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.

NIST	
🖶 National Volu	untary Laboratory Accreditation Program (NVLAP)
	Welcome This customer portal is a secure on-line tool that enables your organization to apply for and manage Our NVLAP accredition while keeping relevant accreditation records up to date. Our NVLAP website Our During Sign In This button will take you to the login gov identity provider authentication site. Dor have a login gov account? Click here to create one.
	Sign in with ULOGIN.GOV
	WARNING *** WARNING This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal. ovil, and/or administrative action. All information on this computer system may be intercepted recorded read. copied. and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.
	OMB Number: 0693-0003 Approval Expires: January 31, 2025
	A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995 unless the information collection has a currently vial OMS Control Number. The approved OMB Control Number for this information collection is 04300. Without this approval, we could not conduct this information collection. Public reporting for this information collection is estimated to be approximately a Johours per response, including the time for reviewing instructions, sending add sacures, galanting the data needed, and completing and reviewing the information collection. All responses to this information collection are required to obtain benefits. Send comments regarding this burdler estimate or any other sagect of this information collection required to obtain benefits. Send comments regarding this burdler estimate of this information collection. Johnes and the provide the obtain benefits. Send comments regarding this burdler estimate of this information collection in estimated to the National Institute of Standards and Technology/NVLAP at: 100 Bureau Drive. Stop 2140, Gaithersburg MD 20899-2140, Atm: Bethany Hackett, Quality Manager.
	powered by TouchStone v1.8

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

	LOGIN.GOV Government Agency Name Placeholder
	NVLAP - rNIS Customer Portal (Dev) is using Login.gov to allow you to sign in to your account safely and securely.
Pe	Sign in Create an account
	Sign in for existing users
	Email address
	Password
	Show password
	Sign 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.

an roomally cloop and y accompany room
Welcome This customer portal is a secure on-line tool that enables your organization to apply for and manage your NVLAP accreditation while keeping relevant accreditation records up to date.
Sign In This button will take you to the Login gov identity provider authentication site. There have a Login gov account? Child Noise to View or and
Webbang *** widebung *** widebung *** widebung This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel, insultationed access or use of this computer system may subject violation to commail, civil, and/or administrative action. All andromation on this comparter system may subject violation to commail, civil, and/or administrative action. All purposes, insularing criminal investigations. Such altornation includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any percent, whether perms.
ONE Number: 0693-0603 Aggrees (Express; january 31, 2225 A Federal agency may not conduct or sponsor, and a person is not required to respond to; nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Ast of 1995 unless the functionation collection has a currently und OMI Correlation Mumber. The approvad OMI Correlation Withomation collection to 0903-0003. Without this approval, we could not conduct this information collection. Public reporting for this information collection to 0903-0003. Without this approval, we response, including the time for relevancy to testications, sanching existing data sources, gathering and munitariang the data needed, and completing and revensing the information collection. All responses to this information collection for reducing the Surface Long Commission gradies and and revensing the information collection. All responses to this information collection for reducing the Surface Long Commission gradies and burdene estimate <i>carry</i> of the information collection, and responses to this information collection for reducing the Surface Long Commission Bartistice of Standards and Technology/WYLAP at: 100 Bureau Drive. Stap 2140. Gathersburg MD 20095-2140. Attr: Bertiany Hockett, Quality Manager.

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

CLOGIN.GOV
Create your account
Select your email language preference Login.gov allows you to receive your email communication in English, Spanish or French. • English (default) • Español • Français • I read and accept the Login.gov Rules of Use @ Submit Cancel Security Practices and Privacy Act Statement @ Privacy Act Statement @

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

LOGIN.GOV Government Agency Name Placeholder	
Check your email We sent an email to pnacelli@penacity.us with a link to confirm your email address. Follow the link to continue creating your account.	
Didn't receive an email? <u>Resend</u>	
Or, <u>use a different email address</u> You can close this window if you're done.	

3a. Email message body with included link



Sent at 2023-06-12T14:29:44.179729Z

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

	LOGIN.GOV Government Agency Name Placeholder
R	You have confirmed your email address
	Create a strong password
	Your password must be 12 characters or longer. Don't use common phrases or repeated characters, like abc or 111.
	Password
	Confirm password
	Show password
	Continue
	Password safety tips +
	Cancel account creation

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:

• <u>Text/Voice message</u>

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

Authentication methods

Authentication application

	Covernment Agency Name Placeholder	
А	dd an authentication app	
Se	up an authentication app to sign in using temporary urity codes. <u>What is an authentication app?</u> 凶	
0	Give it a nickname If you add more than one app, you'll know which one is which.	
e	Open your authentication app	
0	Scan this QR barcode with your app	
	Or enter this code manually into your authentication app	
	2K2EICGE2EDNS6A4GU3H6C32VZJQK5WZ	
0	Enter the temporary code from your app Example: 123456	
	Remember this browser	
	Submit	

Text/Voice Message

Cat your one-time code each time you sign it. De unuber De vorting et your code Our contage De vorting et your code De vorting et at rates may apply. Do not use web-based for phone catility phone services or premum rate (tolit) phone numbers. Duble terms of service Duble terms of service
How you'll get your code Image: Text message (SMS) Image: Text message (SMS) <
V text indedec folds) C house dut You can change this anytime. If you use a landline number, select "Phone call." Send code Message and data rates may apply. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers. Mobile terms of service .Choose another option
Send code Message and data rates may apply. Do not use web-based (VOIP) phone services or premium rate (toll) phone numbers. Mobile terms of service .Choose another ontion
(VOIP) phone services or premium rate (toll) phone numbers. Mobile terms of service
۲ <u>۲ Choose another option</u>

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.
	 Choose a device, such as a computer or mobile device (phone or tablet), on which you can install apps.
	 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.
	 Open a new browser and sign in to your Login.gov account at <u>https://secure.login.gov/</u>.
	 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."