Frequently Asked Questions for Signing Into Research.gov

(Revised November 22, 2024)

Multifactor Authentication

1. What is multifactor authentication?

Multifactor authentication (MFA) is a layered security measure that requires two or more authentication methods (e.g., authentication application, fingerprint, or security key) to verify a user's identity. See *More than a Password: Protect Yourself from Malicious Hackers with Multifactor Authentication* published by the Cybersecurity & Infrastructure Security Agency.

2. Why is NSF implementing MFA for Research.gov?

In today's environment with the growing number and increasing sophistication of cyber threats, accessing systems with just a password is no longer enough. NSF implemented MFA for Research.gov on October 27, 2024, as part of an ongoing commitment to enhancing security and safeguarding NSF's IT systems, user accounts, personal and scientific data, and the integrity of the merit review process. This extra step protects both the research community and NSF by helping to ensure that only authorized users can access Federal resources online. See Dear Colleague Letter (NSF 25-011).

3. Is MFA required each time I sign into Research.gov?

Yes, users are required to use MFA each time they sign into Research.gov.

4. *NEW* Is there a cost to enroll in MFA through Research.gov?

No, NSF does not charge users to enroll in MFA to sign into Research.gov. Users are cautioned not to attempt to enroll in MFA with a generic QR scanning app, as these apps may divert users to webpages with payment walls not associated with NSF.

5. *NEW* How do I sign into Research.gov?

Users can sign into Research.gov with NSF credentials (NSF ID / Primary Email Address + Password + MFA method), organization-issued credentials (InCommon Federation organizations only), or Login.gov credentials.

6. **Where do I enroll in MFA to sign into Research.gov?**
    - If you sign in with your NSF credentials, your MFA enrollment is in Research.gov.
    - If you sign in with your organization-issued credentials through InCommon, your MFA enrollment is with your organization.
    - If you sign in with your Login.gov credentials, your MFA enrollment is through Login.gov. See https://www.login.gov/help/get-started/authentication-methods/.

7. **Why should I set up a secondary MFA method?**

    All users must set up a primary MFA method to sign into Research.gov. NSF urges users to also set up a secondary MFA method in case their primary MFA method is unavailable (e.g., user does not have their mobile phone with them).

8. **What's the difference between standard MFA and phishing-resistant MFA?**

    While standard MFA adds an extra layer of security, phishing-resistant MFA is specifically intended to withstand phishing attacks by using authentication methods such as a fingerprint or a security key that are harder for bad actors to exploit. For this reason, Research.gov users with administrative or financial privileges must use a phishing-resistant MFA method to access Research.gov. New users registering with Research.gov who will be requesting privileged (i.e., administrative or financial) roles must select a phishing-resistant MFA method to ensure access after their role has been approved.

    Although users without an administrative or financial role such as Principal Investigators and Reviewers can use a standard MFA method to sign into Research.gov, NSF strongly encourages all users to use a phishing-resistant MFA method.

9. **Which users must use a phishing resistant MFA method to sign into Research.gov?**

    Users with administrative and financial roles in Research.gov and new users who will be requesting privileged (i.e., administrative or financial) roles must use a phishing-resistant MFA method to sign into Research.gov. If a user has an administrative or financial role and the user is enrolling in MFA in Research.gov, only phishing-resistant MFA methods will display and be available for enrollment. See the MFA Options Overview. The following roles are administrative or financial:

    - Administrator
    - Awardee Preparer
    - Awardee Certifier
    - Awardee Financial Representative
    - Proposed Postdoctoral Fellow
    - Authorized Organizational Representative (AOR)
    - Sponsored Projects Officer (SPO)
    - Foreign Financial Disclosure Report (FFDR) Preparer
    - View Only (View Reports)

10. Which users can use a standard MFA method to sign into Research.gov?

Users with roles in Research.gov that do not have administrative or financial privileges can use a standard MFA method to sign into Research.gov. In addition, users without roles (e.g., newly registered users and reference letter writers) and Education & Training Application (ETAP) participants can use a standard MFA method to sign into Research.gov. However, NSF strongly recommends that all users choose a phishing-resistant MFA. If the user role does not include administrative or financial privileges and the user is enrolling in MFA in Research.gov, both standard and phishing-resistant MFA methods will display and be available for enrollment. See the MFA Options Overview. The following roles do not have administrative or financial privileges:

- Principal Investigator (PI) or co-Principal Investigator (co-PI)
- Other Authorized User (OAU)
- Reviewers (includes *ad hoc* reviewers, panelists, and other meeting participants)
- Graduate Research Fellowship Program (GRFP) Applicant
- GRFP Fellow
- GRFP Coordinating Official (CO)
- GRFP Alternate Coordinating Official (Alt. CO)
- GRFP Financial Official (FO)
- Users without roles including newly registered users, reference letter writers, and Education & Training Application (ETAP) participants

11. What are the phishing-resistant MFA options for signing into Research.gov?

The phishing-resistant MFA options are passkey, PIN *(option not available on Mac computers)*, fingerprint (biometric), facial recognition (biometric) *(option not available on Mac computers)*, and security key. See the MFA Options Overview for information on which users must use a phishing-resistant MFA method to sign into Research.gov. Visit the About Signing Into Research.gov page for additional details as well as how-guides with step-by-step enrollment instructions for each MFA option.

12. What are the standard MFA options for signing into Research.gov?

The standard MFA options are Google Authenticator and Okta Verify. Use of these standard MFA methods requires the user to download and install a free app on a mobile device (i.e., smartphone or tablet) prior to MFA enrollment in Research.gov. The Google Authenticator and Okta Verify apps are available in the Google Play store or Apple store. See the MFA Options Overview for information on which users can use a standard MFA method to sign into Research.gov. Visit the About Signing Into Research.gov page for additional details as well as how-guides and video tutorials with step-by-step enrollment instructions for each MFA option.

13. How do I enroll in standard and phishing-resistant MFA methods in Research.gov?

Visit the About Signing Into Research.gov page for how-guides and video tutorials with step-by-step enrollment instructions for each MFA option. There is also information on devices/equipment and operating system requirements.

14. *NEW* Do I have to change my MFA method if my role in Research.gov changes?

If you previously had a role without administrative or financial privileges (e.g., PI) but you are assigned an administrative or financial role, your standard MFA method will no longer work because your administrative or financial role requires you to use a phishing-resistant MFA to sign into Research.gov. You must re-enroll in a phishing-resistant MFA to sign into Researgh.gov with your NSF credentials (NSF ID/Primary Email Address + Password).

If you are already enrolled in a phishing-resistant MFA method but you no longer have an administrative or financial role in Research.gov, you would not be required to re-enroll in a standard MFA method.

15. Why am I being asked to validate my primary email address when enrolling in an MFA method in Research.gov?

Your primary email address is another form of verification used to ensure you are the NSF account owner. If you are setting up an MFA security method for the first time on your NSF account, you will be prompted to verify your NSF account via your primary email address.

If you no longer have access to your primary email address, you must contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

16. Why am I getting an "Invalid code. Try again" error when I attempt to enter the six-digit code that's in my email?

Please verify the code and try again. If you are still having trouble, please contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

17. *NEW* Why did I receive an email from nsfextloginnoreply@nsf.gov with the subject "New Sign-in Detected for Your NSF Account"?

All users who enroll in an MFA method in Research.gov will receive this email from nsfextloginnoreply@nsf.gov which includes specific sign-in details. Users who add MFA to an additional device will also receive this email. This email alert is another security feature. If you do not recognize the sign-in details in the email, your account may have been compromised. Please

report any suspicious activity to the NSF IT Service Desk at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays). The security of your account is very important to NSF, and we want you to report any suspicious activity so that we can investigate it.

18. Can InCommon credentials be used to sign into Research.gov?

Users affiliated with InCommon Federation participating organizations can continue to use their organization-issued credentials to sign into Research.gov if the participating organization requires MFA for systems access. If the organization does not require MFA to access the organization's systems, users cannot sign into Research.gov with organization-issued credentials as of October 27, 2024. Users can use their NSF credentials or set up a Login.gov account and phishing-resistant MFA to sign into Research.gov if their organization-issued credentials are not an option.

19. *NEW* How does an organization integrate with Research.gov through the InCommon Federation?

Refer to About the InCommon Integration at Research.gov. If your organization is interested in joining Research.gov's Federation Integration through InCommon, please send an email request to rgov@nsf.gov. Please make sure your institution has implemented MFA.

20. Can Login.gov be used to sign into Research.gov?

Yes, users can continue using Login.gov to sign into Research.gov if a phishing-resistant MFA is used.

21. *NEW* Can I use Login.gov to sign into Research.gov if my Login.gov email address does not match my NSF account primary email address?

The Login.gov email address must match the NSF account primary email address in order to sign into Research.gov with Login.gov credentials. The user can either update their Login.gov email address and use a phishing-resistant MFA to sign into Research.gov or they should sign into Research.gov with NSF credentials (NSF ID / primary email address + password) and enroll in an MFA method in Research.gov.

22. Which Login.gov MFA options are phishing-resistant?

The phishing-resistant MFA options in Login.gov are face or touch unlock and security keys. You can set up or change your MFA in Login.gov.

Your phishing-resistant MFA in Login.gov must be set up before signing into Research.gov. If you attempt to sign into Research.gov with Login.gov credentials before setting up your phishing-resistant MFA in Login.gov, you will receive an error message.

Here's how to set up a phishing-resistant MFA method in Login.gov:

- Navigate to https://secure.login.gov/account and sign in or create an account.
- From "Your authentication methods" on the left navigation menu, select one of the phishing-resistant MFA methods and click on the option to enroll:
  - Add face or touch unlock
  - Add security key
- Close Login.gov after your phishing-resistant MFA is set up.

Open Research.gov and click on the "Sign In Using Your Login.gov Credentials" button. You will be prompted for either your face/touch unlock or security key.

23. Does it matter what type of mobile device I use (i.e., Apple or Android)?

Users can use both Apple (iOS) and Android devices for Research.gov standard MFA options.

24. What if I don't have a mobile device (smartphone or tablet) or do not want to use my personal mobile device?

Users without a mobile device they can use or who have a mobile device without the capability to download and install authenticator apps can use the security key or biometric authentication MFA methods with a computer to set up the security key, PIN *(option not available on Mac computers)*, facial recognition *(option not available on Mac computers)*, or fingerprint.

25. *NEW* Can I receive a code on my mobile device to use for Research.gov MFA without having to download and install the Google Authenticator or Okta Verify app

No, users enrolled in Google Authenticator or Okta Verify must download and install the app and then use the app each time you sign into Research.gov. There is not an option to receive a code to a mobile device without one of these apps.

26. What if I don't have a mobile device and my computer does not meet the operating system requirements (e.g., have an earlier version of the Windows or Mac operating system)?

Users should contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

27. *NEW* What do I do if I must enroll in a phishing-resistant MFA but my organization has disabled Windows Hello for Business on my computer and I don't have a mobile device?

If a user cannot utilize the security key MFA method, the NSF IT Service Desk will provide a link to install Okta software on the user's computer to use that as the MFA method to sign into Research.gov. Users can also utilize Windows Hello to enroll in phishing-resistant MFA, unless it is disallowed by their organization.

Users should reach out to their IT department **before** contacting the NSF IT Service Desk to ensure administrative privileges are enabled on the user's computer. Once administrative privileges are confirmed, users should then contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

28. *NEW* What do I do if I must enroll in a phishing-resistant MFA but my computer does not support the PIN, fingerprint, or facial recognition MFA options and I don't have a mobile device?

If a user cannot utilize the security key MFA method, the NSF IT Service Desk will provide a link to install Okta software on the user's computer to use that as the MFA method to sign into Research.gov.

Users should reach out to their IT department **before** contacting the NSF IT Service Desk to ensure administrative privileges are enabled on the user's computer. Once administrative privileges are confirmed, users should then contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

29. *NEW* What is a security key?

A security key is a physical device that can be connected to your computer or mobile device through a USB port to add an extra layer of security to online accounts.

30. What kind of security keys are supported for Research.gov MFA?

Security keys that meet the FIDO2 (Fast IDentity Online 2) standards can be used for Research.gov MFA. Note that not all security keys are phishing-resistant or can be used for Research.gov MFA. Currently YubiKey is the only security key that is supported for Research.gov MFA.

31. *NEW* Does my organization need to issue my security key or can I buy my own security key?

Organizations can purchase security keys for their users, but there is no NSF requirement that security keys used for signing into Research.gov be issued by the user's organization. Users can purchase their own security keys from retailers that sell computer accessories including Amazon. Please note that there are multiple security methods available to users, NSF does not require a security key to be purchased for MFA enrollment.

32. Do I need a mobile device to set up a biometric MFA method?

No, users can set up the fingerprint or facial recognition *(option not available on Mac computers)* MFA methods on a computer. The computer must have a fingerprint scanner to set up the fingerprint MFA method and a built-in camera to set up the facial recognition MFA method.

33. *NEW* Are there prerequisites to use the PIN, fingerprint, or facial recognition MFA methods?

Yes, to use the PIN, fingerprint, or facial recognition MFA methods, the user must have Windows Hello or Windows Hello for Business enabled on their computer and set up prior to enrolling in Research.gov MFA. If Windows Hello is not enabled and set up, then the PIN, fingerprint, and facial recognition MFA methods will not display as available MFA options for the user. Use of the fingerprint MFA method requires a fingerprint reader. Users of the facial recognition MFA method requires the user's computer to have a built-in camera. Note that the PIN and facial recognition MFA methods are not available on Mac computers.

34. Can I use my mobile device instead of a computer to enroll in a biometric MFA method?

No, users cannot enroll in the biometric MFA methods with a mobile device. A computer is needed to enroll in both fingerprint and facial recognition security methods. Please see the how-to guides on the About Signing Into Research.gov page for details.

35. How do I scan the QR code when setting up the Google Authenticator or Okta Verify MFA methods on my mobile device?

The QR code must be scanned from within the Google Authenticator or Okta Verify app on your mobile device. While in the app, the mobile device will ask your permission to allow Google Authenticator or Okta Verify access to the camera, after which you must select “OK.” Selecting "OK" will enable you to point the camera on your mobile device at the QR code and scan it.

36. Why am I getting a "Your code doesn't match our records. Please try again" error when I enter the six-digit code from Google Authenticator?

Entering a Google Authenticator code when it is nearly expired can lead to errors, as each code is valid for only 30 seconds. Please verify the code you input is still valid and try again. If a user's Google Authenticator contains multiple accounts, please also verify the code being input is labeled 'external.nsf.gov:NSF ID'. If you are still having trouble, please contact the NSF IT Service Desk at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

37. Why am I getting a "Your code doesn't match our records. Please try again" error when I enter the six-digit code from Okta Verify?

Entering an Okta Verify code when it is nearly expired can lead to errors, as each code is valid for only 30 seconds. Please verify the code you input is still valid and try again. If a user's Okta Verify contains multiple accounts, please also verify the code being input is labeled 'external.nsf.gov:NSF ID'. If you are still having trouble, please contact the NSF IT Service Desk at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

38. I already have the Google Authenticator/Okta Verify app on my mobile device, can I use it as my MFA method to sign into Research.gov?

Yes, after you scan the NSF QR code, you will see a different entry for your NSF account on your Google Authenticator/Okta Verify app.

39. *NEW* Can I delete Google Authenticator/Okta Verify after I set up MFA?

No, you must use the Google Authenticator/Okta Verify app each time you sign into Research.gov so the app cannot be deleted after the initial MFA set-up.

40. *NEW* Can I use MS Authenticator or Duo Mobile instead of installing a new app (Google Authenticator or Okta Verify)?

Yes, MS Authenticator or Duo Mobile can be used as an MFA security method (though not officially supported by the vendor). Users should complete the steps for Google Authenticator but instead of downloading the app, use the MS authenticator or Duo Mobile app to scan the QR code generated. Users must remember to retrieve their code from the MS Authenticator or Duo Mobile app even though the screen will show as Google Authenticator on subsequent sign-in to Research.gov.

41. How do I change my MFA method in Research.gov or enroll in additional MFA methods?

After signing into Research.gov, navigate to "My Profile" at the top of the screen and then to "Change Password or Security Methods." You must authenticate first and then you can enroll in a different MFA option that is available to you (i.e., if you have an administrative or financial role in Research.gov, your available MFA options will be limited to phishing-resistant methods).

InCommon organization and Login.gov MFA methods must be changed through the organization or through Login.gov.

42. How do I set up MFA if I have multiple mobile devices?

A user can set up MFA for their NSF account on multiple mobile devices by using a different MFA on up to a maximum of three mobile devices. The following MFA methods support sign-in on multiple devices: Passkey, Security Key, Google Authenticator, and Okta Verify. For example, Google Authenticator could be used on one mobile device, Okta Verify could be used on a second mobile device, and either the Passkey or Security MFA could be used on the third mobile device. To use Google Authenticator or Okta Verify, you must install the free Google Authenticator or Okta Verify app on the mobile device. The passkey and security key MFA methods can be set up on a mobile device.

43. **What happens if I only register for one security method tied to a mobile device (i.e., Google Authenticator or Okta Verify) but I no longer have access to the mobile device?**

Please contact the NSF IT Service Desk for assistance to reset your authenticator at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

44. **Are my biometric data being saved by NSF if I use one of the biometric MFA methods?**

No, NSF does not save any biometric information. NSF only uses the biometric information from the device to authenticate identity but does not process or save any biometric information.

45. **Who do I contact for MFA assistance or technical issues?**

Please contact the NSF IT Service Desk for MFA assistance or technical issues at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

46. **Why am I getting an "Unable to sign in" error when I try to sign into Research.gov with my NSF credentials?**

    This means your NSF ID/Primary Email Address or password is incorrect. Please verify and try again. If you are still having trouble, please contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

47. **What do I do if my NSF account is locked?**

    Follow these steps if your NSF account is locked:

    - You will be prompted to unlock it by entering your NSF ID or primary email address
    - After you click "Next" you will be prompted to authenticate with an MFA security method
    - Click "Send me an email"
    - Click "Enter a verification code instead." You will receive an email from 'No-Reply <nsfextloginnoreply@nsf.gov>'
    - Enter the six-digit code from the email and click "Verify"
    - After you enter your password, you will be redirected to Research.gov

48. **How do I reset/change my password?**

    After signing into Research.gov:
    - Navigate to "My Profile" at the top of the Research.gov screen
    - Select "Change Password or Security Methods." You must authenticate with an MFA security method
    - Select "Update" next to Password. Click "Yes" when prompted with "Are you sure you want to reset Password enrollment?"
    - Enter a new password, confirm your password, then click "Reset Password"

    Note that passwords for users with administrative or financial roles expire every 60 days and must be reset.

49. **Why am I getting a "Reset password is not allowed at this time. Please contact support for assistance" error when I try to reset my password?**

This means your primary email address is incorrect. Please verify and try again. If you are still having trouble, please contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

50. What if I do not remember my NSF account password?

If you do not remember your NSF account password, click the "Forgot Password" link after you enter your NSF ID or primary email address and click "Next." For additional guidance, please refer to the Password Reset Guide on the About Signing Into Research.gov page.

51. What if I do not remember my NSF ID or primary email address for my NSF account?

If you do not remember your NSF ID or primary email address for your NSF account, please contact the NSF IT Service Desk for assistance at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.

52. **Who do I contact for assistance with my NSF account or technical issues?**

Please contact the NSF IT Service Desk for NSF account assistance or technical issues at 1-800-381-1532 (7:00 AM – 9:00 PM Eastern Time; Monday – Friday except federal holidays) or rgov@nsf.gov.