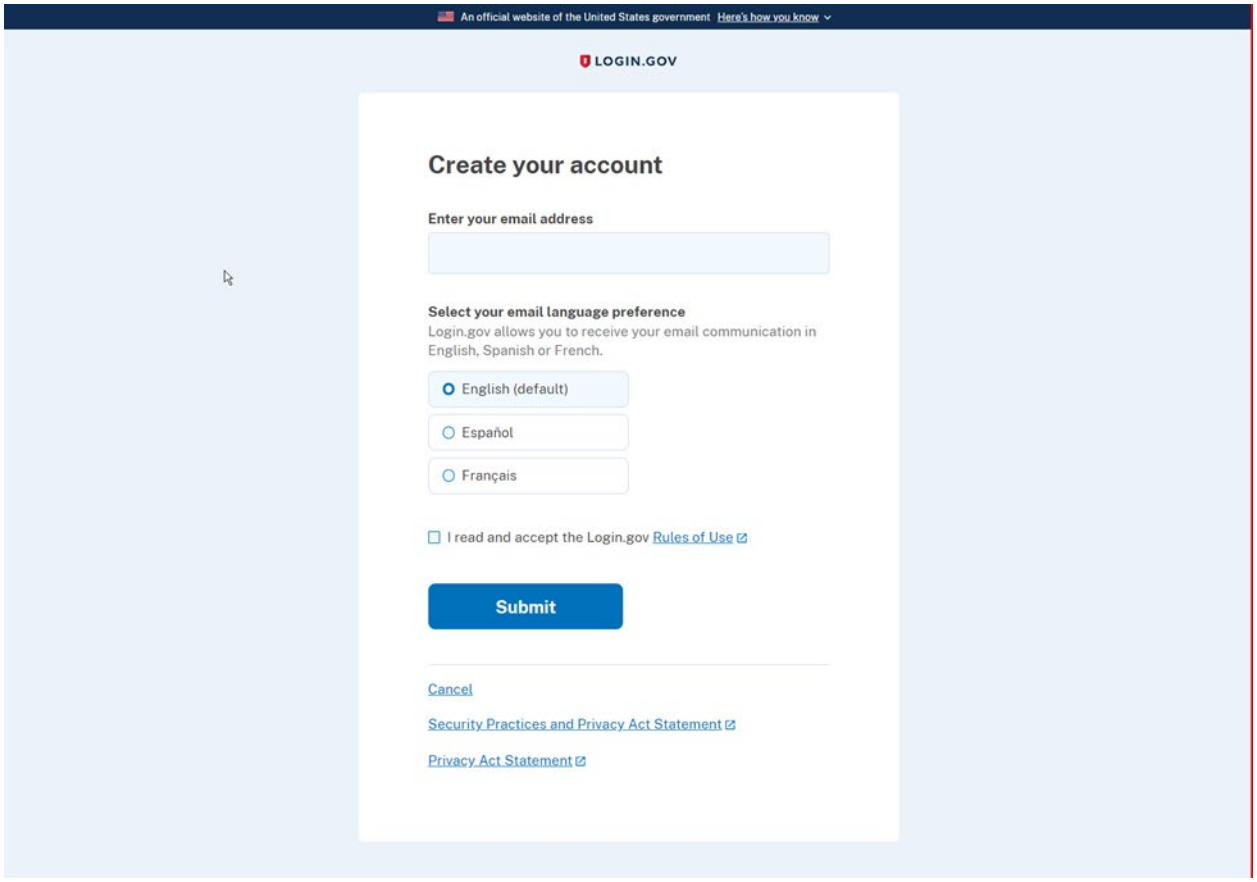
In order to access the NIWS Lab or Assessor Portal, you must have a Login.gov account under the same email that is listed in your NVLAP account. If you already have a Login.gov account under this email, you do not need to create a new account.

Creating a Login.gov Account:

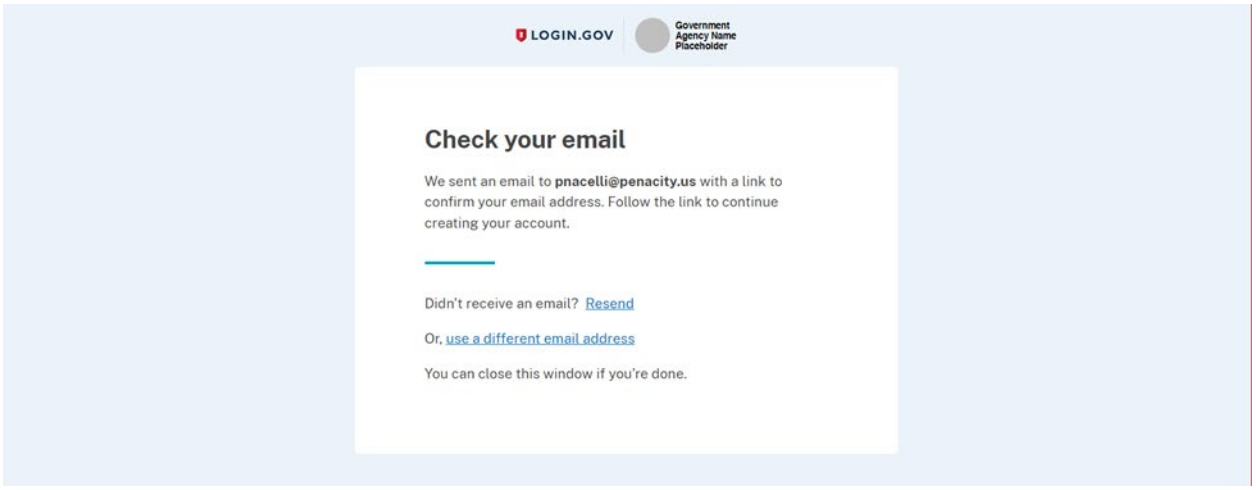
1. Click the “Don’t have a Login.gov account? Click here to create one.” link on the NIWS login page to create an account. This will forward you to Login.gov.



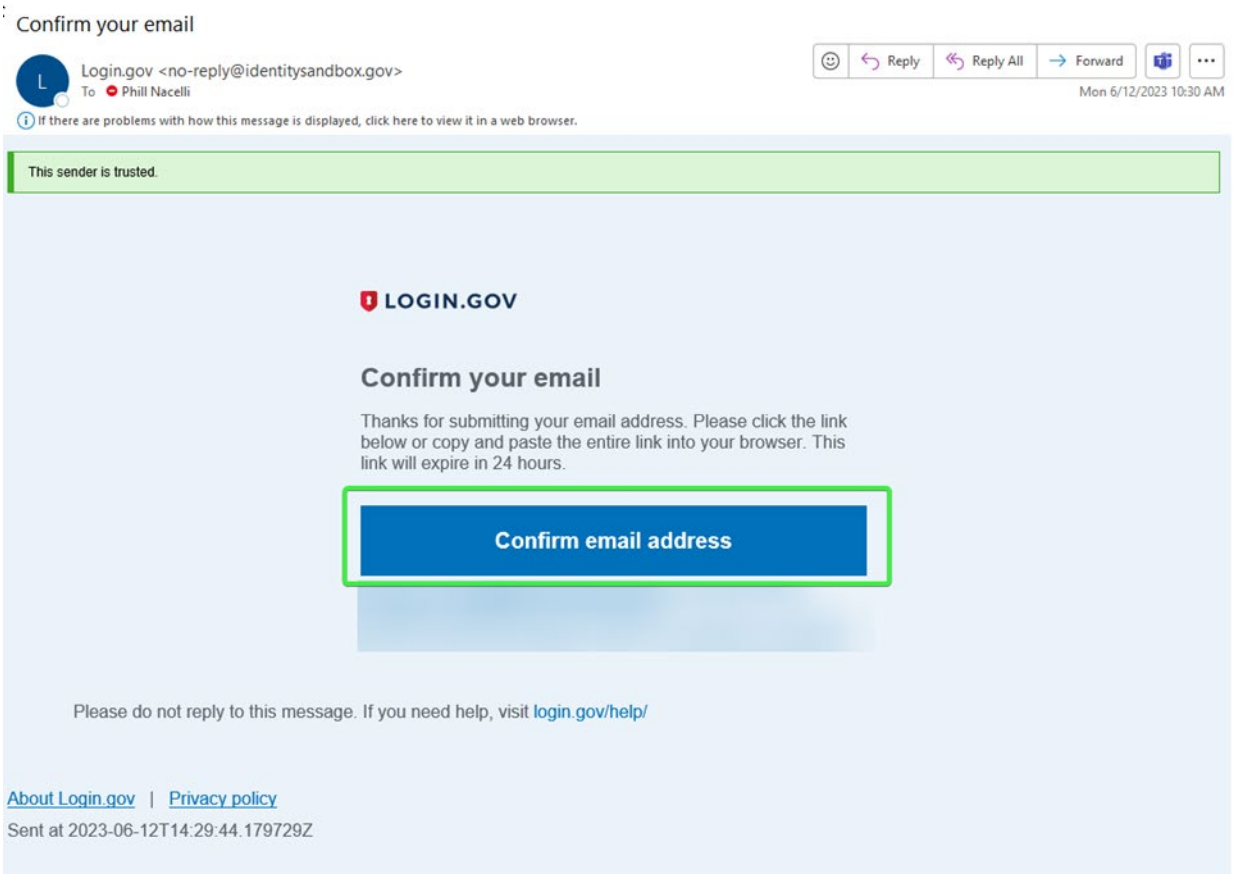
2. Enter the email that was provided to NVLAP and check the “Rules of Use” acceptance checkbox and hit “Submit” button.



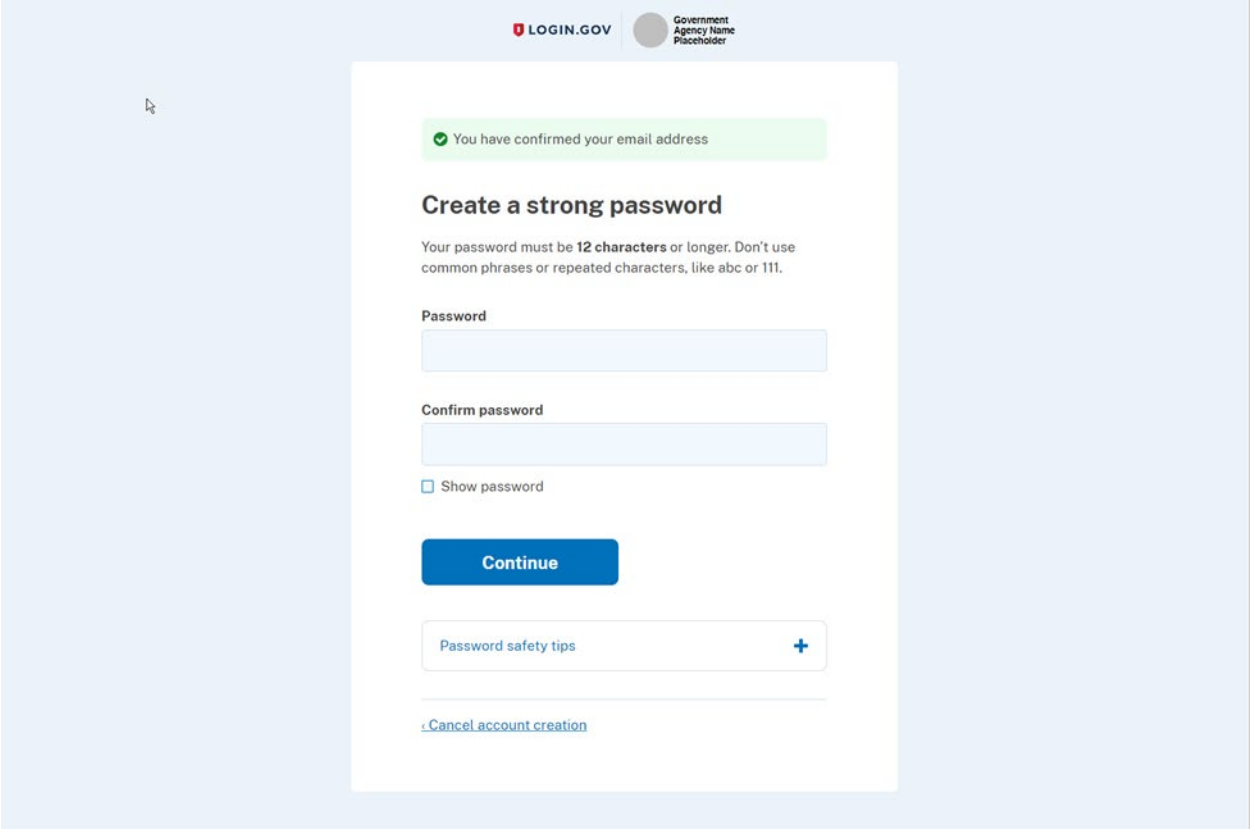
3. Check your email to confirm your account by clicking on the link provided in the message body.



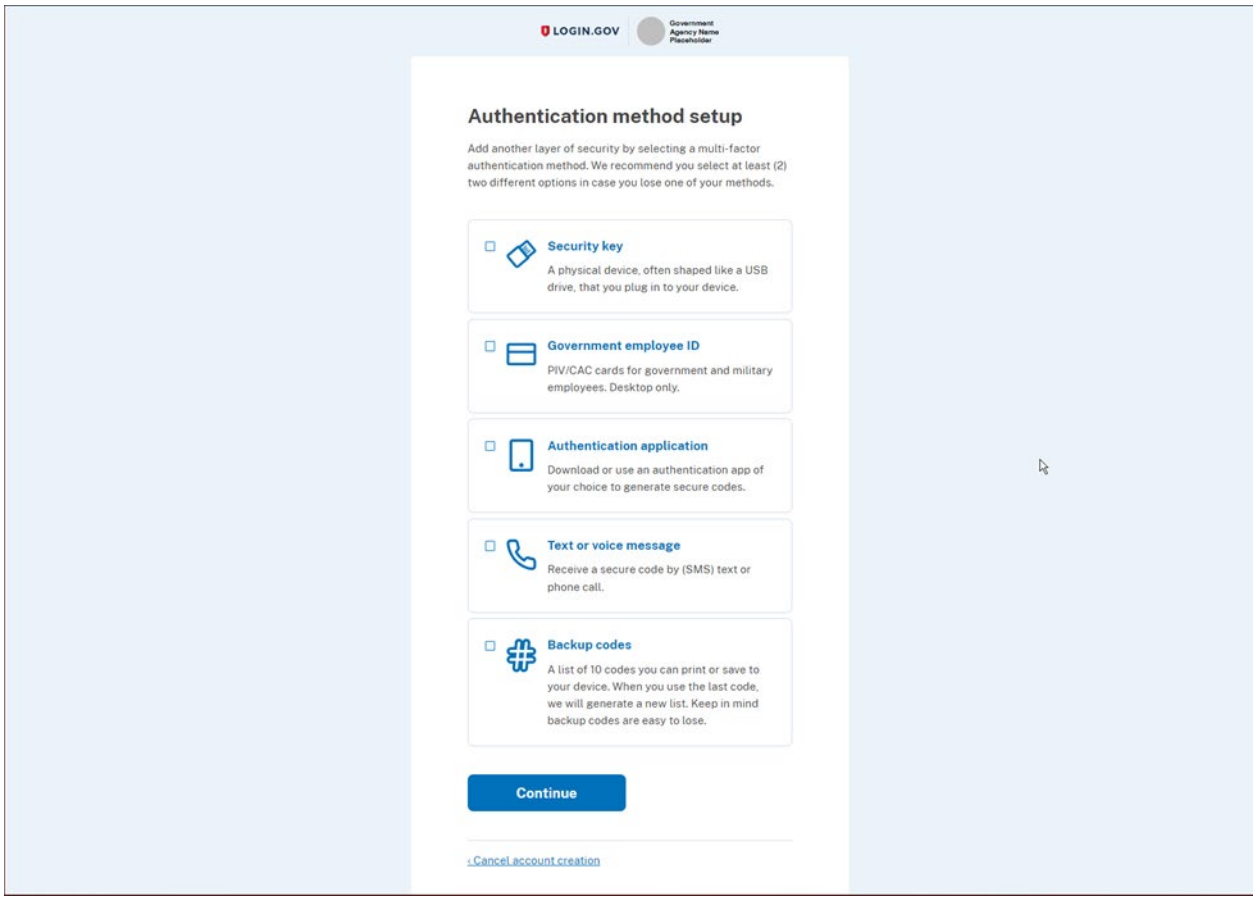
3a. Email message body with included link



4. Create a strong password containing at least 12 characters and be sure to store in a safe place. Click “Continue” button.



5. Select a two-factor authentication method. Login.gov requires you to set up a secondary authentication method to keep your account secure as an added layer of protection. This is referred to as two-factor authentication (2FA).



You can choose from several authentication options:

More secure:

- Authentication application
- PIV or CAC card for federal government employees or military

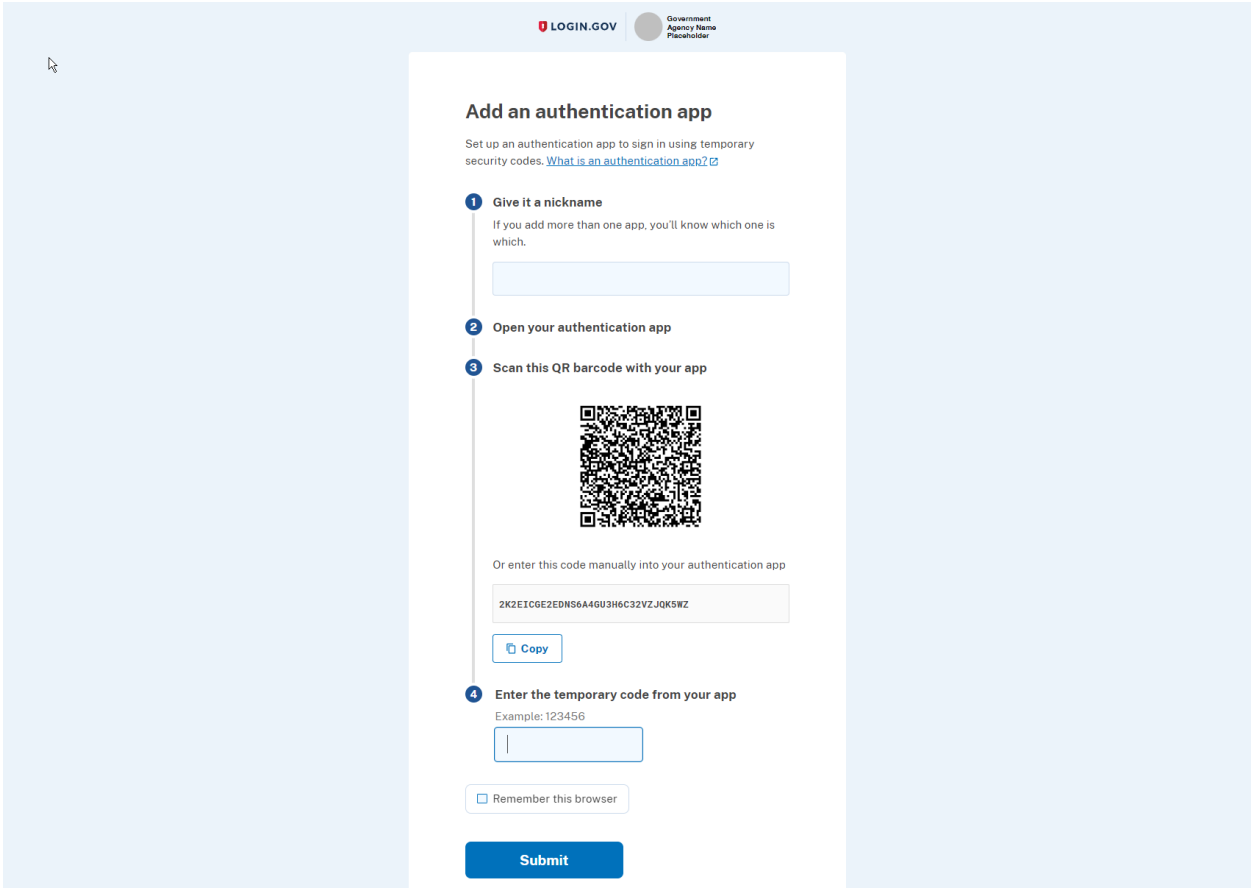
Less secure:

- Text/Voice message

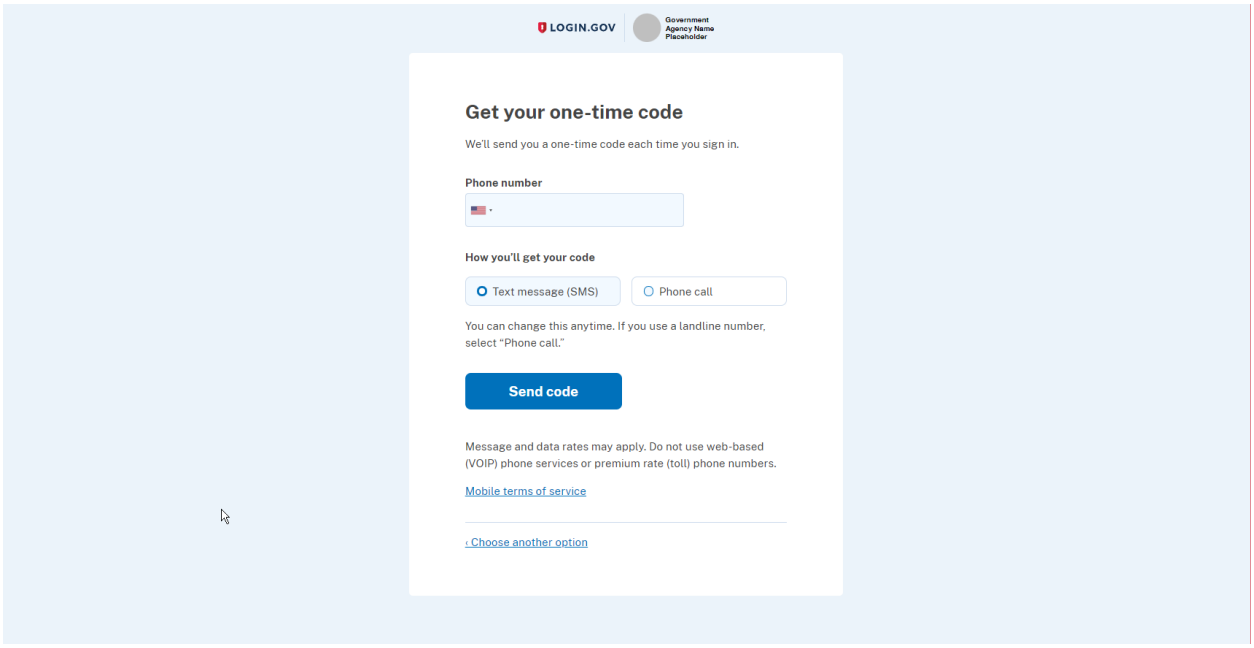
NOTE: For more information on these authentication methods, click here.

Authentication methods

Authentication application



Text/Voice Message



Authentication options

In addition to your password, Login.gov requires that you set up at least one secondary authentication method to keep your account secure. This is two-factor authentication (2FA). We use 2FA as an added layer of protection to secure your information. Although you can choose from several authentication options, some authentication methods such as security keys, PIV/CAC cards, and authentication applications are more secure against phishing and theft. We encourage you to add two methods for authentication to your account. If you lose access to your primary authentication method (i.e., losing your phone), you'll have a second option to gain access to your account. Login.gov is unable to grant you access to your account if you get locked out and/or lose your authentication method.

Authentication options	Definition
Authentication application	Authentication applications are downloaded to your device and generate secure, six-digit codes you use to sign in to your accounts. While authentication applications are not protected if your device is lost or stolen, this method offers more security than phone calls or text messaging against phishing, hacking, or interception. If you choose this secure option, follow these steps to download and install one of the supported applications and configure it to work with Login.gov. 1. Choose a device, such as a computer or mobile device (phone or tablet), on which you can install apps. 2. Download and install an authentication app to your device. Some popular options include: • Android and iOS apps: Google Authenticator, Authy, LastPass, 1Password. • Windows and macOS apps: 1Password, OTP Manager. • Chrome extensions: Authenticator. 3. Open a new browser and sign in to your Login.gov account at https://secure.login.gov/. 4. Select "Enable" next to "Authentication app" and follow the instructions to scan or enter a code associating your authentication app with your account. You will now be able to use the one-time passcodes generated by the application each time you sign in to Login.gov.
Security key	A security key is typically an external physical device, like a USB stick that plugs into your computer. The key is linked to your accounts and will only grant access to those accounts once the key is inserted and activated. Since a security key does not rely on your cell phone, it has the highest level of protection against phishing and built-in protections against hacking if it is lost or stolen. Login.gov requires security keys that meet the FIDO (Fast Identity Online) standards. You can add as many security keys as you want to secure your account. To use this secure option for Login.gov authentication, insert the key into the USB port and assign the key a name to identify it with your

	Login.gov account. You may need to press a button on the key to begin the setup process. The system will then prompt you to activate your key.
PIV or CAC for federal government employees and military	Physical PIV (personal identity verification) cards or CACs (common access cards) are secure options for federal government employees and military personnel. These cards, with encrypted chip technology, are resistant to phishing and difficult to hack if stolen.
Text message / Phone call	Text messages/SMS or phone calls are convenient but are extremely vulnerable to theft, hackers, and other attacks. If you choose to use this less secure option, enter a phone number to which you can receive phone calls or text messages. If you only have a landline, you must receive your security code by phone call. Login.gov cannot send security codes to extensions or voicemails. The system will send a unique security code to that phone number each time you sign in to your Login.gov account. Each security code expires after ten minutes and can only be used once. If you don't enter the security code within ten minutes, request a new code. After you receive the code, type it into the "one-time security code" field. Each time you sign in to Login.gov, you'll have the option of getting a new security code by phone call or by text. You will receive a new security code each time you sign in to your Login.gov account.
Backup codes (less secure)	Backup codes are an accessible option for users who do not have access to a phone. However, backup codes are the least secure option for two-factor authentication. Backup codes must be printed or written down which makes them more vulnerable to theft and phishing. If you select this less secure option, Login.gov will generate a set of ten codes. After you sign in with your username and password, you will be prompted for a code. Each code may be used only once. When the tenth code has been used, you will be prompted to download a new list. Treat your recovery codes with the same level of care as you would your password.
No phone or other authentication method (less secure and not recommended)	If you do not have access to a phone, authentication application, security key, or any other authentication option, you can set up your account with only backup codes. Warning: Setting up your account with backup codes as your only authentication method is not recommended. If you ever lose your backup codes, you will not be able to sign in to your account. When you create your account, you will reach the "Secure your account" page. This is where you must choose your primary authentication method. If you do not have access to any of the other options, select "Backup codes" and click "Continue." On the "Add another method" page, select "I don't have any of the above" and click "Continue."