

## BRICS Login using RAS

The traditional username/password login flow for BRICS has been replaced by NIH's Researcher Auth Service (RAS). This change will require all users to follow a set of steps to log in/sign up for RAS and link your BRICS account to your RAS account. RAS supports these identity providers: **NIH PIV/CAC, VA PIV, DOD CAC cards. Login.gov account with assurance level 2 or an ID.me account with assurance level 2.**

Users with an NIH/HHS/DOD account should use their NIH PIV/CAC, VA PIV, DOD CAC cards as the identity provider when logging in with RAS.

Users based in the US and without one of the cards listed above will need to use Login.gov with identity assurance level 2. If the user does not already have a Login.gov account, they will need to create one and then select Login.gov as the identity provider when logging in with RAS. Then verify for identity assurance level 2 before they will be able to use their BRICS instance.

International users will need to use an [ID.me](#) account with identity assurance level 2. If the user does not already have an account, they will need to create one and select it when logging in with RAS. Then verify for identity assurance level 2 before they will be able to use their BRICS instance.

[Click here to learn more about Researcher Auth Service \(RAS\)](#)

## INDEX

- 1. Logging in using RAS**
  - 1.1. Logging in with PIV/Smart Cards
  - 1.2. Logging in with Login.gov
  - 1.3. Logging in with ID.me
- 2. Linking RAS and BRICS account**
- 3. Request BRICS Account**
- 4. Login.gov – Identity Assurance Level 2 (IAL2)**
  - 4.1. Verifying state-issued ID
  - 4.2. Verifying personal details
  - 4.3. Verifying phone or address
  - 4.4. Secure your account
- 5. ID.me – Identity Assurance Level 2 (IAL2)**
  - 5.1. Verifying identification document
- 6. Other Changes**
  - 6.1. Logging out of BRICS/RAS
  - 6.2. API Token
- 7. Contacts and Links**

## Logging in using RAS

Users can log into their BRICS system by using one of the following login methods:

1. Using their PIV/Smart card which includes **NIH PIV/CAC, VA PIV, DOD CAC cards.**
2. Using Login.gov
3. Using ID.me

**NOTE: Users signing in with login.gov or ID.me will be required to get Identity Assurance Level 2 (IAL2). This guide will show the necessary steps.**

## Logging in with PIV/Smart Cards

For current users with a NIH PIV/CAC card, please follow these steps:

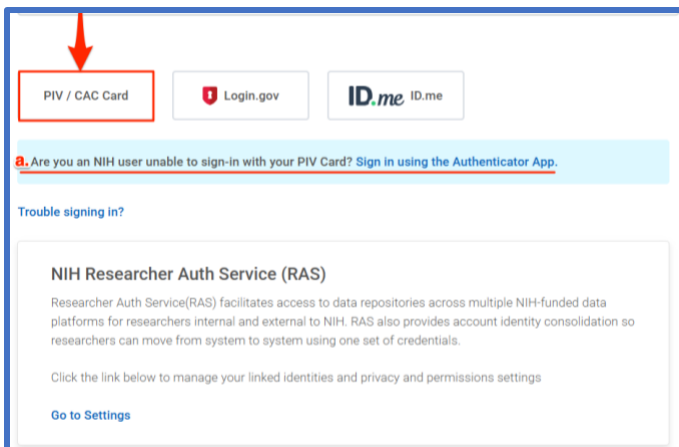
1. Navigate to your BRICS instance and select Log in.
2. Here you will see the new Log in page. Should you have a NIH PIV/CAC card, it is preferred to Log in with it. Click the “**Log In**” button and continue to the next step.  
If you do not have a PIV card you will need to follow the steps in [Existing user Log in with Login.gov](#)

NOTE: BRICS will no longer be handling your Log in credentials. For assistance with your account credentials follow steps:

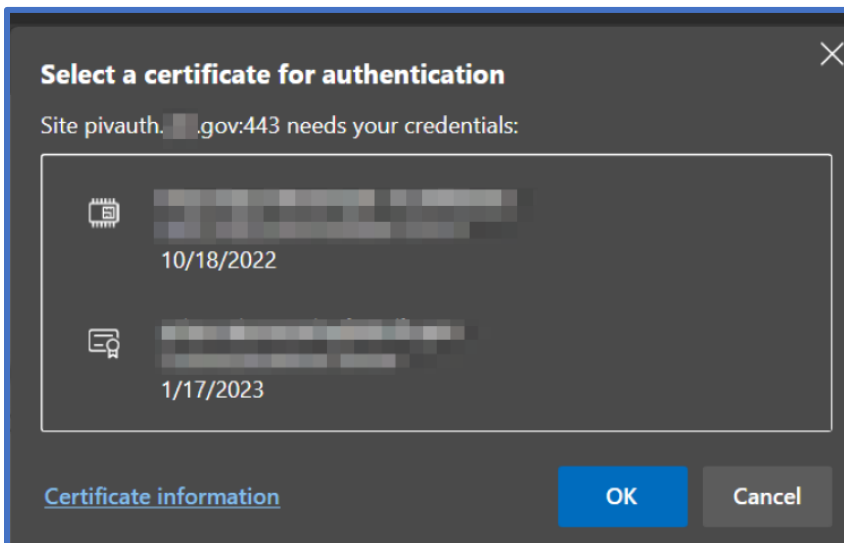
- a. Forgot NIH PIV credentials: <https://auth.nih.gov/CertAuthV3/forms/mfa/Help.html>
- b. Forgot Login.gov password: <https://secure.login.gov/users/password/new>
- c. Forgot ID.me password: <https://help.id.me/hc/en-us>

<h3>Log In to Your Account</h3> <p>Please log in using one of the Researcher Auth Service (RAS) identities (Smart Card, Login.gov, or ID.me), the required multi-factor authentication, to access NEI.</p> <p>If you have any of the following smart cards: NIH PIV, VA PIV or DoD CAC, please use it to log in. Otherwise, use your Login.gov or ID.me account.</p> <div><b>Log In with RAS</b></div> <p>If you are a new user you will need to <a href="#">create a Login.gov account</a> or <a href="#">an ID.me account</a>.</p>	<p>For security reasons, please log out and exit your web browser when you are done accessing services that require authentication.</p> <p><b>Issues with PIV/CAC cards?</b> Please contact <a href="#">NIH Help Desk</a> 301-496-4357(6-HELP) or 866-319-4357 (toll-free) for further assistance.</p> <hr/> <p><b>Issues with Login.gov?</b> Please contact <a href="#">Login.gov Help Center</a> for further assistance.</p> <hr/> <p><b>Issues with ID.me?</b> Please contact <a href="#">ID.me Help Center</a> for further assistance.</p> <hr/> <p><b>Warning Notice</b></p> <p>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, civil, and/or administrative action.</p> <p>All information in 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. There is no right of privacy in this system.</p>
--	--

3. After clicking with “**Log In**” you will be taken to the following page. Select **PIV/Smart Card**.
  - a. If you are unable to sign in with your PIV card, then you may sign in using the [Authenticator App](#) instead.



4. Provide your NIH PIV/CAC card authentication by selecting the appropriate certificate and provide your PIN:



5. If you are a new user, please proceed here to [create your BRICS account](#).  
If you are an old user that use to use the traditional email/password login and has not signed in with RAS, please proceed [to link your account with RAS](#).

## Logging in with Login.gov

1. Navigate to your BRICS instance and select Log in.
2. Here you will see the new Login page. If you have a NIH PIV/CAC card is recommended to Log in with it by following steps in [Existing user Log in with a NIH PIV/CAC card](#).

If you do not have a Login.gov account select the “**create a Login.gov account**” link under the login button. Otherwise skip to logging into RAS at step 4.

**NOTE:** BRICS will no longer be handling your Log in credentials. For assistance with your account credentials follow steps:

- a. Forgot NIH PIV credentials: <https://auth.nih.gov/CertAuthV3/forms/mfa/Help.html>
- b. Forgot Login.gov password: <https://secure.login.gov/users/password/new>
- c. Forgot ID.me password: <https://help.id.me/hc/en-us>

### Log In to Your Account

Please log in using one of the Researcher Auth Service (RAS) identities (Smart Card, Login.gov, or ID.me), the required multi-factor authentication, to access NEI.

If you have any of the following smart cards: NIH PIV, VA PIV or DoD CAC, please use it to log in. Otherwise, use your Login.gov or ID.me account.

Log In with RAS

If you are a new user you will need to [create a Login.gov account](#) or [an ID.me account](#).

For security reasons, please log out and exit your web browser when you are done accessing services that require authentication.

**Issues with PIV/CAC cards?**  
Please contact [NIH Help Desk](#) 301-496-4357(6-HELP) or 866-319-4357 (toll-free) for further assistance.

---

**Issues with Login.gov?**  
Please contact [Login.gov Help Center](#) for further assistance.

---

**Issues with ID.me?**  
Please contact [ID.me Help Center](#) for further assistance.

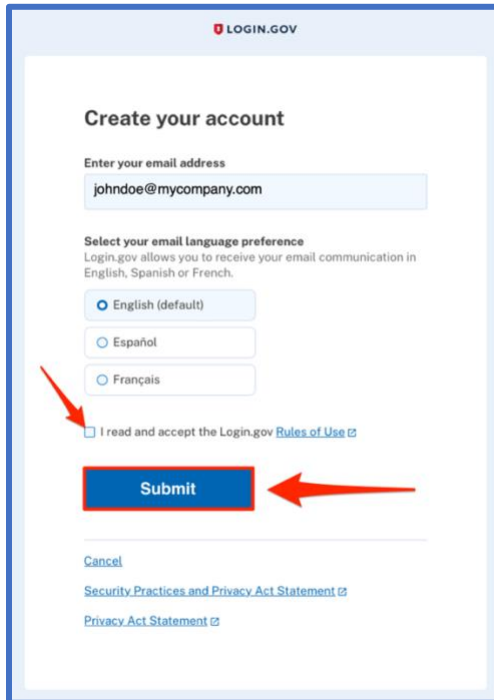
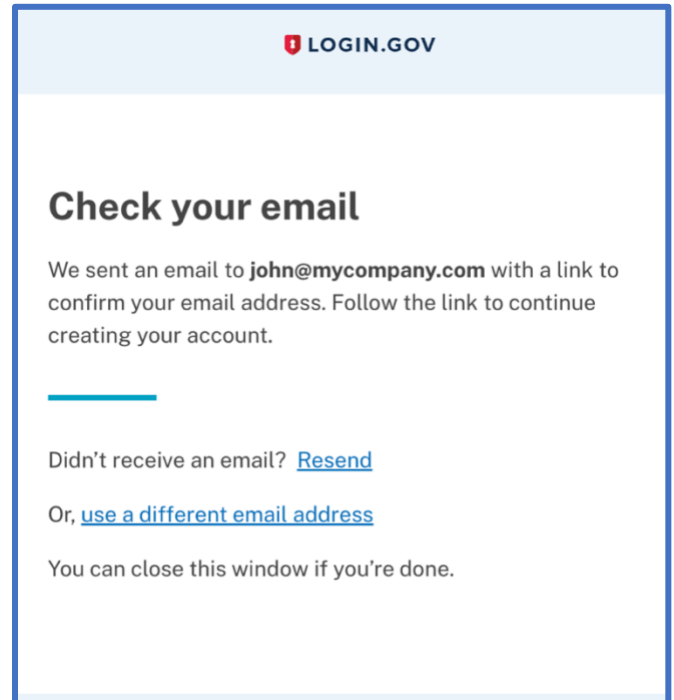
---

**Warning Notice**

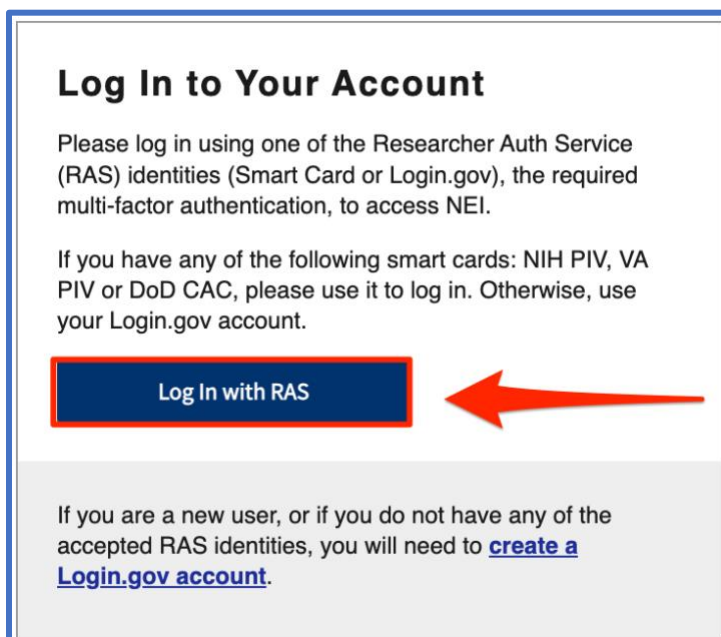
This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information in 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. There is no right of privacy in this system.

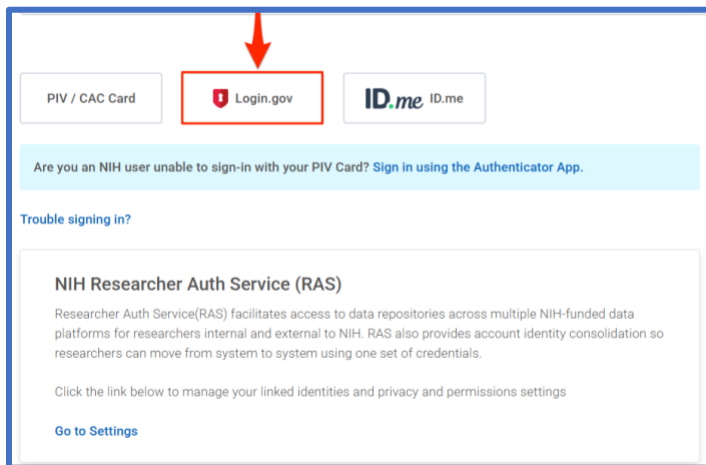
3. Create your Login.gov account with your desired email. Afterwards check your email to verify and finish creating your Login.gov account.

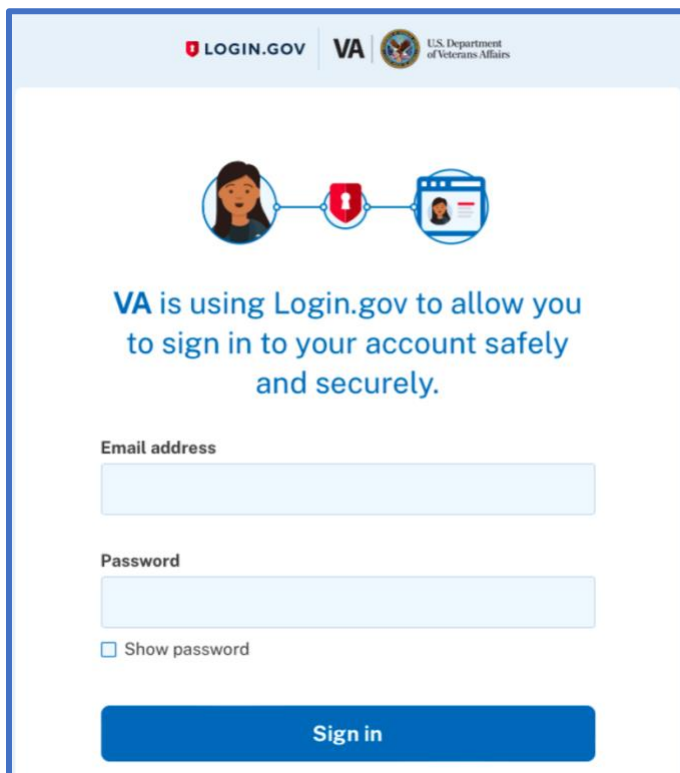
4. After creating and verifying your Login.gov account, navigate back to your BRICS instance Log in page and select “**Log In**”.



5. Select “**Login.gov**”



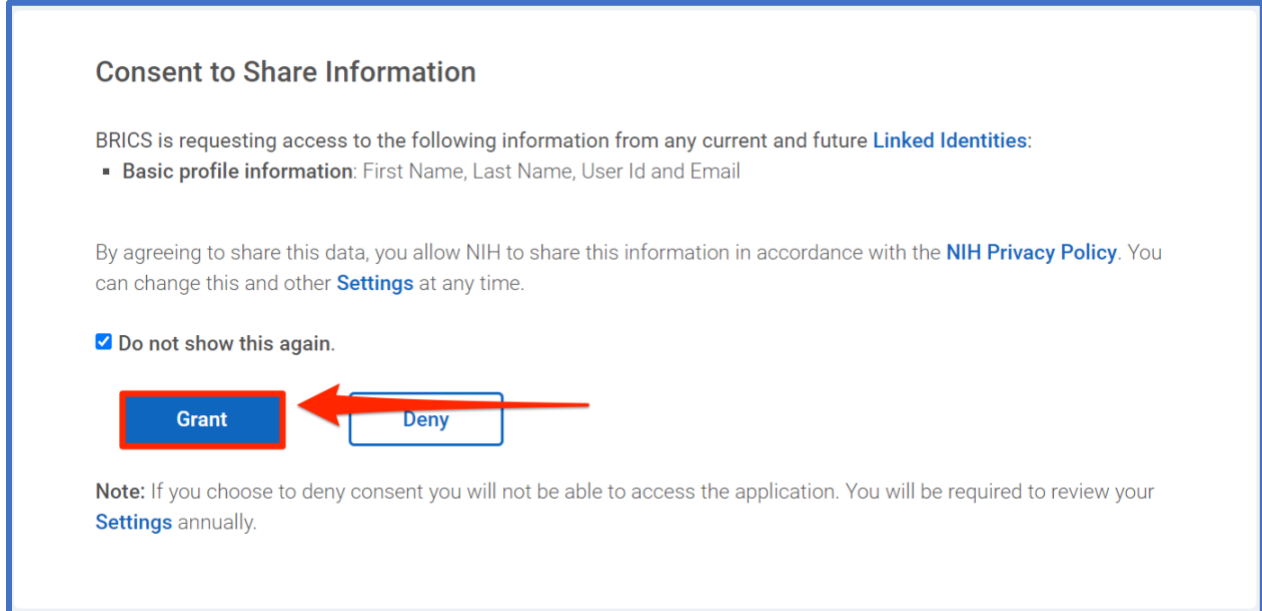
6. Enter your **Login.gov** credentials and select **Sign In**:



7. After logging in, users that have not verified their identities for Login.gov may be prompted too. Please follow the steps at section [Login.gov – Identity Assurance Level 2 \(IAL2\)](#)



8. After verifying identity for IAL2, when users first authenticate through Login.gov, they will need to grant permission to BRICS to have access to their basic profile information.



**Consent to Share Information**

BRICS is requesting access to the following information from any current and future [Linked Identities](#):

- **Basic profile information:** First Name, Last Name, User Id and Email

By agreeing to share this data, you allow NIH to share this information in accordance with the [NIH Privacy Policy](#). You can change this and other [Settings](#) at any time.

☒ Do not show this again.

[Grant](#) [Deny](#)

**Note:** If you choose to deny consent you will not be able to access the application. You will be required to review your [Settings](#) annually.

9. If you are a new user, please proceed here to [create your BRICS account](#).  
If you are an old user that use to use the traditional email/password login and has not signed in with RAS, please proceed [to link your account with RAS](#).

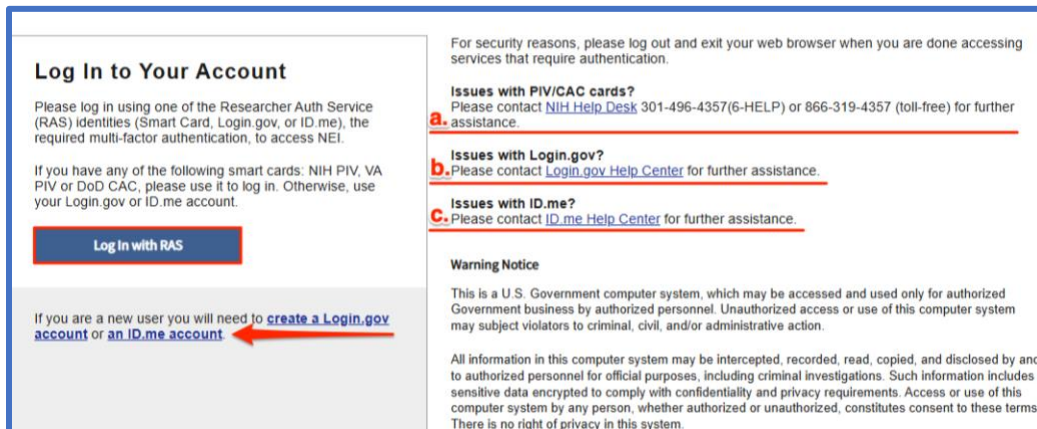
## Logging in with ID.me

1. Navigate to your BRICS instance and select Log in.
2. Here you will see the new Log in page. If you have a NIH PIV/CAC card is recommended to Log in with it by following steps in [Existing user Log in with a NIH PIV/CAC card](#).

ID.me accounts can be used for **international users** allowing users **outside of the US to still get access to BRICS**.

If you do not have a ID.me account select the “[create a ID.me account](#)” link under the login button. Otherwise skip to step 4.

- a. Forgot NIH PIV credentials: <https://auth.nih.gov/CertAuthV3/forms/mfa/Help.html>
- b. Forgot Login.gov password: <https://secure.login.gov/users/password/new>
- c. Forgot ID.me password: <https://help.id.me/hc/en-us>



**Log In to Your Account**

Please log in using one of the Researcher Auth Service (RAS) identities (Smart Card, Login.gov, or ID.me), the required multi-factor authentication, to access NEI.

If you have any of the following smart cards: NIH PIV, VA PIV or DoD CAC, please use it to log in. Otherwise, use your Login.gov or ID.me account.

**Log In with RAS**

If you are a new user you will need to [create a Login.gov account](#) or [an ID.me account](#)

For security reasons, please log out and exit your web browser when you are done accessing services that require authentication.

**Issues with PIV/CAC cards?**  
Please contact [NIH Help Desk](#) 301-496-4357(6-HELP) or 866-319-4357 (toll-free) for further assistance.

**Issues with Login.gov?**  
Please contact [Login.gov Help Center](#) for further assistance.

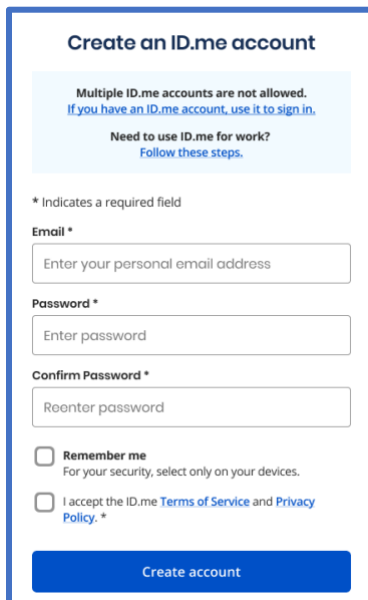
**Issues with ID.me?**  
Please contact [ID.me Help Center](#) for further assistance.

**Warning Notice**

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, civil, and/or administrative action.

All information in 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. There is no right of privacy in this system.

3. Enter account details and click create account. User will need to then verify their email.



**Create an ID.me account**

Multiple ID.me accounts are not allowed.  
If you have an ID.me account, use it to sign in.

Need to use ID.me for work?  
Follow these steps.

\* Indicates a required field

**Email \***

Enter your personal email address

**Password \***

Enter password

**Confirm Password \***

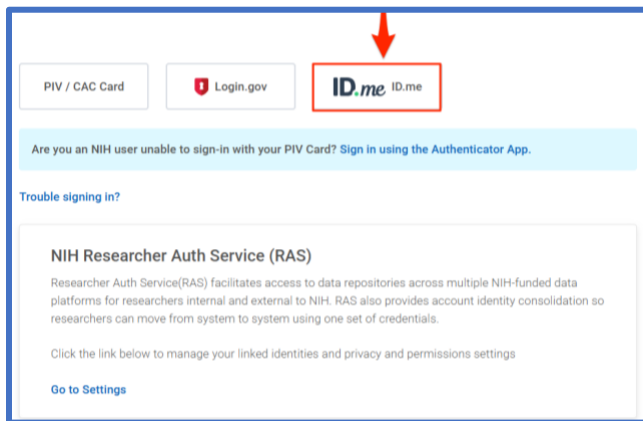
Reenter password

☐ **Remember me**  
For your security, select only on your devices.

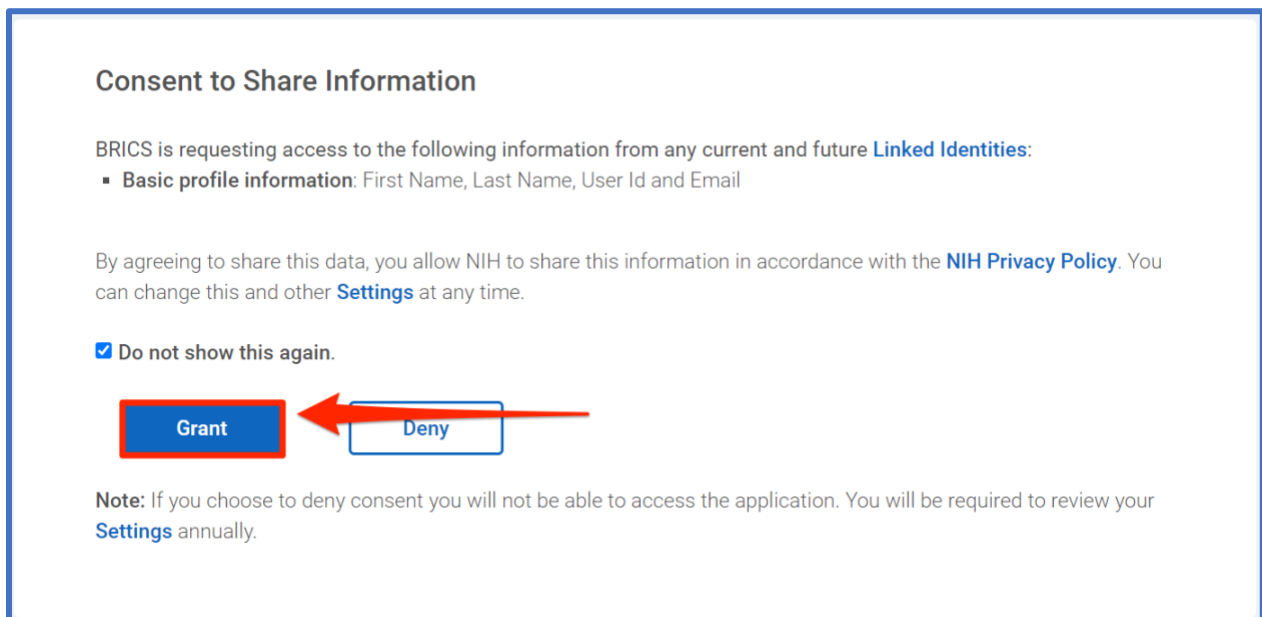
☐ I accept the ID.me [Terms of Service](#) and [Privacy Policy](#). \*

**Create account**

- After creating your account navigate back and log into BRICS using RAS and select ID.me



- After creating the ID.me account and signing into it through BRICS. Users that have not verified their identities for ID.me may be prompted to verify their identities: Please follow the steps at section [ID.me –Identity Assurance Level 2 \(IAL2\)](#)
- After verifying identity for IAL2, when users first authenticate through ID.me, they will need to grant permission to BRICS to have access to their basic profile information.

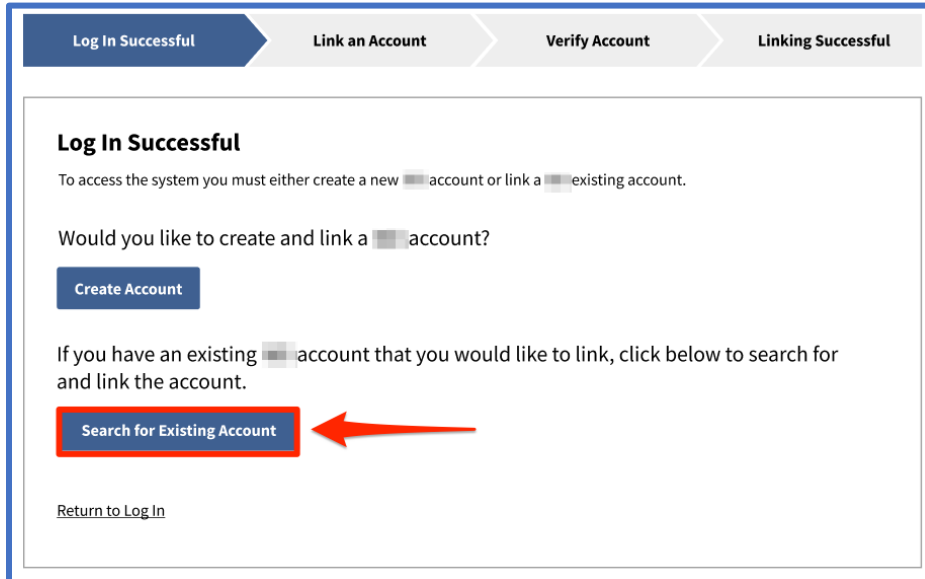


- If you are a new user, please proceed here to [create your BRICS account](#).  
If you are an old user that use to use the traditional email/password login and has not signed in with RAS, please proceed [to link your account with RAS](#).

## Linking RAS and BRICS account

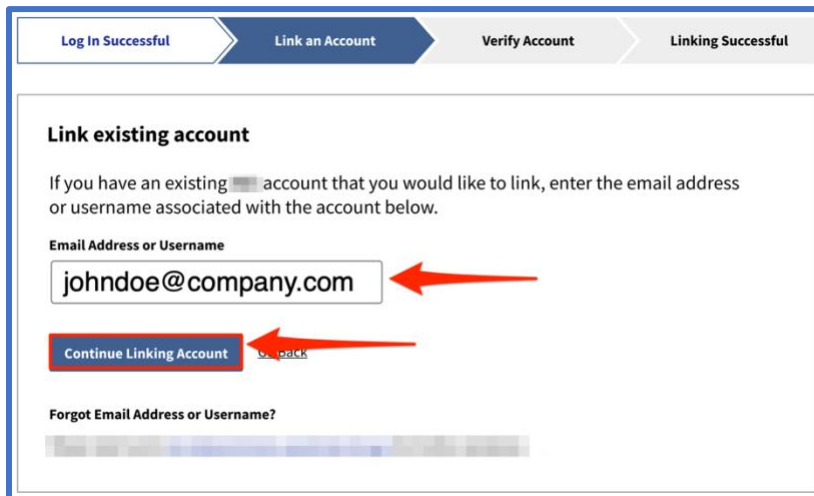
This section is only for users who had a BRICS account with a traditional email/password login and never linked their RAS account with their BRICS account.

1. After logging in via RAS: If you have an account continue by selecting “[Search for Existing Account](#)”.



The screenshot shows a progress bar at the top with four steps: 'Log In Successful' (active), 'Link an Account', 'Verify Account', and 'Linking Successful'. The main content area is titled 'Log In Successful' and contains the following text: 'To access the system you must either create a new account or link a existing account.' Below this is the question 'Would you like to create and link a account?' with a 'Create Account' button. Further down, it says 'If you have an existing account that you would like to link, click below to search for and link the account.' The 'Search for Existing Account' button is highlighted with a red box and a red arrow points to it. At the bottom left, there is a link 'Return to Log In'.

2. Enter your email/username of your BRICS account you wish to link:

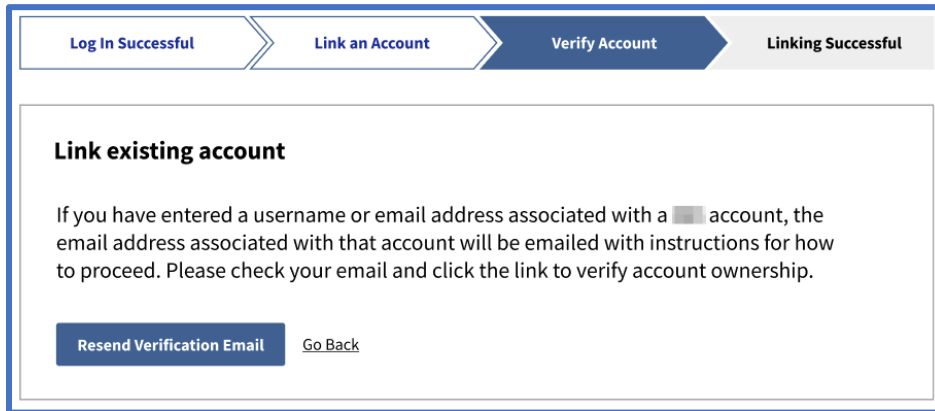


The screenshot shows the same progress bar as the previous screen. The main content area is titled 'Link existing account' and contains the text: 'If you have an existing account that you would like to link, enter the email address or username associated with the account below.' Below this is a label 'Email Address or Username' and an input field containing 'johndoe@company.com'. A red arrow points to the input field. Below the input field is a 'Continue Linking Account' button, which is highlighted with a red box and a red arrow points to it. At the bottom left, there is a link 'Forgot Email Address or Username?'.

3. Verify your account by going to the email account associated to your BRICS account and clicking the verify account ownership link.

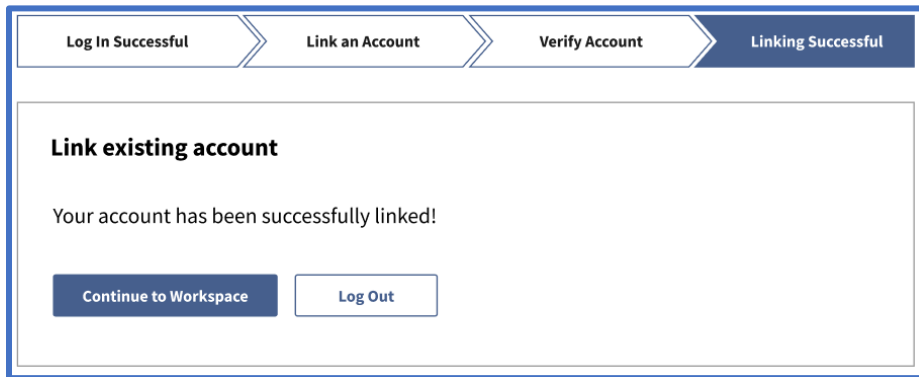
**If you do not see your email, please do the following:**

- a. Wait for the email to be received.
- b. Check your spam folder for the email.
- c. Resend the verification email using the “[Resend Verification Email](#)” button.
- d. Ensure you have entered your email/username correctly in step 6.
- e. Contact your operations team for any additional help.



The screenshot shows a progress bar at the top with four steps: 'Log In Successful', 'Link an Account', 'Verify Account' (highlighted), and 'Linking Successful'. Below the progress bar, the heading 'Link existing account' is followed by a paragraph: 'If you have entered a username or email address associated with a [redacted] account, the email address associated with that account will be emailed with instructions for how to proceed. Please check your email and click the link to verify account ownership.' At the bottom, there is a dark blue button labeled 'Resend Verification Email' and a text link labeled 'Go Back'.

4. Congratulations! Your account should now be successfully linked, and you can continue to your BRICS workspace.



The screenshot shows a progress bar at the top with four steps: 'Log In Successful', 'Link an Account', 'Verify Account', and 'Linking Successful' (highlighted). Below the progress bar, the heading 'Link existing account' is followed by a message: 'Your account has been successfully linked!'. At the bottom, there are two buttons: a dark blue button labeled 'Continue to Workspace' and a white button with a dark blue border labeled 'Log Out'.

5. You may be redirected to the E-signature page if you have not submitted your e-signature before.

**NOTE: Submission of your E-Signature is required to access your BRICS instance.**

## Electronic Signature

The system uses electronic documentation which may require you to provide an electronic signature when you enter, submit, change, access, download, or audit electronic data records.

**ELECTRONIC SIGNATURE.** This Acknowledgement and Certification of Understanding ("Acknowledgement") is to inform you that by submitting an electronic signature, you are providing an electronic mark that is held to the same standard as a legally binding equivalent of a handwritten signature provided by you. For purposes of the acknowledgement, a digital mark is considered your legally typed First and Last Name (legal name may include middle name, initial or suffix). A date will be recorded with both entries. Any part of the system requiring an electronic signature may contain a signature acknowledgment statement provided in the same area requiring the electronic signature.

**AGREEMENT:** By signing this Acknowledgement, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding. I also understand that it is a violation for any individual to sign/e-sign any transactions that occur within system on behalf of me. Any fraudulent activities related to electronic signatures must be immediately reported to the system operations team. Violation of these terms could lead to disciplinary action, up to termination, and prosecution under applicable Federal laws.

**CERTIFICATION OF UNDERSTANDING:** I also understand, acknowledge, agree and certify that:

- I accept my responsibilities in the use of electronic signatures as described on this form.
- My execution of any form of an electronic signature function performed on the system to be the legally binding equivalent of my traditional handwritten signature, and that I am accountable and responsible for actions performed under such an electronic signature.
- I will not share components of my electronic signature such that my signature could be executed by another individual. Such components may include, but are not limited to legal name, passwords or any such identifiers.

**First Name\***

**Middle Name**

**Last Name\***

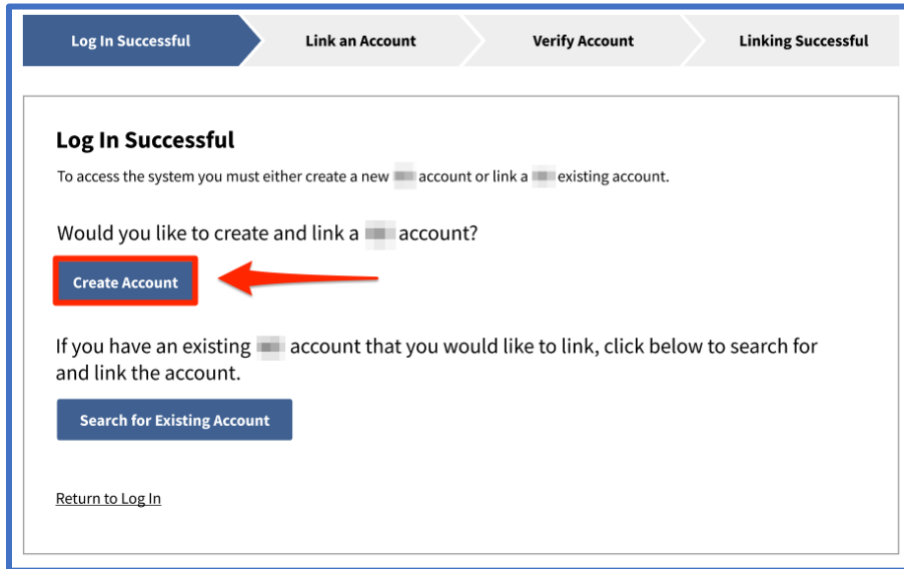
☐ I understand and agree to all of the Terms and Conditions in this electronic documentation for use of Electronic Signature Agreement. Please check the appropriate box to provide your signature.

**Submit**

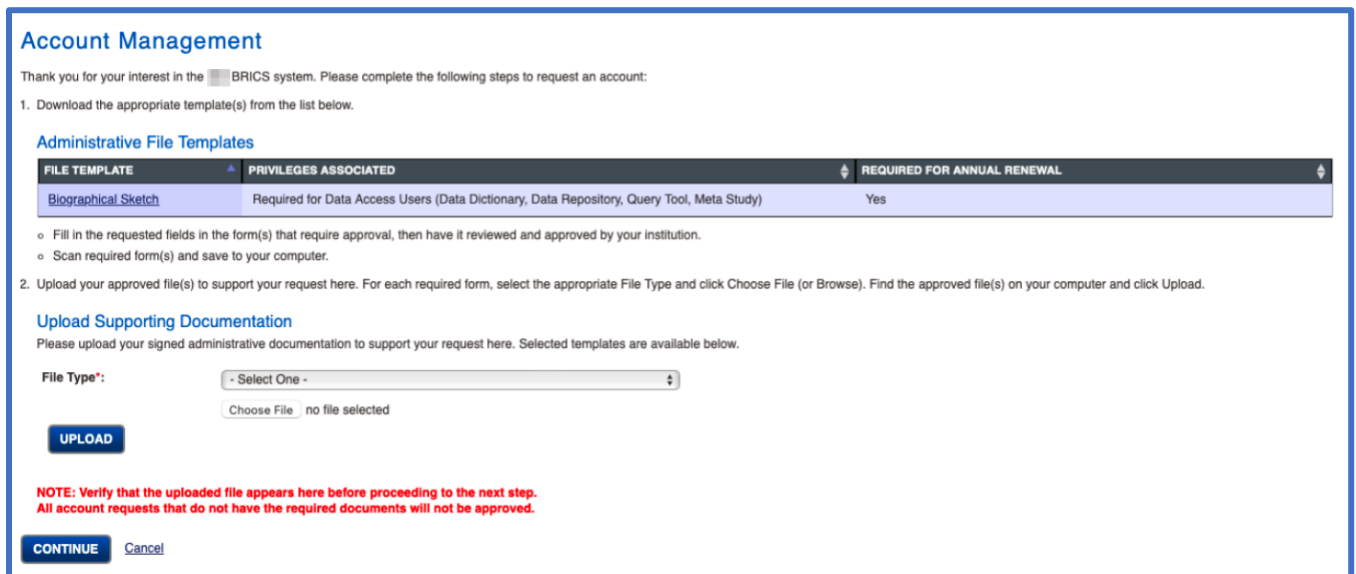
## Request BRICS Account

For new users that do not have an account on the BRICS instance yet follow these steps:

1. After logging in via RAS. Select the “**Create Account**” button to create a new account.



2. The account management page will load where you will need to upload supporting documentation for your BRICS account. After an account request you will need to wait until your account is approved to get access to the BRICS instance. Users will have access to the account management module before approval and may log back in to upload additional supporting documentation at any time.



FILE TEMPLATE	PRIVILEGES ASSOCIATED	REQUIRED FOR ANNUAL RENEWAL
Biographical Sketch	Required for Data Access Users (Data Dictionary, Data Repository, Query Tool, Meta Study)	Yes

**Administrative File Templates**

- Fill in the requested fields in the form(s) that require approval, then have it reviewed and approved by your institution.
- Scan required form(s) and save to your computer.

**Upload Supporting Documentation**

Please upload your signed administrative documentation to support your request here. Selected templates are available below.

File Type\*: - Select One -

Choose File no file selected

UPLOAD

**NOTE:** Verify that the uploaded file appears here before proceeding to the next step. All account requests that do not have the required documents will not be approved.

CONTINUE Cancel

3. On your first Log in to your BRICS instance, you will be prompted with an E-signature page.

**NOTE: Submission of your E-Signature is required to access your BRICS instance.**

### Electronic Signature

The system uses electronic documentation which may require you to provide an electronic signature when you enter, submit, change, access, download, or audit electronic data records.

**ELECTRONIC SIGNATURE.** This Acknowledgement and Certification of Understanding ("Acknowledgement") is to inform you that by submitting an electronic signature, you are providing an electronic mark that is held to the same standard as a legally binding equivalent of a handwritten signature provided by you. For purposes of the acknowledgement, a digital mark is considered your legally typed First and Last Name (legal name may include middle name, initial or suffix). A date will be recorded with both entries. Any part of the system requiring an electronic signature may contain a signature acknowledgment statement provided in the same area requiring the electronic signature.

**AGREEMENT:** By signing this Acknowledgement, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding. I also understand that it is a violation for any individual to sign/e-sign any transactions that occur within system on behalf of me. Any fraudulent activities related to electronic signatures must be immediately reported to the system operations team. Violation of these terms could lead to disciplinary action, up to termination, and prosecution under applicable Federal laws.

**CERTIFICATION OF UNDERSTANDING:** I also understand, acknowledge, agree and certify that:

- I accept my responsibilities in the use of electronic signatures as described on this form.
- My execution of any form of an electronic signature function performed on the system to be the legally binding equivalent of my traditional handwritten signature, and that I am accountable and responsible for actions performed under such an electronic signature.
- I will not share components of my electronic signature such that my signature could be executed by another individual. Such components may include, but are not limited to legal name, passwords or any such identifiers.

First Name\*

Middle Name

Last Name\*

☐ I understand and agree to all of the Terms and Conditions in this electronic documentation for use of Electronic Signature Agreement. Please check the appropriate box to provide your signature.

Submit

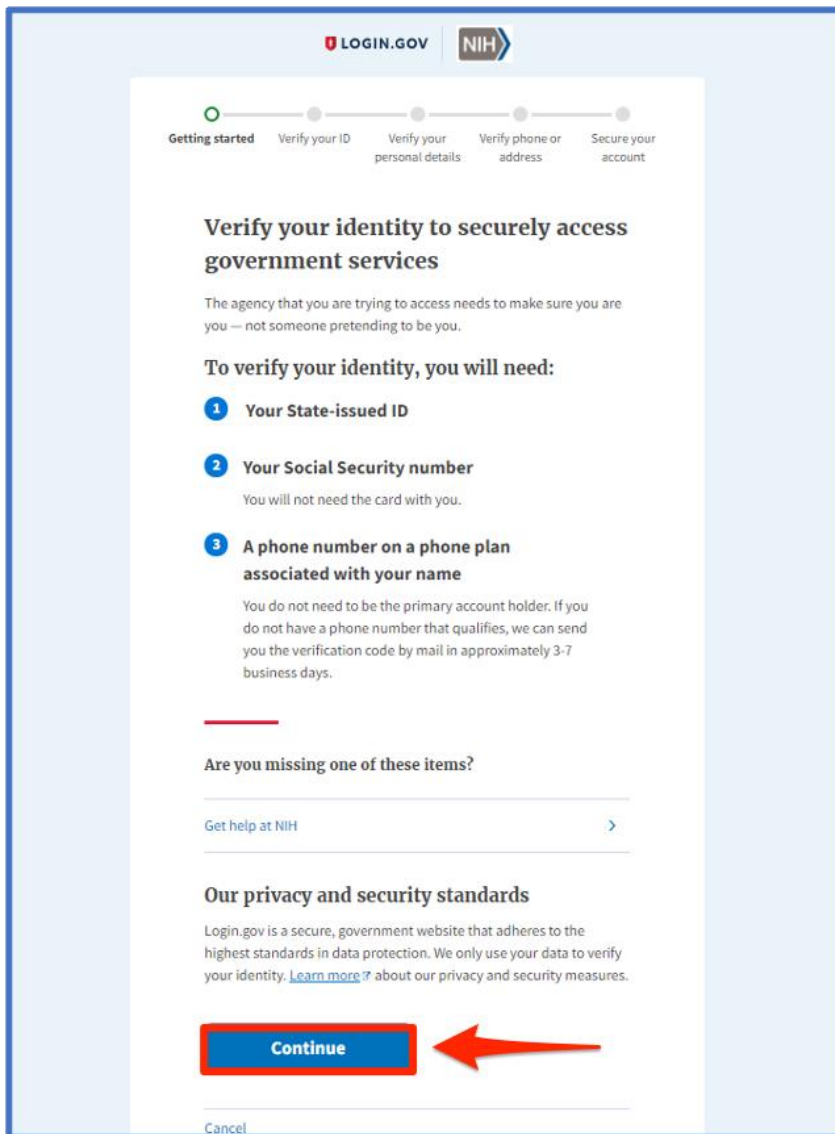


## Login.gov – Identity Assurance Level 2 (IAL2)

BRICS instances now require additional identity proofing so login.gov accounts will need identity assurance level 2.

When user's login to a BRICS instance via Login.gov, they will be prompted to verify their identity with the following requirements:

- a. **Your State-Issued ID.** You can upload a photo by phone or by computer.
- b. **A phone or computer with a camera** to take a photo of yourself (not always required).
- c. **Social Security Number.**
- d. **A phone number on a phone plan that is in your name.**
  - i. **NOTE:** If you do not have a phone plan that is in your name, we can send you the verification code by mail which takes approximately 3-5 days.



LOGIN.GOV NIH

Getting started Verify your ID Verify your personal details Verify phone or address Secure your account

### Verify your identity to securely access government services

The agency that you are trying to access needs to make sure you are you — not someone pretending to be you.

To verify your identity, you will need:

- 1 **Your State-issued ID**
- 2 **Your Social Security number**  
You will not need the card with you.
- 3 **A phone number on a phone plan associated with your name**  
You do not need to be the primary account holder. If you do not have a phone number that qualifies, we can send you the verification code by mail in approximately 3-7 business days.

Are you missing one of these items?

[Get help at NIH](#)



### Our privacy and security standards

Login.gov is a secure, government website that adheres to the highest standards in data protection. We only use your data to verify your identity. [Learn more](#) about our privacy and security measures.

**Continue**

[Cancel](#)

Read the following page and accept by clicking the box to grant permissions and click continue.

**Getting started**
Verify your ID
Verify your personal details
Verify phone or address
Secure your account

## Let's get started

Identity verification happens in two parts:

### Verify your identity

We'll ask for your personal information. We'll use, keep and share some of your personal information to verify your identity against public records.

### Secure your account

After you verify, we'll ask you to encrypt your account. Encryption means your data is protected and only you, the account holder, will be able to access or change your information.

☐ By checking this box, you are letting Login.gov ask for, use, keep, and share your personal information. We will only use it to verify your identity. [Learn more](#)

Continue

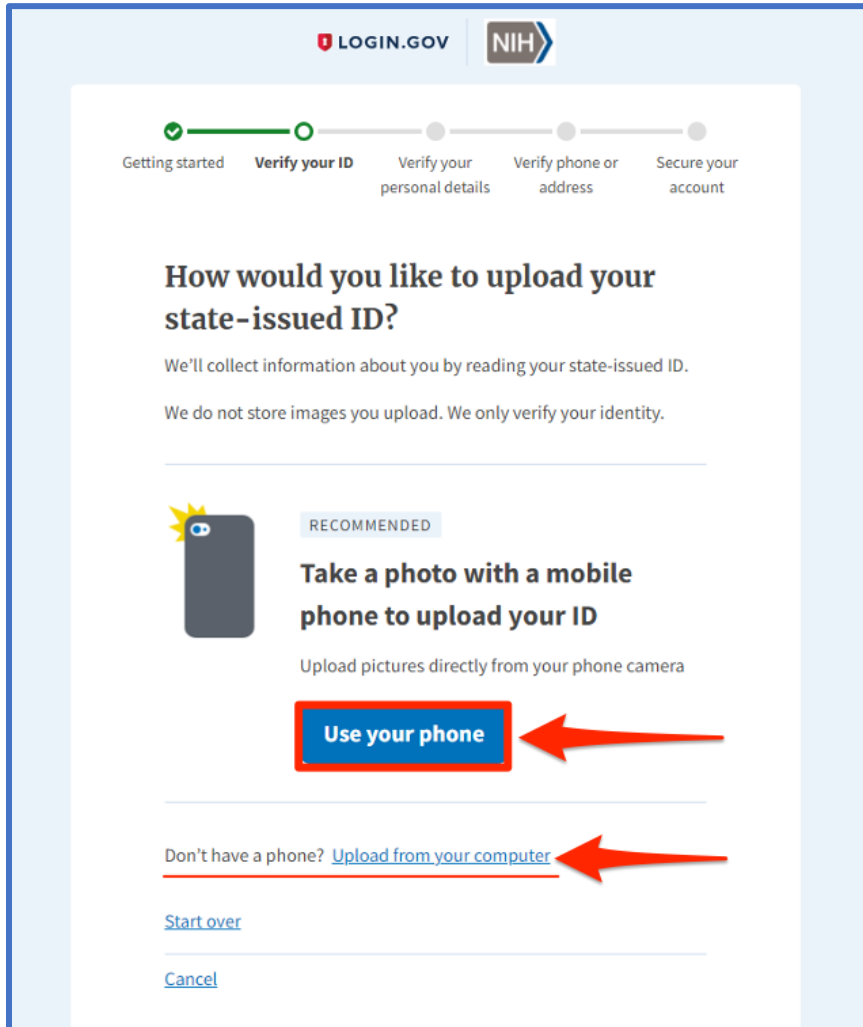
Cancel

### 3.1 Verifying state-issued ID

Users are required to upload their state issue ID. Users can upload a photo of their state issued ID on either their phone or by uploading the photo from their computer (a front and back photo are required).

**Users uploading by their phone can follow these steps:**

1. Click Use your phone.




LOGIN.GOV NIH

Getting started **Verify your ID** Verify your personal details Verify phone or address Secure your account

### How would you like to upload your state-issued ID?

We'll collect information about you by reading your state-issued ID.  
We do not store images you upload. We only verify your identity.

 **RECOMMENDED**

**Take a photo with a mobile phone to upload your ID**

Upload pictures directly from your phone camera

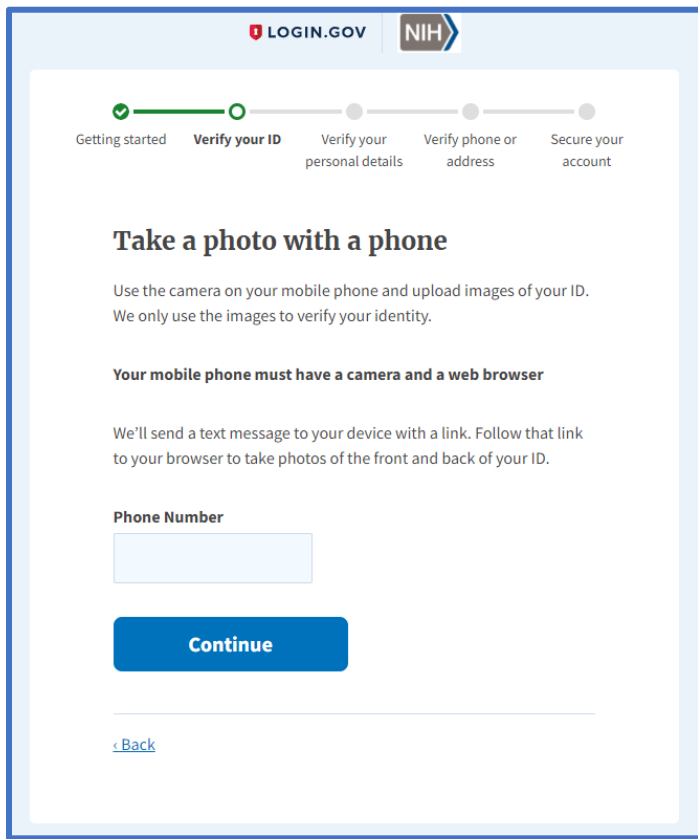
**Use your phone**



Don't have a phone? [Upload from your computer](#)

[Start over](#)

[Cancel](#)

2. Enter the phone number of the phone you wish to use.



Getting started **Verify your ID** Verify your personal details Verify phone or address Secure your account

### Take a photo with a phone

Use the camera on your mobile phone and upload images of your ID. We only use the images to verify your identity.

**Your mobile phone must have a camera and a web browser**

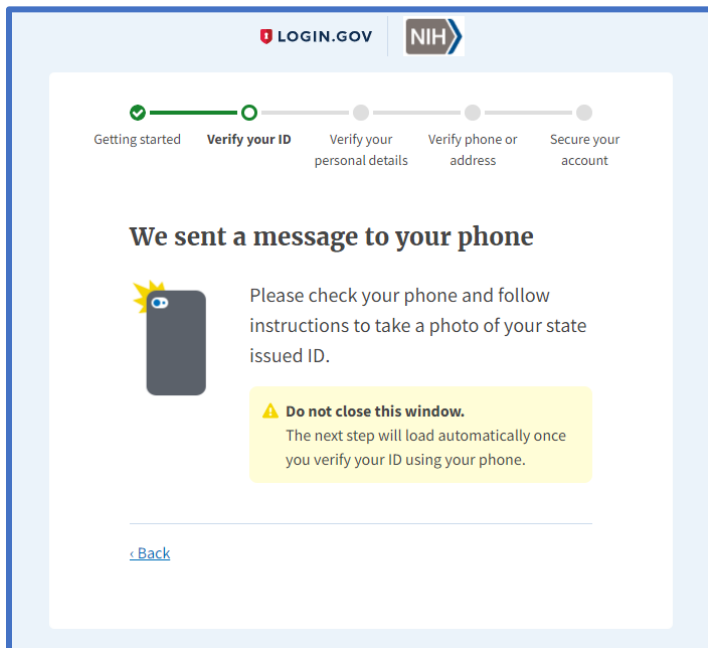
We'll send a text message to your device with a link. Follow that link to your browser to take photos of the front and back of your ID.



**Phone Number**

**Continue**

[Back](#)


3. You will get a confirmation message, **do not close the confirmation page**, that a link has been sent to your phone to upload the photos. Open the message on your phone and follow the link in the message.




Getting started **Verify your ID** Verify your personal details Verify phone or address Secure your account

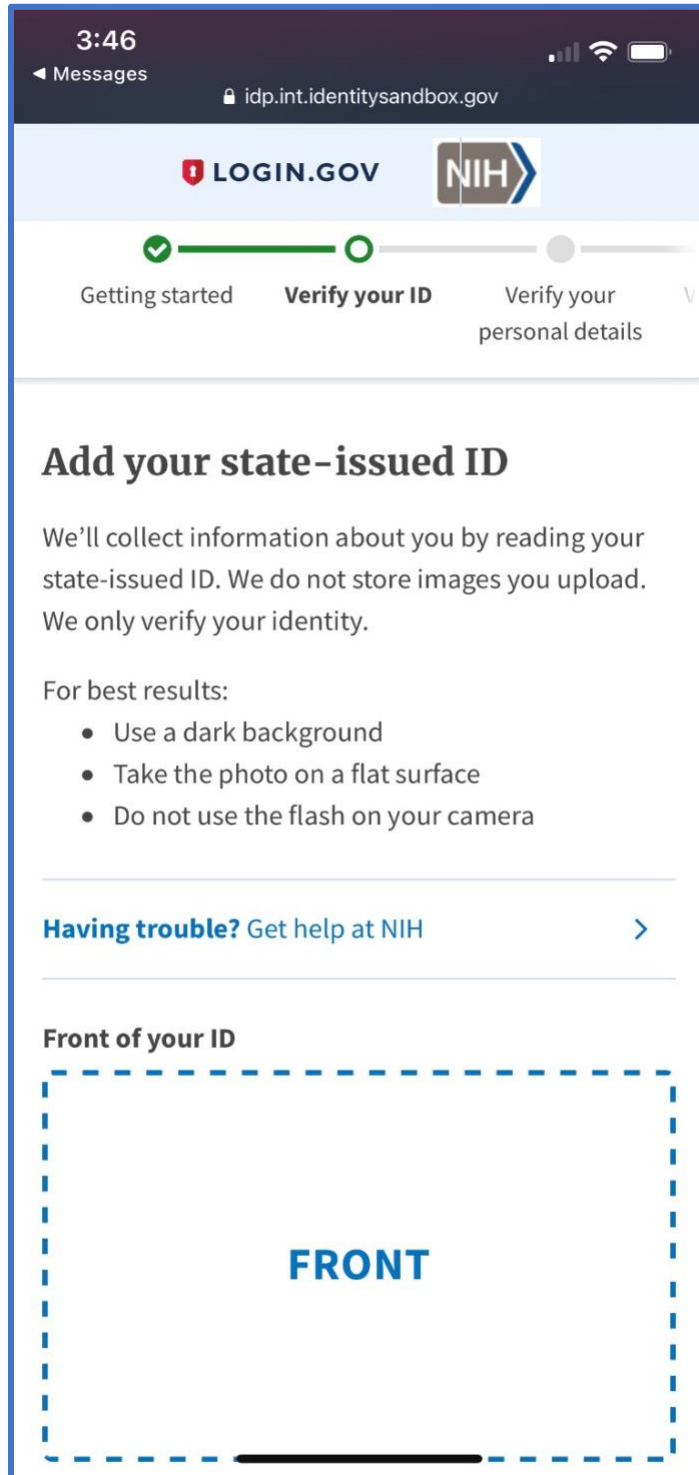
### We sent a message to your phone


 Please check your phone and follow instructions to take a photo of your state issued ID.


**Do not close this window.**  
 The next step will load automatically once you verify your ID using your phone.

[Back](#)

- a. [Mobile screenshot 1/4]: Click **Take photo** for both the front/back of the ID or upload a photo of the front/back.



3:46  
Messages  
idp.int.identitysandbox.gov

**FRONT**

[Take photo](#) or [Upload photo](#)

Back of your ID


**BACK**

[Take photo](#) or [Upload photo](#)

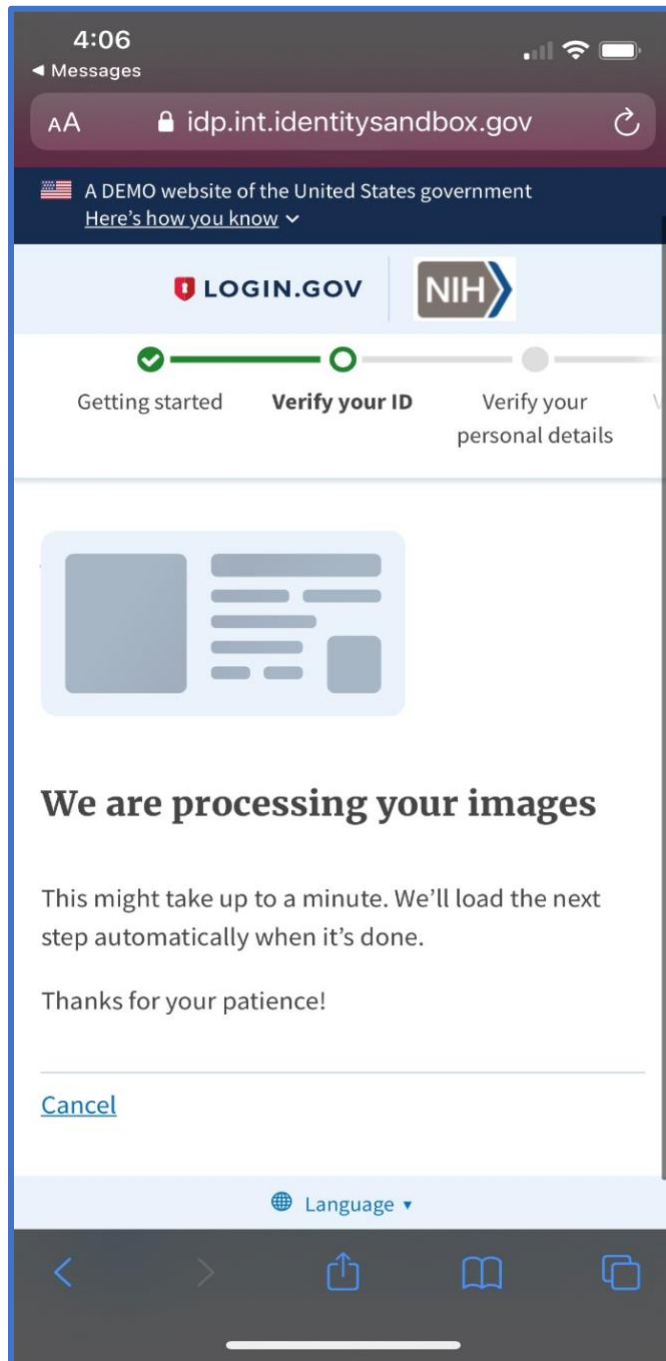
**Submit**

[Cancel](#)

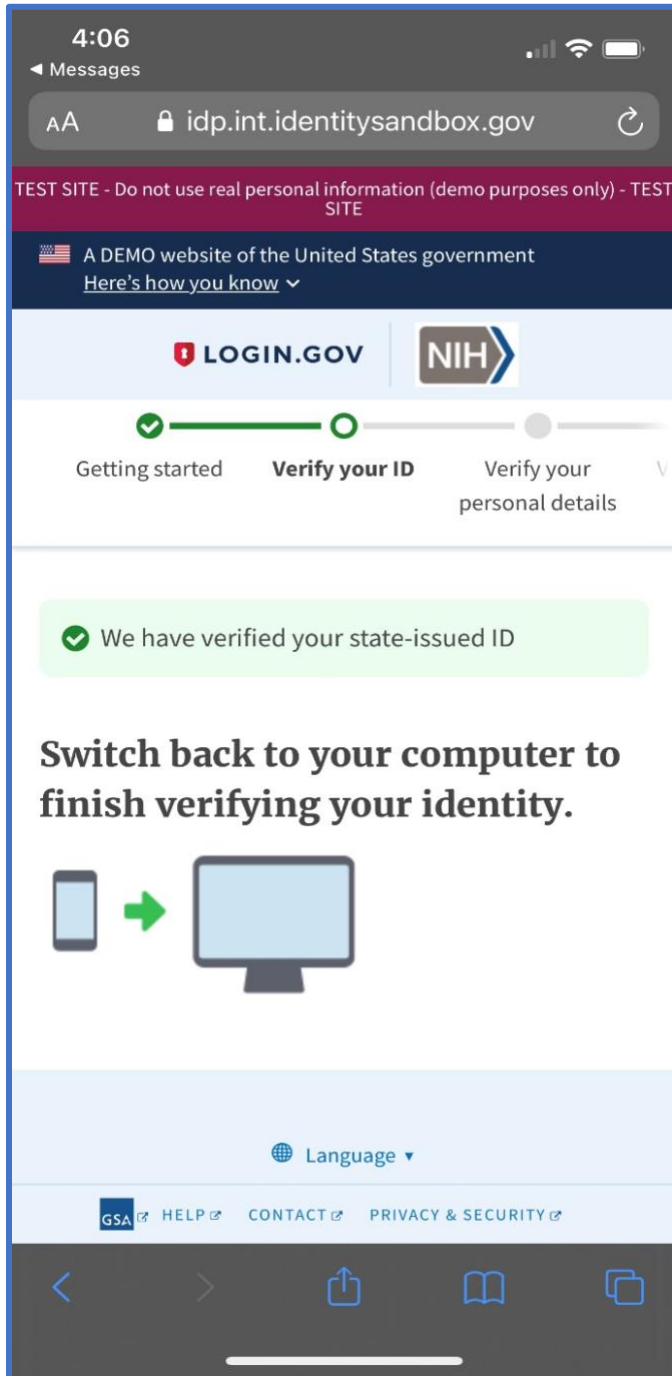
Language ▼

 [HELP](#) [CONTACT](#) [PRIVACY & SECURITY](#)

- b. [Mobile Screenshot 3/4] Do not close this page. The images are being verified and will automatically load the next step after it has processed.



- c. [Mobile screenshot 4/4] Your state issue ID has been verified. Switch back to your computer to continue the verification process.

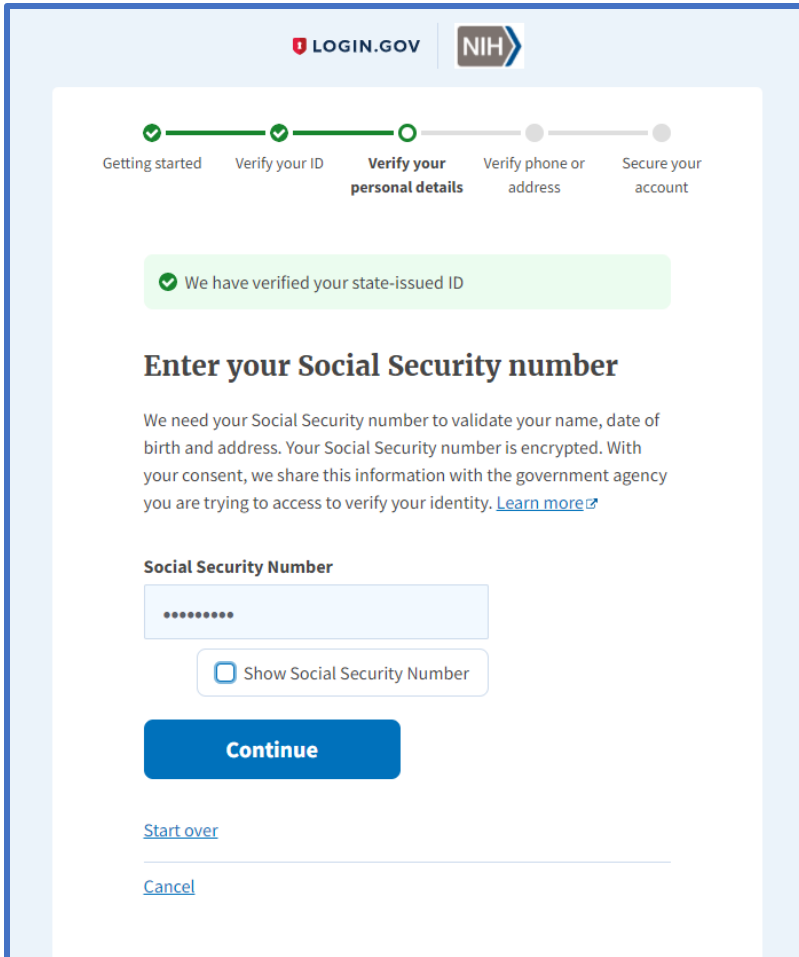




## 3.2 Verifying personal details

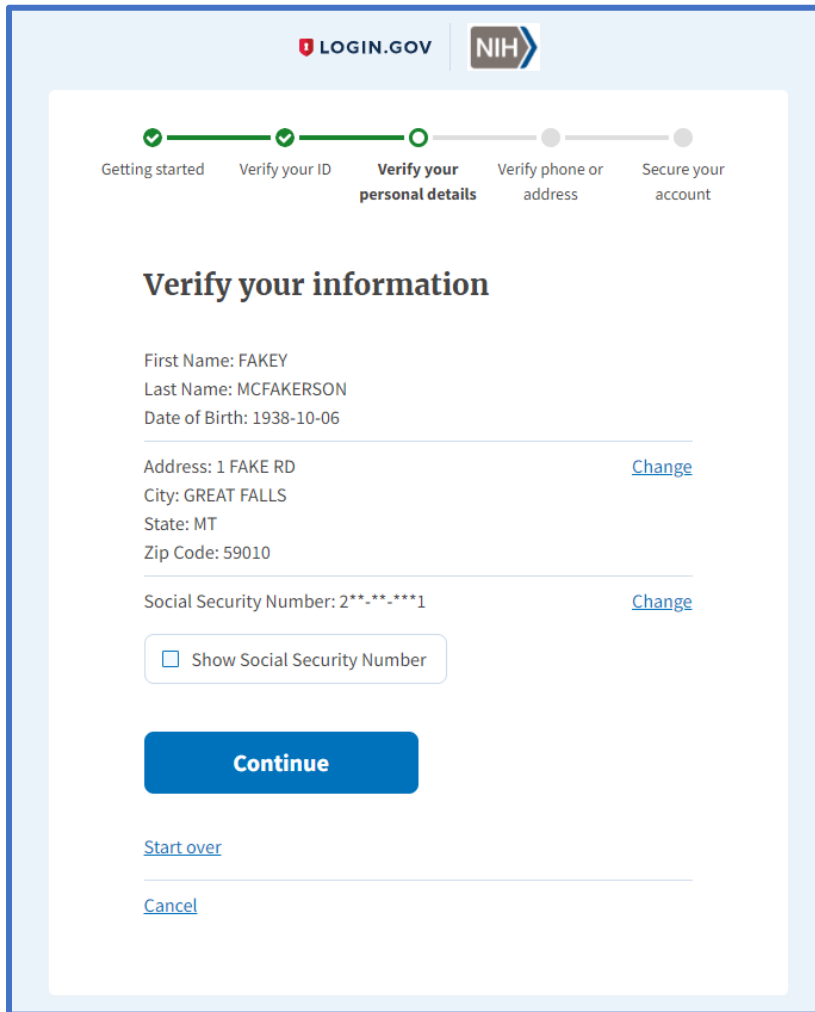
After verifying the state issue ID, the next page will load to verify the user's personal details.

1. Enter your social security number and click continue.



The screenshot shows the NIH LOGIN.GOV verification interface. At the top, there are logos for LOGIN.GOV and NIH. Below the logos is a progress bar with five steps: 'Getting started' (completed), 'Verify your ID' (completed), 'Verify your personal details' (current step), 'Verify phone or address' (pending), and 'Secure your account' (pending). The current step, 'Verify your personal details', is highlighted. Below the progress bar, a green checkmark icon and the text 'We have verified your state-issued ID' are displayed. The main heading is 'Enter your Social Security number'. Below this, a paragraph explains that the Social Security number is needed to validate the user's name, date of birth, and address, and that it is encrypted. A link to 'Learn more' is provided. Below the text, there is a label 'Social Security Number' followed by a text input field containing seven dots. To the right of the input field is a checkbox labeled 'Show Social Security Number'. Below the input field and checkbox is a blue 'Continue' button. At the bottom of the form, there are two links: 'Start over' and 'Cancel'.

2. A page showing your personal details will display. Verify your information and click continue.



**LOGIN.GOV** **NIH**

Getting started **Verify your ID** **Verify your personal details** Verify phone or address Secure your account

## Verify your information

First Name: FAKEY  
Last Name: MCFAKERSON  
Date of Birth: 1938-10-06

Address: 1 FAKE RD [Change](#)  
City: GREAT FALLS  
State: MT  
Zip Code: 59010

Social Security Number: 2\*\*-\*\*-\*\*\*\*1 [Change](#)

☐ Show Social Security Number

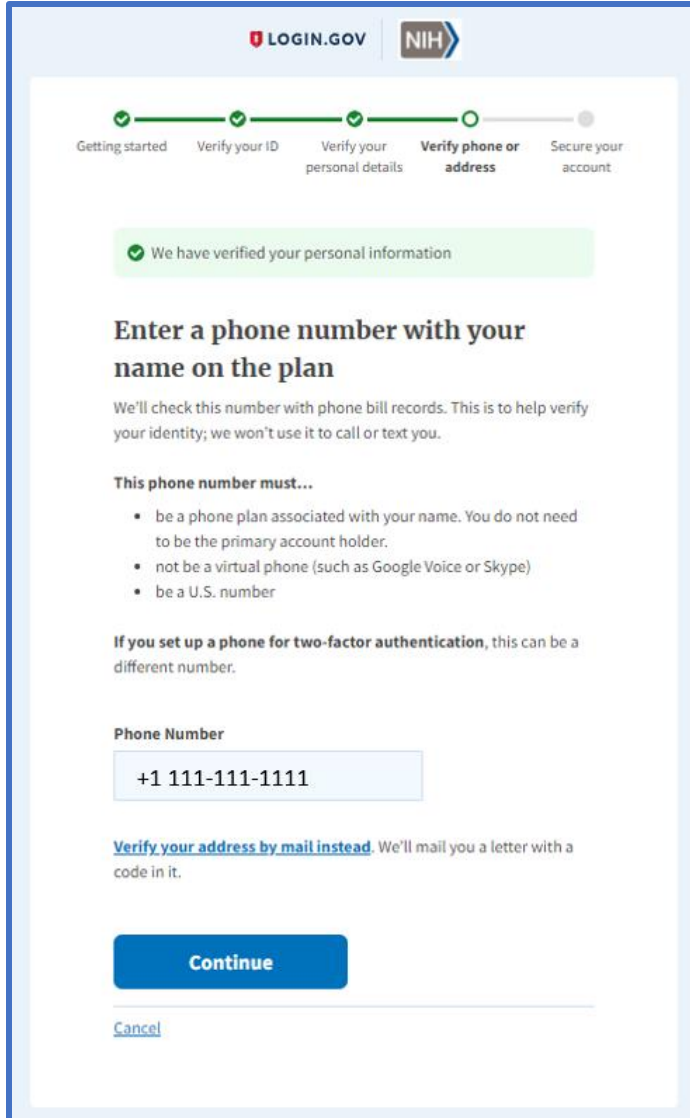
**Continue**



[Start over](#)

[Cancel](#)


### 3.3 Verifying phone or address

1. The user is required to enter a phone number that has them on the plan. If the user does not have a phone number that their name is associated with then they can click, **Verify your address by mail Instead**. Otherwise, please enter your phone number and click continue.



Getting started    Verify your ID    Verify your personal details    **Verify phone or address**    Secure your account

 We have verified your personal information

### Enter a phone number with your name on the plan

We'll check this number with phone bill records. This is to help verify your identity; we won't use it to call or text you.

**This phone number must...**

- be a phone plan associated with your name. You do not need to be the primary account holder.
- not be a virtual phone (such as Google Voice or Skype)
- be a U.S. number

If you set up a phone for two-factor authentication, this can be a different number.

**Phone Number**

+1 111-111-1111

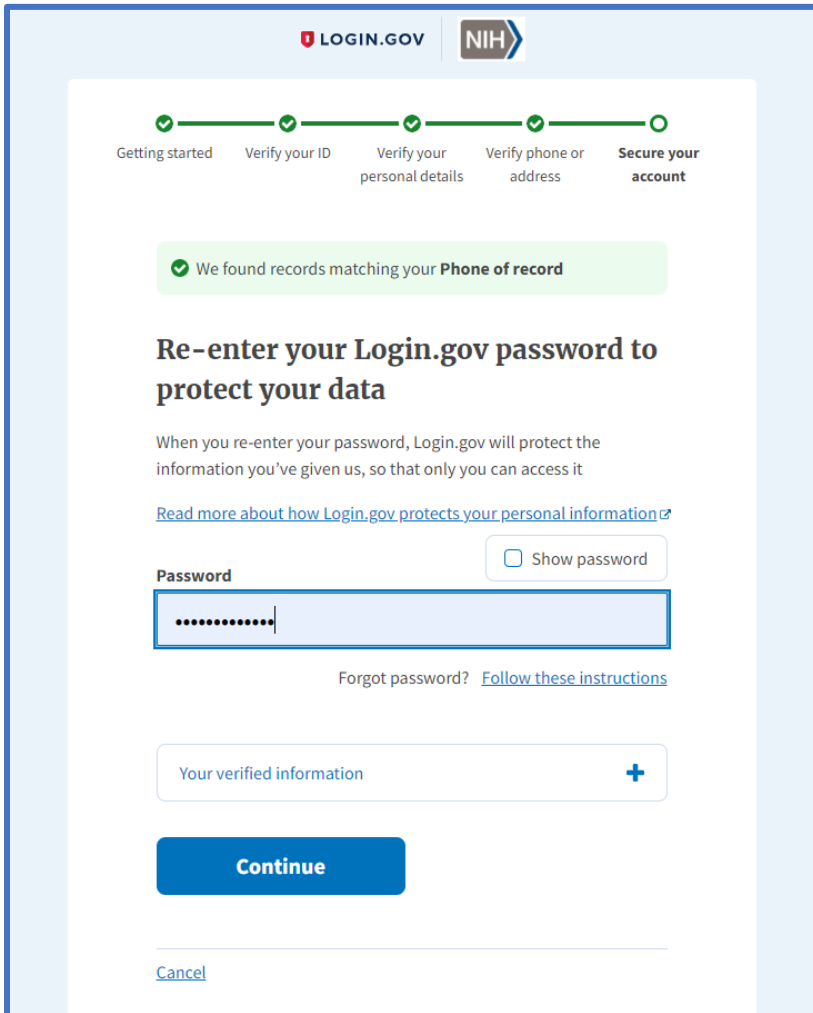
[Verify your address by mail instead](#). We'll mail you a letter with a code in it.



**Continue**

[Cancel](#)


## 3.4 Secure your account

1. User will be prompted to enter their login.gov password to save their verified information.



Getting started    Verify your ID    Verify your personal details    Verify phone or address    **Secure your account**

 We found records matching your **Phone of record**


**Re-enter your Login.gov password to protect your data**

When you re-enter your password, Login.gov will protect the information you've given us, so that only you can access it

[Read more about how Login.gov protects your personal information](#)

Password  ☐ Show password

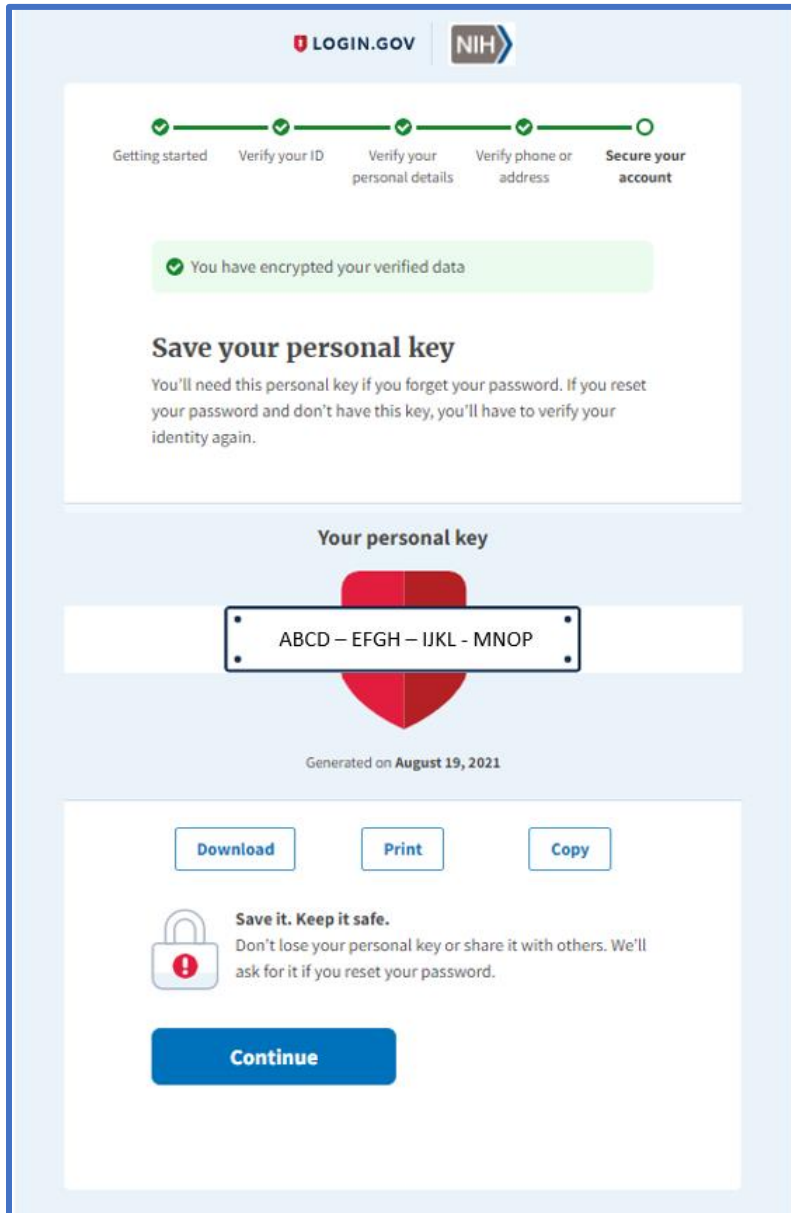
Forgot password? [Follow these instructions](#)

Your verified information 

**Continue**

[Cancel](#)

2. On the next screen you will get a **personal key**. **This personal key should be saved and kept somewhere safe.** It will be needed if the user needs to reset their password. If the user does not have their personal key when resetting their password, they will have to verify their information again. **Users will need this personal key on the next step.**



LOGIN.GOV NIH

Getting started Verify your ID Verify your personal details Verify phone or address **Secure your account**

✓ You have encrypted your verified data

### Save your personal key


You'll need this personal key if you forget your password. If you reset your password and don't have this key, you'll have to verify your identity again.

#### Your personal key

ABCD – EFGH – IJKL – MNOP

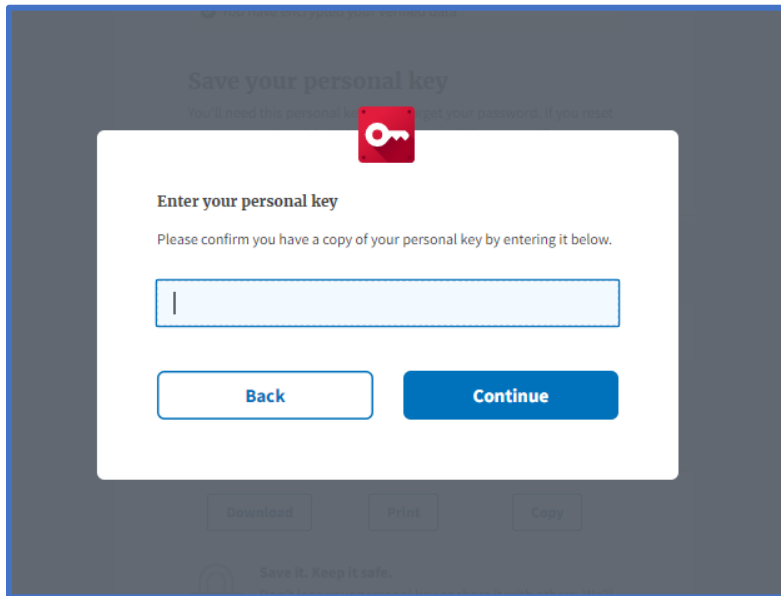
Generated on August 19, 2021

Download Print Copy

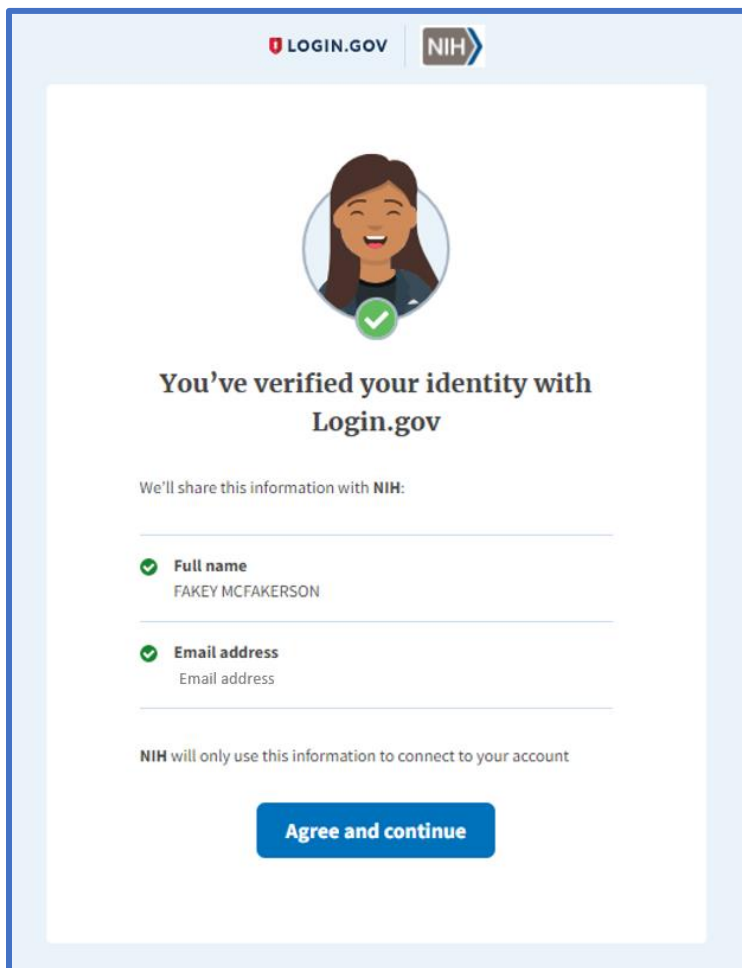
 **Save it. Keep it safe.**  
Don't lose your personal key or share it with others. We'll ask for it if you reset your password.

**Continue**

3. Enter your personal key.



4. Click **Agree and continue** – this is the last step of the verification process.



## ID.me – Identity Assurance Level 2

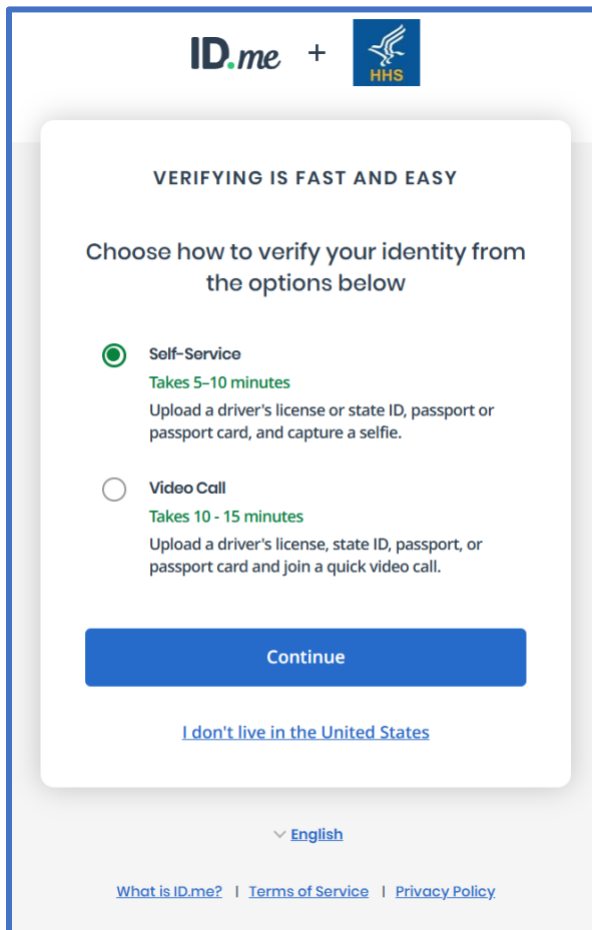
BRICS instances now require additional identity proofing so ID.me accounts will need identity assurance level 2.

When user's login to a BRICS instance via ID.me, they will be prompted to verify their identity with the following requirements:

- a. One of the following: **Driver's license, State ID, Passport, Passport card**
- b. Mobile phone to upload the documents and to provide a selfie with.

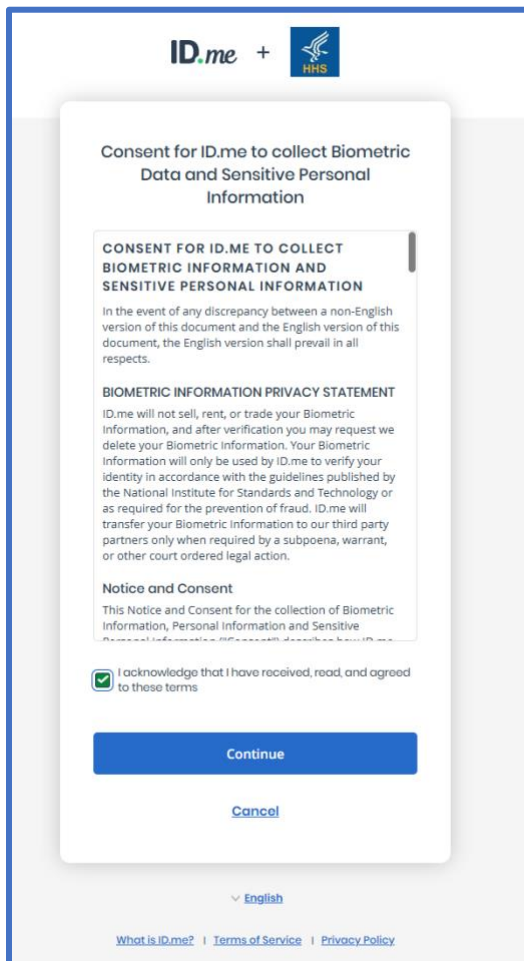
### 4.1 Verifying identification document

1. Click either Self-Service or Video Call to verify your documentation. **In this guide we will be selecting Self-Service.**



The image shows a screenshot of the ID.me verification interface. At the top, there is a header with the ID.me logo and the HHS (Department of Health and Human Services) logo. Below the header, the text "VERIFYING IS FAST AND EASY" is displayed. The main content area prompts the user to "Choose how to verify your identity from the options below". There are two options: "Self-Service" and "Video Call". The "Self-Service" option is selected, indicated by a green radio button. It states "Takes 5-10 minutes" and "Upload a driver's license or state ID, passport or passport card, and capture a selfie." The "Video Call" option is unselected, indicated by a white radio button. It states "Takes 10 - 15 minutes" and "Upload a driver's license, state ID, passport, or passport card and join a quick video call." Below the options is a blue "Continue" button. At the bottom of the main content area, there is a link that says "I don't live in the United States". Below the main content area, there is a language selector showing "English" with a dropdown arrow. At the very bottom, there are links for "What is ID.me?", "Terms of Service", and "Privacy Policy".

- Users will need to consent for ID.me to collect personal data.



The image shows a mobile app interface for ID.me, featuring the NHS logo. The screen displays a consent form titled "Consent for ID.me to collect Biometric Data and Sensitive Personal Information". The form includes a scrollable section with the following text:

**CONSENT FOR ID.ME TO COLLECT BIOMETRIC INFORMATION AND SENSITIVE PERSONAL INFORMATION**

In the event of any discrepancy between a non-English version of this document and the English version of this document, the English version shall prevail in all respects.

**BIOMETRIC INFORMATION PRIVACY STATEMENT**

ID.me will not sell, rent, or trade your Biometric Information, and after verification you may request we delete your Biometric Information. Your Biometric Information will only be used by ID.me to verify your identity in accordance with the guidelines published by the National Institute for Standards and Technology or as required for the prevention of fraud. ID.me will transfer your Biometric Information to our third party partners only when required by a subpoena, warrant, or other court ordered legal action.

**Notice and Consent**

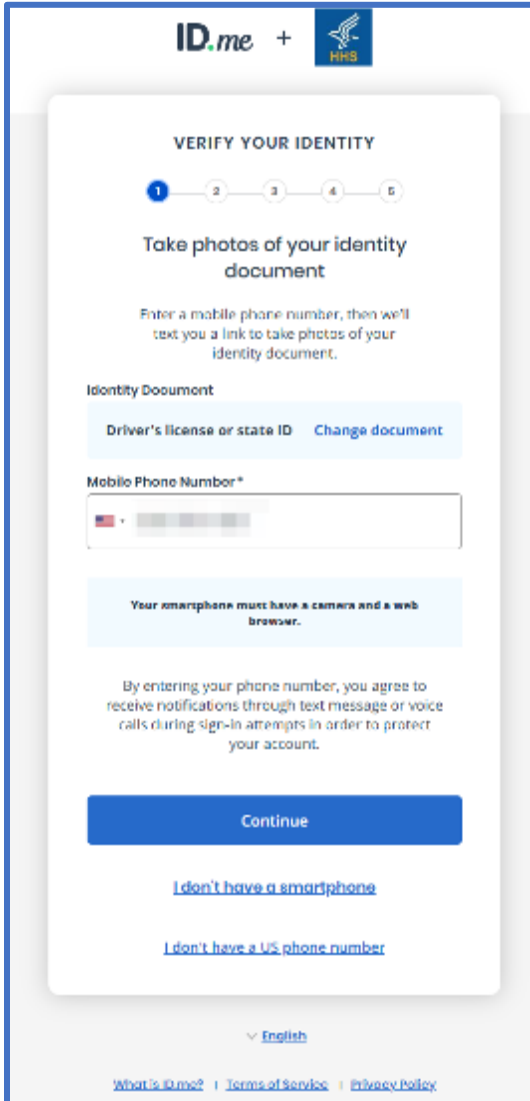
This Notice and Consent for the collection of Biometric Information, Personal Information and Sensitive Personal Information.

☒ I acknowledge that I have received, read, and agreed to these terms

Below the form are two buttons: a blue "Continue" button and a blue "Cancel" link. At the bottom of the screen, there is a language selector set to "English" and a footer with links for "What is ID.me?", "Terms of Service", and "Privacy Policy".



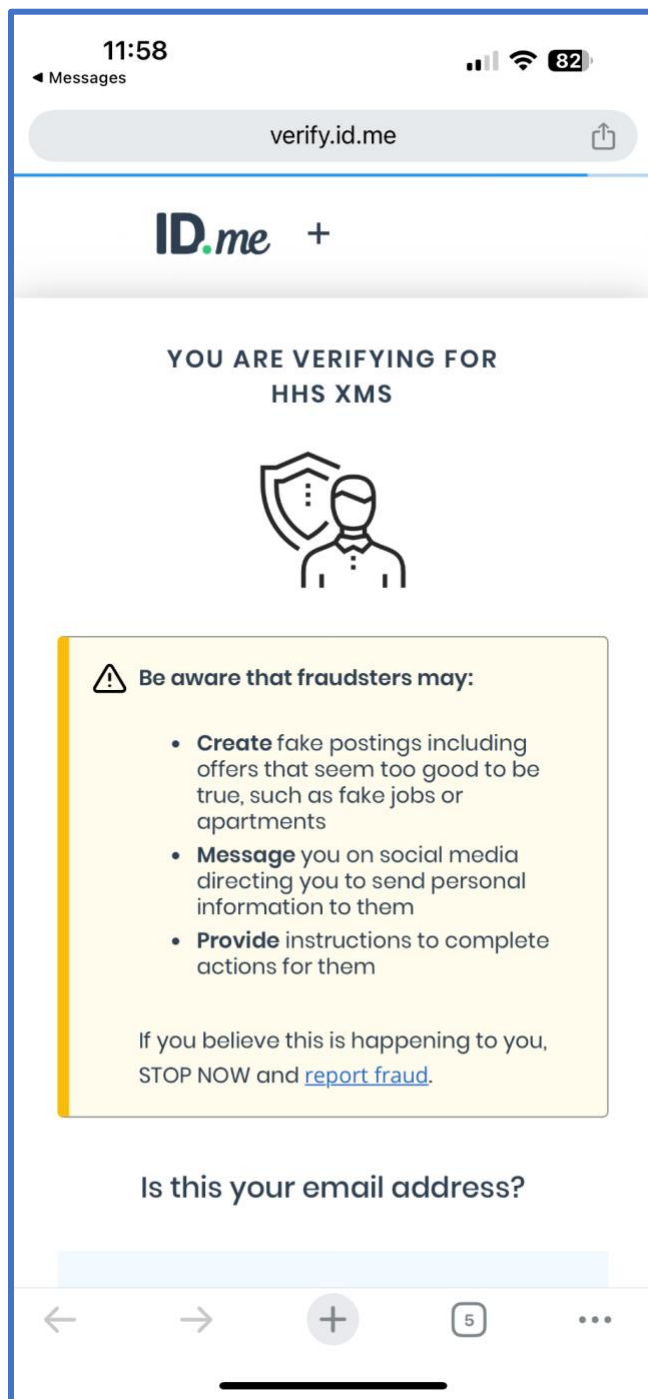
- Choose the identification document that will be uploaded and enter a phone number to receive a link to upload the relevant document(s).



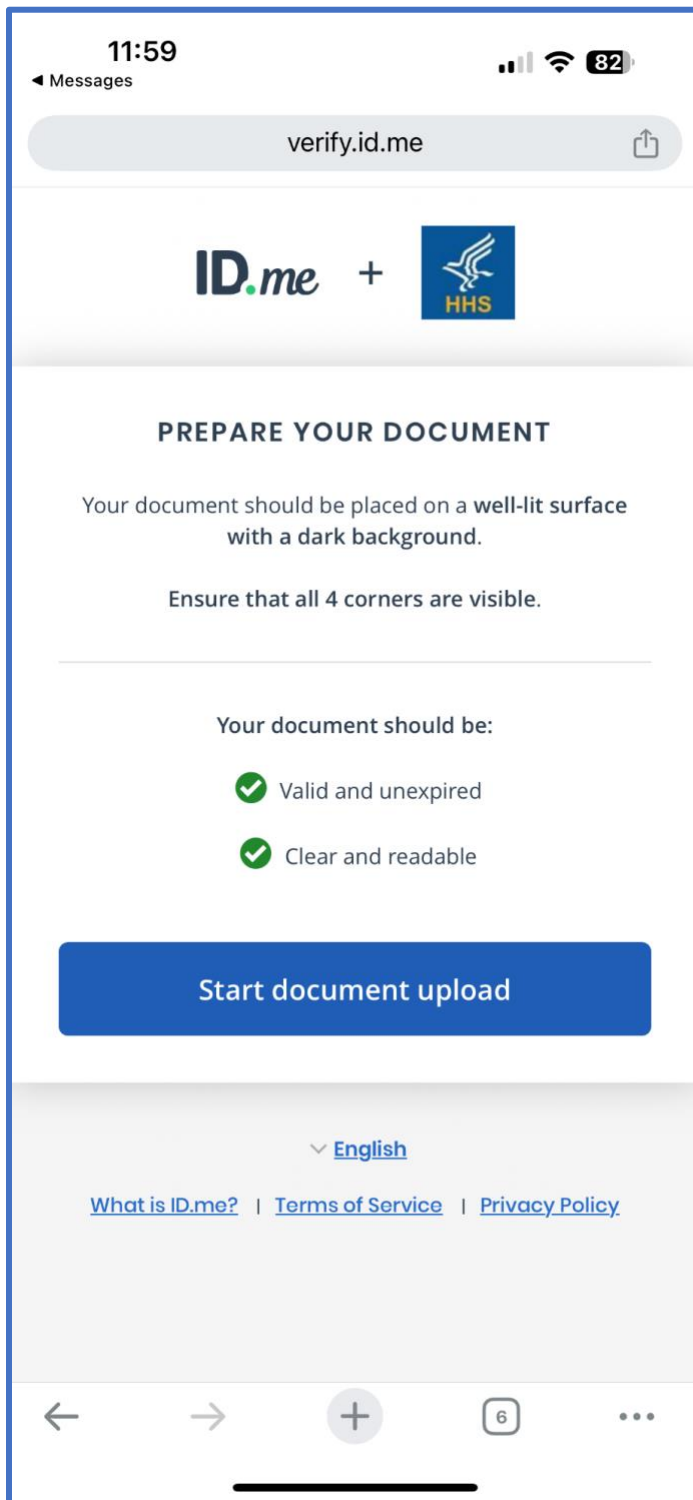
- [Mobile image 1/7] Check the messages on the phone that was entered in the previous step and open the link received.

This message is from [ID.me](#). Your identity is being used to log in to HHS XMS. Please click this link to upload a picture or to report unauthorized use of your identity: <https://verify.id.me/en/phones/c3615f7af6384b6eb03a7fbef43c8b28/authorize?vfp=wZ52kaAU>

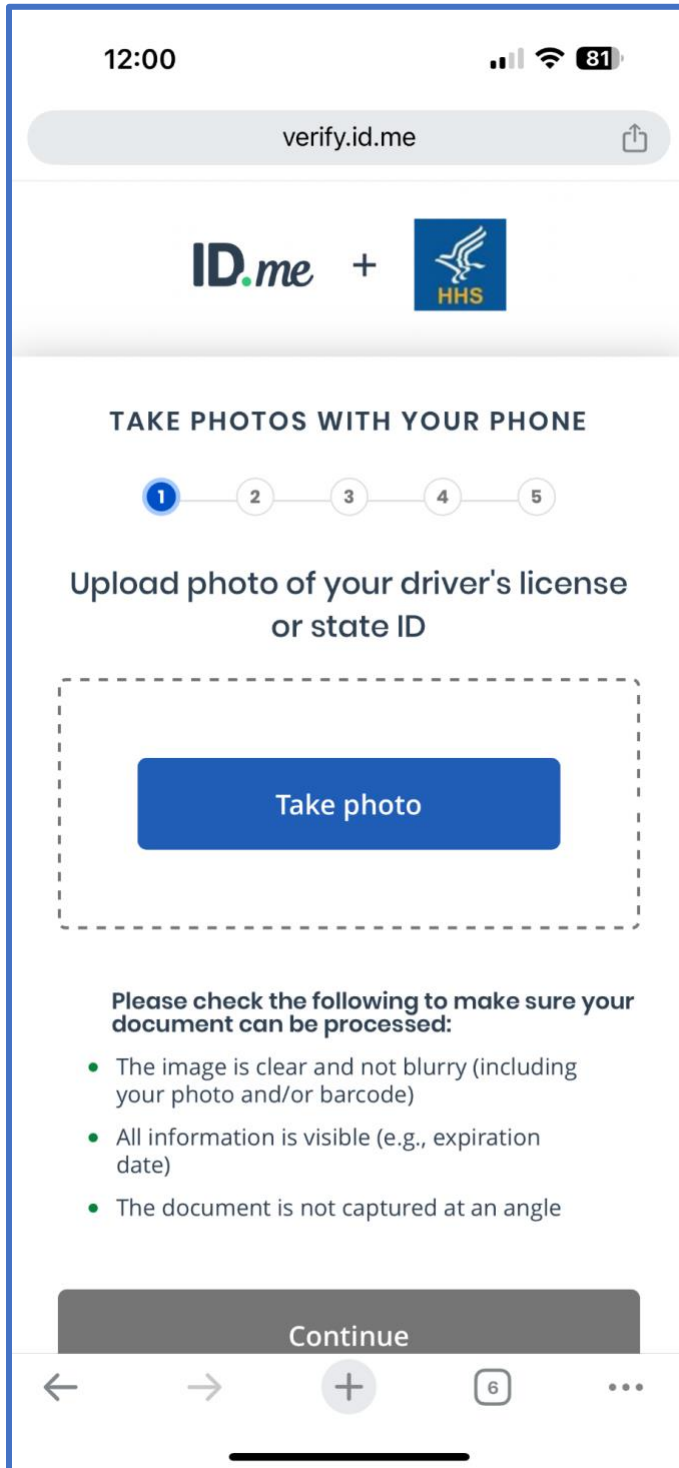
5. [Mobile image 2/7] Verify your email address



6. [Mobile image 3/7] Select start document upload




7. [Mobile image 4/7] Follow through the steps to take photos of both the front and back. Then fill in the contact details and submit.



12:00 📶 81%

verify.id.me

**ID.me** + 

**TAKE PHOTOS WITH YOUR PHONE**

1 — 2 — 3 — 4 — 5

Upload photo of your driver's license  
or state ID

**Take photo**

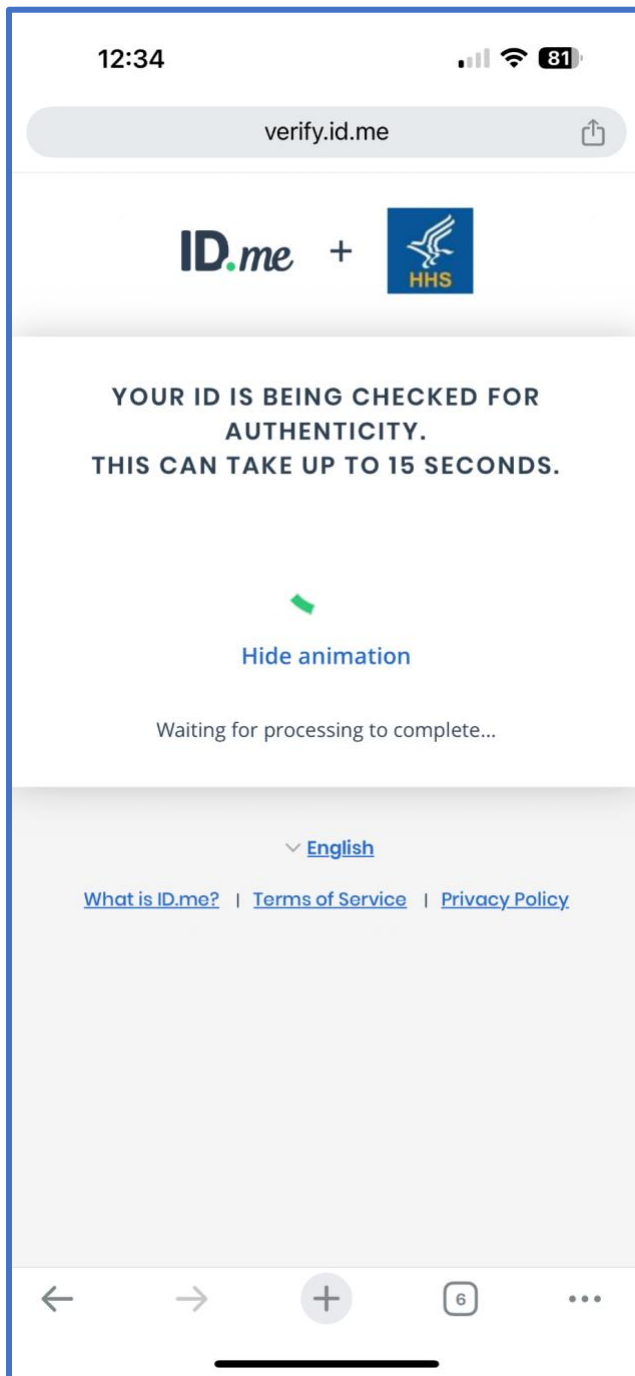
**Please check the following to make sure your document can be processed:**

- The image is clear and not blurry (including your photo and/or barcode)
- All information is visible (e.g., expiration date)
- The document is not captured at an angle

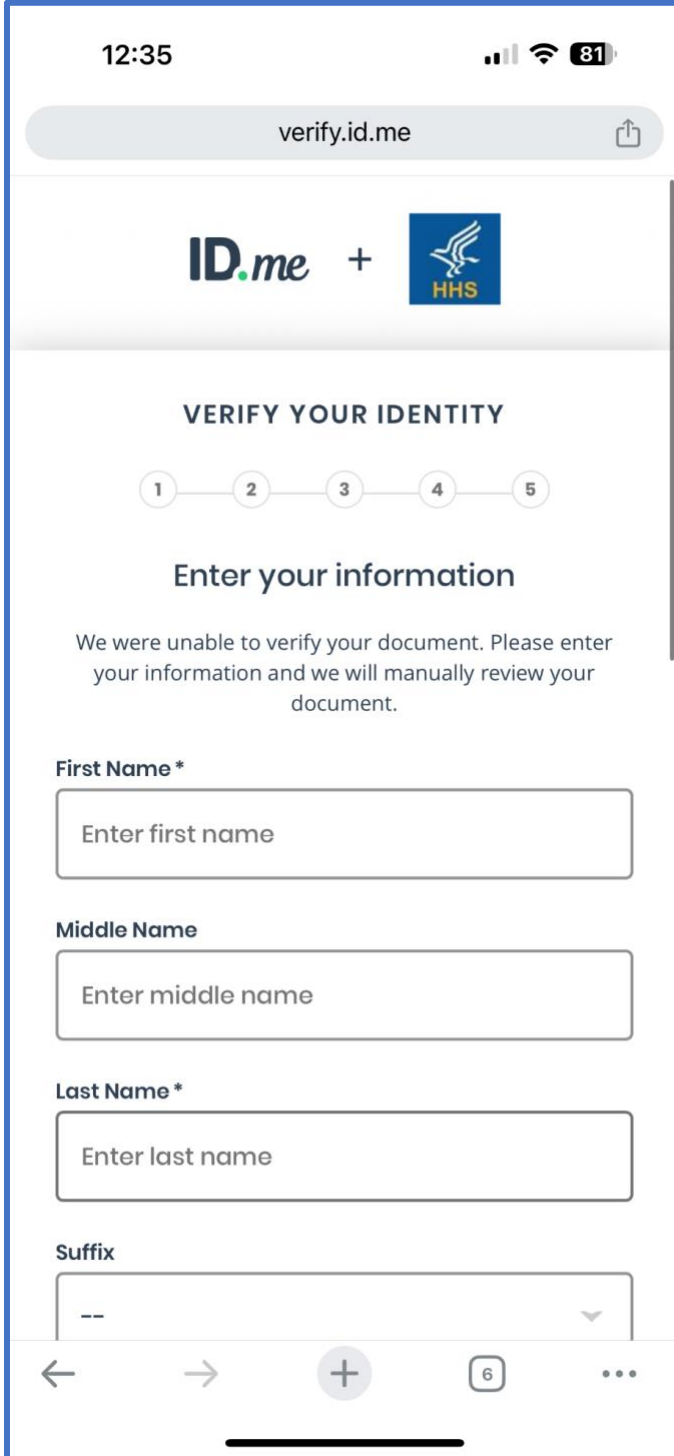
**Continue**

← → + 6 ...

8. [Mobile image 5/7] There will be a short processing screen.




9. [Mobile image 6/7] If the document was unable to be verified automatically, users will be taken to enter in all of their information for manual verification.



12:35 📶 81%

verify.id.me 🔗

**ID.me** + 

**VERIFY YOUR IDENTITY**

1 — 2 — 3 — 4 — 5

**Enter your information**

We were unable to verify your document. Please enter your information and we will manually review your document.

**First Name \***

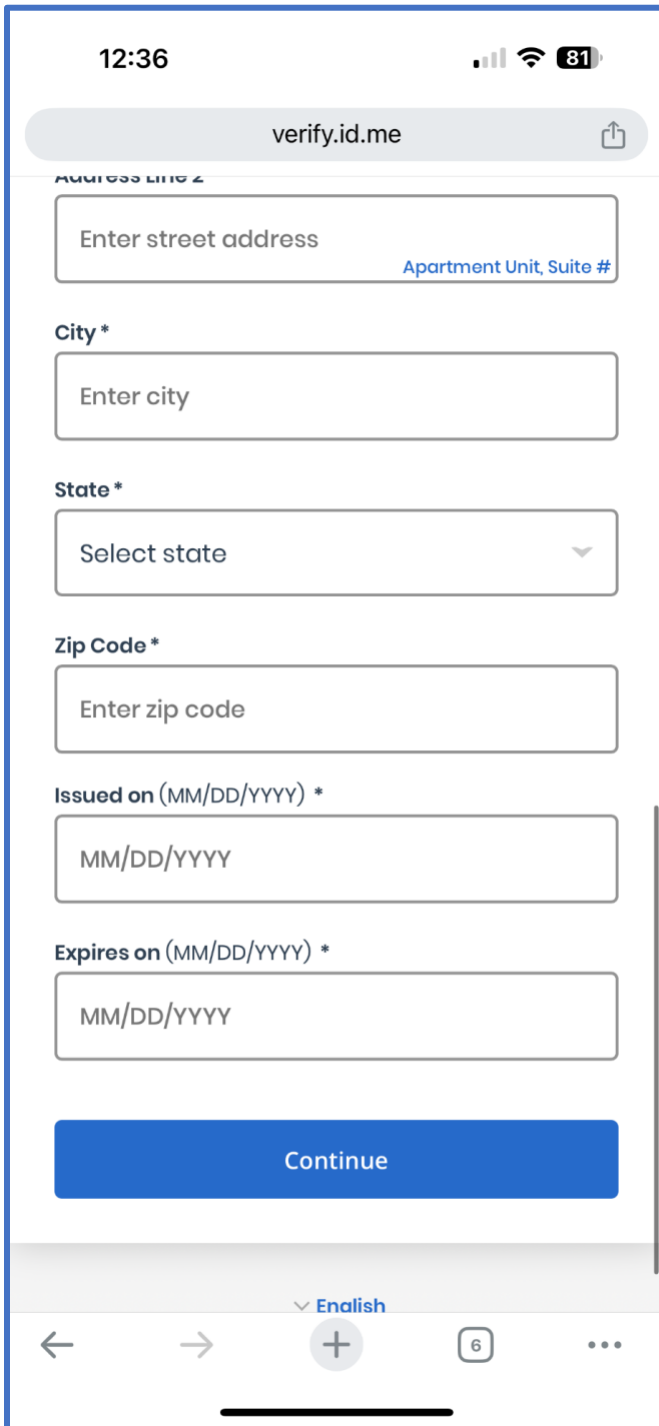
**Middle Name**

**Last Name \***

**Suffix**

← → + 6 ...

10. [Mobile image 7/7] After entering all the relevant information press continue.



12:36 81

verify.id.me

Address Line 2

Enter street address Apartment Unit, Suite #

City \*

Enter city

State \*

Select state

Zip Code \*

Enter zip code

Issued on (MM/DD/YYYY) \*

MM/DD/YYYY

Expires on (MM/DD/YYYY) \*

MM/DD/YYYY

Continue

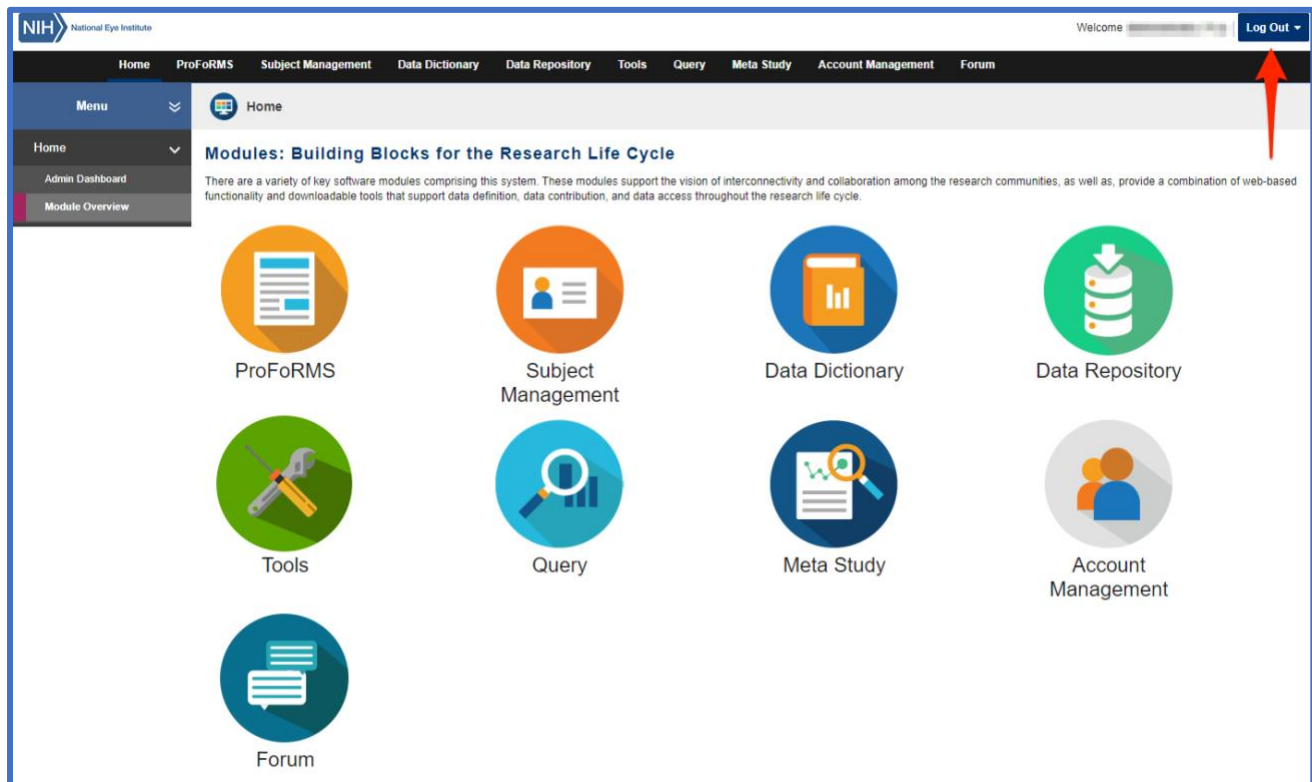
English

11. Once the details have been entered and has been successfully reviewed and verification is complete then the user's account is now IAL2 and will be able to access their BRICS instance.

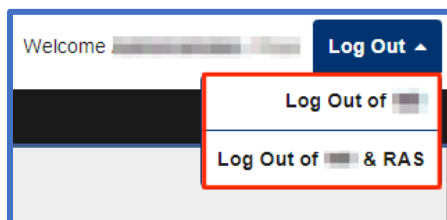
## Other Changes

### 5.1 Logging out of your BRICS account and/or your RAS account.

1. When logged into your BRICS account, you will see a logout dropdown at the top left beside your username.



2. Should you wish to stay logged into other applications using RAS you may choose to only log out of your BRICS instance. If you wish to logout of all RAS applications you are currently signed into, select **Log out of [Your BRICS Instance] & RAS**.



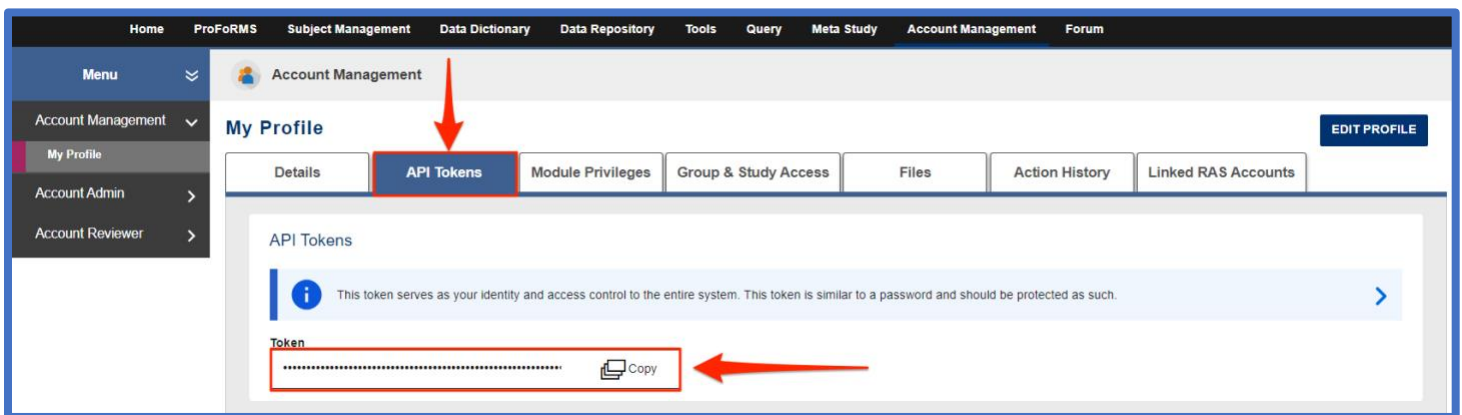


## 5.2 API token

The API token serves as your identity and access control to the entire system. This token is like a password and should be protected as such. The token updates every ~30 minutes minimum, on every login, and every session update.

Previously the API token was retrieved by making a request to `/auth/login` with the user's username/password. However, this has now changed:

For users to retrieve/refresh the API token, they will need to log into BRICS and navigate to the Account Management module. The "My Profile" page will load, and then select the 'API tokens' tab and your token is accessible there.



## Contacts and Links

1. **Help with RAS log in credential issues:**
  - a. Link to Login.gov password recovery: <https://secure.login.gov/users/password/new>
  - b. Link for NIH PIV card issues: <https://auth.nih.gov/CertAuthV3/forms/mfa/Help.html>
  - c. Link for ID.me issues: <https://help.id.me/hc/en-us>
2. **General Information on NIH Researcher Auth Service:** <https://datascience.nih.gov/researcher-auth-service-initiative>