



FALL 2024 NSF

---

# VIRTUAL GRANTS CONFERENCE

---

DECEMBER 9 - 12, 2024

## NSF Proposal & Award Policy Update



# Speakers

## **Jean Feldman**

Head, Policy Office, Division of Institution and Award Support; Office of Budget, Finance and Award Management

## **Dan Hofherr**

Division Director, Assistant CIO for Operations and CISO, Office of the Chief Information Officer; Division of Security and Operations



# Topics

- NSF implementation of the revised 2 CFR part 200
- NSF *Proposal and Award Policies and Procedures Guide* (PAPPG)
  - Current version (NSF 24-1)
  - Proposed changes (NSF 26-1)
- Multifactor Authentication (MFA) requirements for Research.gov
- Resources
- Q&A





# Revising 2 CFR - Background

- The Office of Management and Budget (OMB) directed agencies to incorporate 2 CFR revisions by October 1, 2024
- The Council on Federal Financial Assistance (COFFA) has included the revisions and associated documents on its website





# NSF Implementation of the Revised 2 CFR

- OMB directed agencies to implement the revisions to 2 CFR for awards made on or after October 1, 2024
- NSF implements 2 CFR in two ways:
  - NSF *Proposal and Award Policies and Procedures Guide* (PAPPG)
  - Award Terms and Conditions
- NSF has revised the Grant General Conditions (GC-1) for awards made on or after October 1st
- The Research Terms and Conditions (RTC) are no longer referenced in awards made on or after October 1, 2024
  - The RTC page has been modified to make clear that the RTCs have not been modified for consistency with the revised 2 CFR and will not be incorporated into NSF award made on or after October 1, 2024



# Revising 2 CFR – Suite of NSF Terms and Conditions

- Grant General Conditions (GC-1)
- Cooperative Agreement Financial and Administrative Conditions (CA-FATC)
- Cooperative Agreement Modifications and Supplemental Financial and Administrative Terms and Conditions for Major Multi-User Research Facility Projects and Federally Funded Research and Development Centers
- Cooperative Agreement Modifications and Supplemental Financial and Administrative Terms and Conditions for Mid-Scale Research Infrastructure Projects
- Special Terms and Conditions for Administration of NSF Conference or Travel Grants (FL 26)
- Small Business Innovation Research (SBIR)/Small Business Technology Transfer (STTR) Terms and Conditions
- International Research Terms and Conditions (IRTC)
- Special Terms and Conditions for Administration of NSF Conference or Travel Awards Made to International Organizations (FL 26 for IRTC)



# Revision of 2 CFR – NSF Implementation Process

- Unless otherwise specified, the Grant General Conditions (GC-1) will apply to all recipients of NSF grant awards, including:
  - Institutions of Higher Education (IHEs);
  - Non-profit, non-academic organizations;
  - For-profit organizations (other than Small Business Innovation Research/Small Business Technology Transfer recipients);
  - State and local governments; and
  - Tribal Nations.
- In the case of any inconsistency between the coverage contained in the NSF *Proposal and Award Policies and Procedures Guide* and 2 CFR (including 2 CFR part 200), the coverage specified in 2 CFR applies





# Revision of 2 CFR – NSF Implementation Process

- The following statement appears on NSF program pages:

“NSF Financial Assistance awards (grants and cooperative agreements) made on or after October 1, 2024, will be subject to the applicable set of award conditions, dated October 1, 2024, available on the [NSF website](#). These terms and conditions are consistent with the revised guidance specified in the [OMB Guidance for Federal Financial Assistance](#) published in the Federal Register on April 22, 2024”
- The following appears as a header in each PAPPG (NSF 24-1) Chapter:

“In the case of any inconsistency between the coverage contained in the NSF *Proposal and Award Policies and Procedures Guide* and 2 CFR (including 2 CFR part 200), the coverage specified in 2 CFR applies”





# Summary of Changes Made to the GC-1

- The Policy Office held a webinar covering all the changes to the Grant General Conditions (GC-1)
- View the presentation on-demand on the [Policy Outreach website](#)

## Revision of the NSF Award Conditions to Implement the Revised 2 CFR

This webinar will discuss important changes to Title 2 of the Code of Federal Regulations (2 CFR) for grant proposers and awardees effective October 1, 2024. Learn how these revisions will improve the stewardship of Federal funds.

Held on September 12, 2024

*Presenter: Jean Feldman*

A thumbnail image for a YouTube video. It features a collage of scientific images on the left, including a person in a lab coat, a microscope, and various scientific equipment. On the right, the NSF logo is at the top, followed by the text "2024 NSF POLICY OFFICE WEBINAR SERIES" in large blue letters. Below that, a red play button icon is centered, and the text "Revision of the NSF Award Conditions to Implement the Revised 2 CFR" is written in blue. At the top right of the thumbnail, there are icons for "Watch later" and "Share".

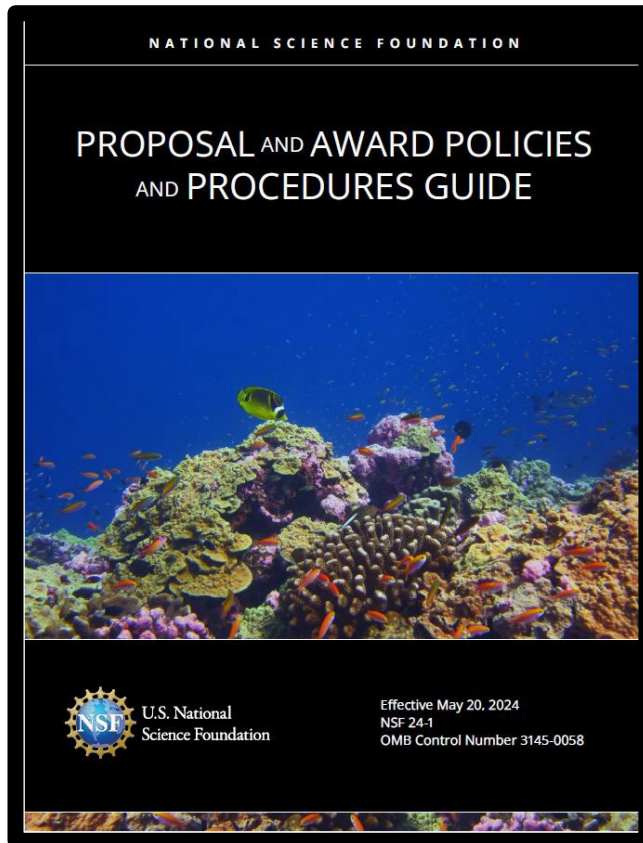
2024 NSF POLICY OFFICE  
**WEBINAR SERIES**

Revision of the NSF Award Conditions  
to Implement the Revised 2 CFR



# Current NSF PAPPG (NSF 24-1)

**Effective for proposals submitted or due on or after May 20, 2024**



## Summary of Changes to the PAPPG (NSF 24-1)

### [Home Proposal & Award Policies & Procedures Guide \(PAPPG\) \(NSF 24-1\)](#)

[PAPPG - printable version \(PDF\)](#)

#### [Summary of Changes to the PAPPG](#)

[Table of Contents](#)

[Introduction](#) +

[Part I: Proposal Preparation and Submission Guidelines](#) +

[Part II: Award, Administration and Monitoring of NSF Assistance Awards](#) +

[Subject Index](#)

[Privacy Act and Public Burden Statements](#)

*Effective Date May 20, 2024*

#### Overall Document

- Editorial changes have been made throughout to either clarify or enhance the intended meaning of a sentence or section.
- Website and document references have been updated to reflect current information.
- Updates have been made to ensure consistency with data contained in NSF systems or guidance located and terminology used in other NSF or Federal policy documents.

#### By-Chapter Changes

##### Chapter I: Pre-Submission Information

- **Chapter I.D, Concept Outlines**, has been updated to provide additional clarity on the use of concept outlines and the Program Suitability and Proposal Concept Tool (ProSPCT).
- **Chapter I.D, Types of Submissions**, includes new coverage on the use of concept outlines and the required use of the Program Suitability and Proposal Concept Tool (ProSPCT) for submission. Additional changes on the use of concept outlines and the use of ProSPCT for specific proposal types is available in Chapter II.E.
- **Chapter I.E, Who May Submit Proposals**



# Proposed PAPPG Timeline (NSF 26-1)

- December 2024 – 60-day comment period in the Federal Register begins
- Spring/Summer 2025 – Published on the NSF website
- October 2025 – PAPPG implementation







# PAPPG Proposed Changes (NSF 26-1)

## Overall Document:

- Revised the PAPPG for consistency with the **Revised 2 CFR part 200**, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*, including:
  - Equipment-Related Thresholds
  - *De minimis* Indirect Cost Rates
  - Modified Total Direct Costs
  - Cybersecurity Internal Controls
  - Single Audit
- Implements the OSTP Memorandum entitled, ***Ensuring Free, Immediate, and Equitable Access to Federally Funded Research*** (Nelson Memorandum)





# PAPPG Proposed Changes (NSF 26-1)

## Highlighted Proposed Changes:

- Updates the NSF Introduction section to include revised coverage on funding of **human disease research**
- Incorporates a new proposal type in the Types of Submission coverage for **Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) Project Pitch**
- Implements the CHIPS and Science Act of 2022 requirement that no NSF funds may be awarded to an IHE that maintains a contract or agreement with a **Confucius Institute**
- Enhances **NSF's Deadline Date** policy to identify the medical leave of a senior/key person as an exception to the deadline date policy
- Incorporates new coverage on **NSF's Education and Training Application (ETAP)** that connects individuals, such as students and teachers, with NSF-funded education and training opportunities



# PAPPG Proposed Changes (NSF 26-1)

- Revises the Font, Spacing and Margin section to require **descriptive alternative text** for all images, graphs and charts to ensure legibility and readability for individuals with visual impairments
- Supplements the Allowable and Unallowable Costs section with new coverage on the **American Drone Security Act of 2024**, which prohibits use of NSF funds on or after December 22, 2025, (1) to procure unmanned aircraft systems (drones) that are manufactured or assembled by a covered foreign entity; or (2) in connection with the operation of such a drone or unmanned aircraft systems
- Clarifies **NSF's Mentoring Plan** requirements to indicate that for each proposal that requests salary or stipend support for postdoctoral scholars or graduate students, the proposer must upload a "Mentoring Plan" in the supplementary documentation section of Research.gov



# PAPPG Proposed Changes (NSF 26-1)

- Modifies **Data Management and Sharing Plans** requirements to:
  - Highlight the presumption that all publications and supporting data will be made publicly and freely available at the time of publication. Exceptions may be granted, but justifications must be provided if there are any access limitations for either the publications or supporting data
  - Require use of a fillable webform available in Research.gov with pulldowns for common cases, designed to ease PI burden and yield structured data regarding data/publication sharing and requested exceptions and justifications.
- Eliminates the limitation for “**Beginning Investigators**” to the Biological Sciences Directorate from being duplicates of proposals to other Federal agencies for simultaneous consideration
- Implements the revised U.S. Government Policy of Oversight of **Dual Use Research of Concern (DURC)** and Pathogens with Enhanced Pandemic Potential (PEPP) requirements



# PAPPG Proposed Changes (NSF 26-1)

- Modifies **Rapid Response Research (RAPID)** Proposal coverage to increase maximum budget to \$300,000 for up to one year
- Modifies **EARly-Concept Grants for Exploratory Research (EAGER)** Proposal coverage to increase maximum budget for up to \$400,000 for up to two years
- Incorporates new coverage that addresses postaward changes that may impact **Tribal Nation Resources or Interests**
- Updates the policy covering **Individual Development Plans** for postdoctoral scholars and graduate students to incorporate a new definition of “substantial support” that addresses payment via stipends
- Enhances the **Foreign Financial Disclosure Report (FFDR)** section to address lessons learned from the initial reporting cycle





# PAPPG Proposed Changes (NSF 26-1)

- Amends the **Responsible and Ethical Conduct of Research** coverage to require training in the responsible and ethical conduct of research specified in the CHIPS and Science Act of 2022, to include, in addition to mentor training and mentorship, training to raise awareness of potential research security threats, and federal export control, disclosure, and reporting requirements
- Modifies the **Research Security** policy to include new coverage on research security assessment and required documentation and research security training requirements included in the CHIPS and Science Act of 2022
- Modifies the **Property Management Standards** policy for consistency with 2 CFR part 200 and the conditional vesting of title to equipment



# PAPPG Proposed Changes (NSF 26-1)

- Revises the **Research Involving Recombinant or Synthetic Nucleic Acid Molecules** section has been revised to divide the coverage into two sections: a) Use of Recombinant or Synthetic Acid Molecules; and b) Procurement of Synthetic Nucleic Acids
- Modifies coverage on **Public Access to Copyrighted Material and Dissemination and Sharing of Research Results** to implement the public access requirements specified in the Nelson Memorandum
- Clarifies the **Research Misconduct** policy to reiterate that research misconduct means “fabrication, falsification, or plagiarism (whether committed by an individual directly or through the use or assistance of other persons, entities, or tools, including artificial intelligence (AI)-based tools) in proposing or performing research funded by NSF, reviewing research proposals submitted to NSF, or in reporting research results funded by NSF.”



# Multifactor Authentication for Research.gov Sign-in

- Effective Oct. 27, 2024, NSF implemented mandatory multifactor authentication (MFA) for Research.gov sign-in.
- MFA is a layered security measure that requires two or more authentication methods to verify a user's identity.
- MFA protects both research community users and NSF.
- Users with administrative or financial roles signing into Research.gov with NSF credentials must use a phishing-resistant MFA.
- All users must use MFA each time they sign into Research.gov.
- See [Dear Colleague Letter \(NSF 25-011\)](#) and the [About Signing Into Research.gov](#) page for details.



Contact [rgov@nsf.gov](mailto:rgov@nsf.gov)



# Multifactor Authentication for Research.gov Sign-in

**Step 1:** Determine how you will sign into Research.gov. MFA enrollment depends on how you access Research.gov (NSF credentials, organization credentials or Login.gov credentials)

Research.gov Sign-in Option	MFA Enrollment	Prerequisite
<b>NSF Credentials</b> <ul style="list-style-type: none"><li>• NSF ID + Password</li><li>• Primary Email + Password</li></ul>	Through Research.gov: <ul style="list-style-type: none"><li>• Users must enroll in MFA method in Research.gov</li><li>• See the <a href="#">About Signing Into Research.gov page</a> for a how-to enroll guide and video tutorial for each MFA method</li></ul>	<ul style="list-style-type: none"><li>• Users with administrative or financial roles must use a phishing-resistant MFA method</li><li>• Other users such as PIs and reviewers can use a standard MFA method*</li></ul> <p><i>*However, NSF encourages all users to use a phishing-resistant MFA method</i></p>
<b>Organization-Issued Credentials**</b>  <i>**InCommon Federation participating organizations only</i>	Through InCommon Federation participating organization	InCommon organization must enforce MFA for system access on the organization's side
<b>Login.gov Credentials</b>	Through <a href="#">Login.gov</a>	Users must use a phishing-resistant MFA in Login.gov





# Multifactor Authentication for Research.gov Sign-in

**Step 2:** Users signing into Research.gov with NSF credentials determine their available MFA options based on their user role in Research.gov.

	User Role	MFA Options Set Up in Research.gov
Phishing-resistant MFA	<b>Users with Administrative or Financial Roles:</b> <ul style="list-style-type: none"><li>Administrator</li><li>Awardee Preparer</li><li>Awardee Certifier</li><li>Awardee Financial Representative</li><li>Proposed Postdoctoral Fellow</li><li>Authorized Organizational Representative (AOR)</li><li>Sponsored Projects Officer (SPO)</li><li>Foreign Financial Disclosure Report (FFDR) Preparer</li><li>View Only (View Reports)</li></ul>	<ul style="list-style-type: none"><li>Passkey</li><li>PIN</li><li>Fingerprint (biometric)</li><li>Facial Recognition (biometric)</li><li>Security Key</li></ul>
Standard MFA	<b>Other Users:</b> <ul style="list-style-type: none"><li>Principal Investigator (PI) or co-Principal Investigator (co-PI)</li><li>Other Authorized User (OAU)</li><li>Reviewers (includes <i>ad hoc</i> reviewers, panelists, and other meeting participants)</li><li>Graduate Research Fellowship Program (GRFP) Applicant</li><li>GRFP Fellow</li><li>GRFP Coordinating Official (CO)</li><li>GRFP Alternate Coordinating Official (Alt. CO)</li><li>GRFP Financial Official (FO)</li><li>Users without roles including newly registered users, reference letter writers, and Education &amp; Training Application (ETAP) participants</li></ul>	<ul style="list-style-type: none"><li>Google Authenticator</li><li>Okta Verify</li></ul> <p><i>Google Authenticator or Okta Verify app must be downloaded and installed to mobile device.</i></p>

**Note:** Users with administrative or financial roles must use a phishing-resistant MFA. Other users can opt to use a phishing-resistant MFA.

















# Research.gov MFA Help Resources

**Step 3:** Users follow the relevant step-by-step guide and video tutorial to enroll in the selected MFA method in Research.gov.


- [MFA Options Overview](#)
- [MFA Quick Reference Guide](#)
- [Frequently Asked Questions](#)
- [About Signing Into Research.gov page](#)
  - How-to guide for each MFA method
  - Video tutorial for each MFA method
  - Physical device and operating system requirements for each MFA method
  - Installation requirements (e.g., Google Authenticator and Okta Verify apps) for each MFA method
- [How Ad Hoc Reviewers Access Assigned Proposals for Review Guide](#): Walk-through of steps in Research.gov for *ad hoc* reviewers
- [Meetings at NSF](#): Walk-through of steps in Research.gov for panelists and other meeting participants

Screenshot from [About Signing Into Research.gov page](#)


				Requirements			
	Security Methods	How to Guides	Video Tutorials	Physical Devices	Operating System	Installation	Allows Sign-in from Multiple Devices?
Phishing-resistant MFA	PassKey		 PassKey Tutorial	Mobile device (smartphone or tablet)	<ul style="list-style-type: none"><li>Windows 10/11</li><li>Mac 12/13/14</li></ul>		Yes
	PIN		 PIN Setup Tutorial	Windows computer with Windows Hello for Business + PIN (PIN option not available on MAC computers)	<ul style="list-style-type: none"><li>Windows 10/11</li></ul>		No
	Fingerprint		 Fingerprint Scanning Tutorial	Windows or Mac computer with Windows Hello for Business + Fingerprint reader	<ul style="list-style-type: none"><li>Windows 10/11</li><li>Mac 12/13/14</li></ul>		No
	Facial Recognition		 Facial Recognition Tutorial	Windows computer with Windows Hello for Business + Built-in Camera (Facial recognition option not available on MAC computers)	<ul style="list-style-type: none"><li>Windows 10/11</li></ul>		No
	Security Key		 Security Key Tutorial	Windows or Mac computer with FIDO2 token (e.g., YubiKey)	<ul style="list-style-type: none"><li>Windows 10/11</li><li>Mac 12/13/14</li></ul>		Yes
MFA	Google Authenticator		 Google Authenticator Tutorial	Mobile device (smartphone or tablet)	<ul style="list-style-type: none"><li>Android 10+</li><li>iOS 16/17</li></ul>	Google Authenticator app	Yes
	Okta Verify		 Okta Verify Tutorial	Mobile device (smartphone or tablet)	<ul style="list-style-type: none"><li>Android 10+</li><li>iOS 16/17</li></ul>	Okta Verify app	Yes



# Research.gov New User Sign In Page

**Research.gov**  
ONLINE GRANTS MANAGEMENT  
FOR THE NSF COMMUNITY

Sign In | Register | Home | Contact | Help


 **NSF User Sign In**  
Choose a secure method to sign in to your NSF account in Research.gov

**NSF Credentials**

- Uses NSF ID or Primary Email address
- Step-by-step verification using your phone, app, security key or biometrics
- Learn more [About Research.gov Sign In](#)

**Sign In Using NSF Credentials**

New to NSF? [Register](#)

 [Sign In for NSF Staff](#)

or

**Organization Credentials**

- Directs you to sign in to your organization
- Redirects you back to Research.gov

Select an Option ▼


**Sign In Using Organization Credentials**

Don't see your organization? [Learn more](#) / [Register for InCommon](#)

or

**Login.gov Credentials**

- Directs you to sign in using login.gov
- Redirects you back to Research.gov

 **LOGIN.GOV**

**Sign In Using login.gov Credentials**

- One-time MFA setup required for users signing in with NSF credentials
- Users can continue to use their organization-issued credentials to sign in if their organization implements MFA
- Users can continue to sign in with Login.gov provided they use a phishing-resistant MFA





# Research.gov MFA Tips

- Set up MFA as far in advance as possible of upcoming proposal deadlines or meetings to avoid unexpected MFA enrollment issues. Some issues can take more than one business day to resolve (e.g., no access to primary email address)
- Users enrolling in Research.gov MFA must have access to their NSF account primary email address to receive the one-time passcode (OTP) from [nsfextloginnoreply@nsf.gov](mailto:nsfextloginnoreply@nsf.gov) to start the MFA enrollment process. Please check your spam and junk folders if you do not receive this email
- There is **no cost** to enroll in MFA in Research.gov. Do not 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
- If you are using the Google Authenticator or Okta Verify MFA method, do not delete the app after you set up your MFA method. You will need to use the app each time you sign into Research.gov
- Avoid the line at the NSF IT Service Desk! Many MFA questions are answered in the [Frequently Asked Questions](#), how-to guides, and video tutorials on the [About Signing Into Research.gov page](#)
- If your Research.gov MFA issue will prevent you from submitting a proposal or completing reviewer activities, communicate to the cognizant Program Officer or meeting Point of Contact as soon as possible. Provide screenshots of your issue





# Contacting the NSF IT Service Desk for MFA Assistance

- Due to increased traffic, NSF IT Service Desk support wait times are longer than normal. The IT Service Desk is prioritizing users with upcoming meetings and deadlines. We appreciate your patience
- A screenshot of errors you encounter is helpful so that the IT Service Desk can identify the problem faster
- Additional information to provide to the NSF IT Service Desk:
  - Description of the issue
  - Full name
  - NSF ID
  - Research.gov role (or intended role) at the organization (e.g., PI, AOR, Administrator)
  - Email address that is currently associated to your NSF account or phone number registered to your NSF account If you don't know the email address
  - Organization your NSF account is affiliated with
  - Please advise if you are participating in an upcoming panel. What is the panel ID?
  - Please advise if you have any upcoming proposal deadlines (funding opportunity number/due date/deadlines). What is your proposal number?



# Providing Research.gov MFA Feedback

NSF wants your feedback! Submit your comments and suggestions for improvement to <https://www.research.gov/research-web/feedback> or use the orange Feedback button at the bottom of the Research.gov homepage to access the Feedback page.

## Research.gov Feedback

We at Research.gov are dedicated to delivering you the best federal grants management services on the web. We value your thoughts and suggestions. Although we cannot reply to each individual response, we do appreciate your feedback and will use it to evaluate changes and make improvements in our site.

**\* Required Field**

Name:

Email Address:

Site Area:

Select One

Select One

Account access – Multi Factor Authentication (MFA)

Account Profile and Roles

Prepare and Submit Proposals

Panels and Review Proposals

Awards, Reporting, Post-award

Fellowships and Honorary Awards

Financials

Foreign Financial Disclosure Report

Other

\* Comments or Suggestions:

(3000 character limit)

Need help immediately?

If you need immediate attention, instead of filling out the feedback form, please contact the IT Service Desk.

**Email:** [rgov@nsf.gov](mailto:rgov@nsf.gov)  
**Call:** 1-800-381-1532

The NSF Research.gov logo, featuring the NSF logo and the text 'Research.gov'.

The National Science Foundation logo, featuring a stylized globe and the text 'National Science Foundation'.



# Key Documents and Information

[Proposal & Award Policies & Procedures Guide](#)

[Policy Office Website](#)

[Policy Outreach Information](#)

[Research.gov](#)

[About Signing Into Research.gov page](#)





For More Information

**“Ask Early, Ask Often!”**

**[nsf.gov/staff](https://www.nsf.gov/staff)**

**[nsf.gov/staff/orglist.jsp](https://www.nsf.gov/staff/orglist.jsp)**

**[new.nsf.gov/careers/rotator-programs](https://www.new.nsf.gov/careers/rotator-programs)**



# Appendix



# Research.gov New MFA Screens

As of October 27, 2024, **ALL** users signing into Research.gov with NSF credentials are required to complete a one-time set-up of a security method by entering their password **AND** verifying their primary email address by entering a one-time passcode (OTP) sent to their primary email address on file.

## Step 1

Sign-in using NSFID/Primary Email Address

## Step 2

Select password to enter.

## Step 3

Enter your password.

Steps highlighted in green must be completed each time a user signs into Research.gov





# Research.gov New MFA Screens

Primary email address verification steps and a one-time passcode (OTP) will be triggered to a user's primary email address

**Step 4** Get a verification email to your primary email address on file

The screenshot shows the NSF Research.gov login page. At the top is the NSF logo and the text "U.S. National Science Foundation". Below this is an email icon and a grey pill-shaped button containing a person icon and the email address "john.doe@gmail.com". The main heading is "Get a verification email". Below it, the text reads: "Send a verification email to F\*\*\*t@nsf.gov by clicking on 'Send me an email'." There is a large blue button labeled "Send me an email". At the bottom, there are two links: "Need Help ?" with an external link icon, and "Back to sign in".

**Step 5** Enter the one-time code received in your primary email address

The screenshot shows the "Verify with your email" screen. At the top is the NSF logo and the text "U.S. National Science Foundation". Below this is an email icon and a grey pill-shaped button containing a person icon and the email address "john.doe@gmail.com". The heading is "Verify with your email". The text below reads: "We sent an email to F\*\*\*t@nsf.gov. Click the verification link in your email to continue or enter the code below." There is a red rectangular box around a button labeled "Enter a verification code instead". At the bottom, there are two links: "Need Help ?" with an external link icon, and "Back to sign in".

The screenshot shows the "Verify with your email" screen with the code entry state. At the top is the NSF logo and the text "U.S. National Science Foundation". Below this is an email icon and a grey pill-shaped button containing a person icon and the email address "john.doe@gmail.com". The heading is "Verify with your email". The text below reads: "We sent an email to F\*\*\*t@nsf.gov. Click the verification link in your email to continue or enter the code below." Below this is a section titled "Enter Code" with a text input field containing the code "825410". There is a large blue button labeled "Verify". At the bottom, there are two links: "Need Help ?" with an external link icon, and "Back to sign in".



# Research.gov New MFA Screens

The user's MFA security method options are based on their role(s) in Research.gov. Users with administrative or financial privileges must use a phishing-resistant MFA method.

**Step 6** Select an Authenticator for the 2<sup>nd</sup> factor and complete the login.

Regular User

U.S. National Science Foundation

john.doe@gmail.com

### Set up security methods

Security methods help protect your research.gov account by ensuring only you have access.

**Set up required**

**Google Authenticator**  
Enter a temporary code generated from the Google Authenticator app.  
Used for access  
[Set up →](#)

**Okta Verify**  
Okta Verify is an authenticator app, installed on your phone or computer, used to prove your identity  
Used for access  
[Set up →](#)

**Security Key or Biometric Authenticator**  
Use a security key or a biometric authenticator to sign in  
Used for access  
[Set up →](#)

Administrative or  
or Financial User

U.S. National Science Foundation

0000A0MRG

### Set up security methods

Security methods help protect your research.gov account by ensuring only you have access.

**Set up required**

**Security Key or Biometric Authenticator**  
Use a security key or a biometric authenticator to sign in  
Used for access  
[Set up →](#)

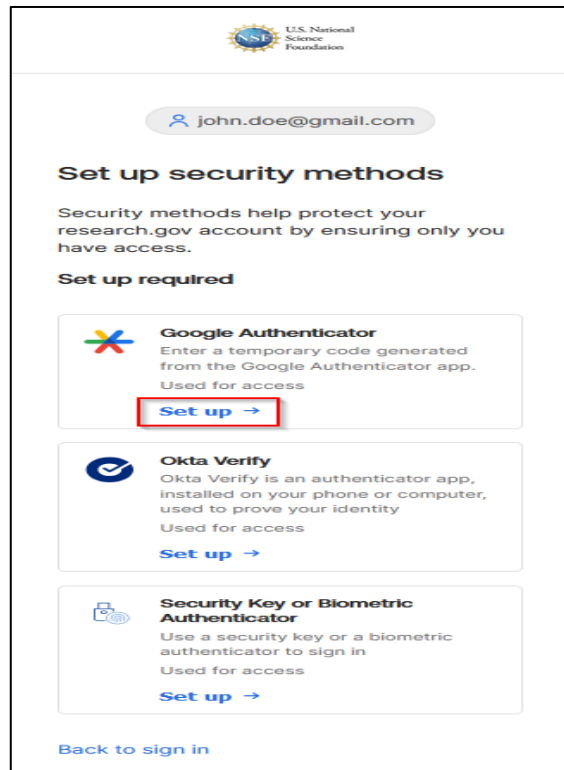
[Back to sign in](#)



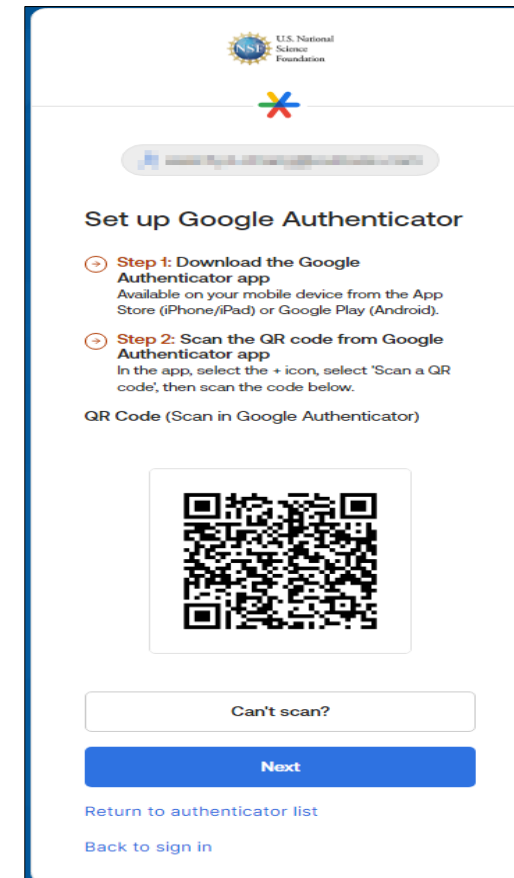
# Research.gov New MFA Screens

Google Authenticator setup for non-privileged users (users without an administrative or financial role in Research.gov):

**Step R7** Click setup under Google Authenticator from the setup security methods screen.



**Step R8** Scan the QR code into the Google Authenticator from your mobile device.




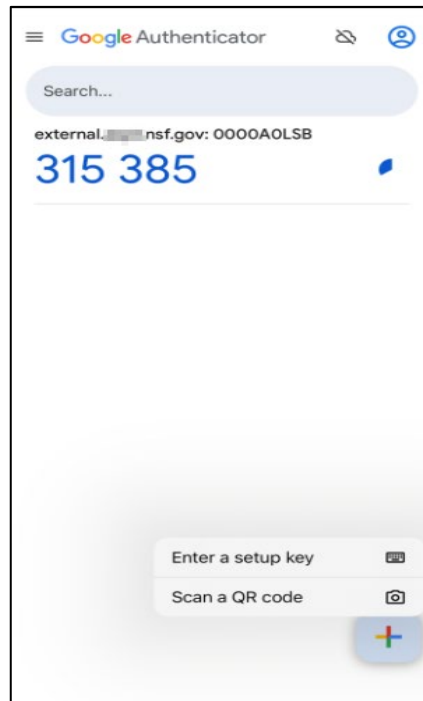




# Research.gov New MFA Screens

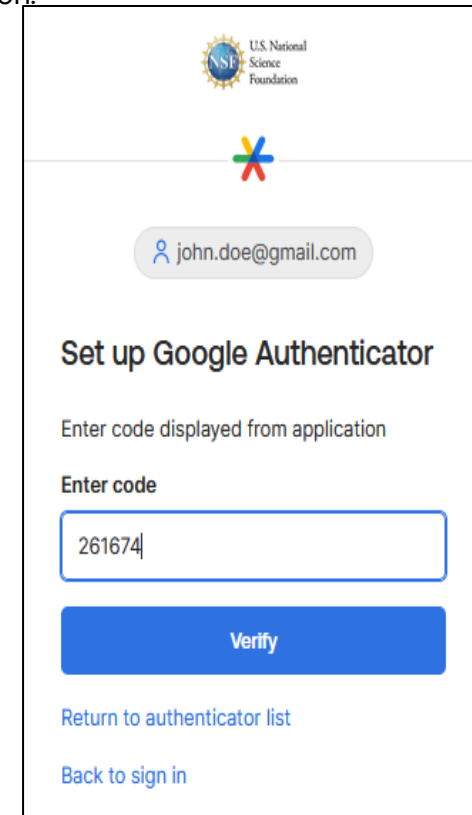
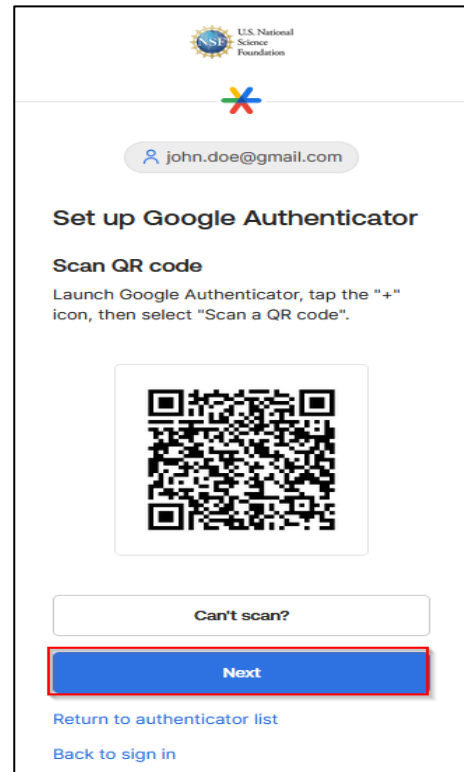
Google Authenticator setup for non-privileged users (users without an administrative or financial role in Research.gov):

**Step R9** Open Google Authenticator App on your mobile device. Click on the  icon and select Scan a QR code



## Step R10

Once you scan the QR code, you will see a 6-digit rotating code on the Google Authenticator app. Enter the 6-digit code on the browser screen and click verify and log into Research.gov application.



Steps highlighted in green must be completed each time a user signs into Research.gov



# Research.gov New MFA Screens

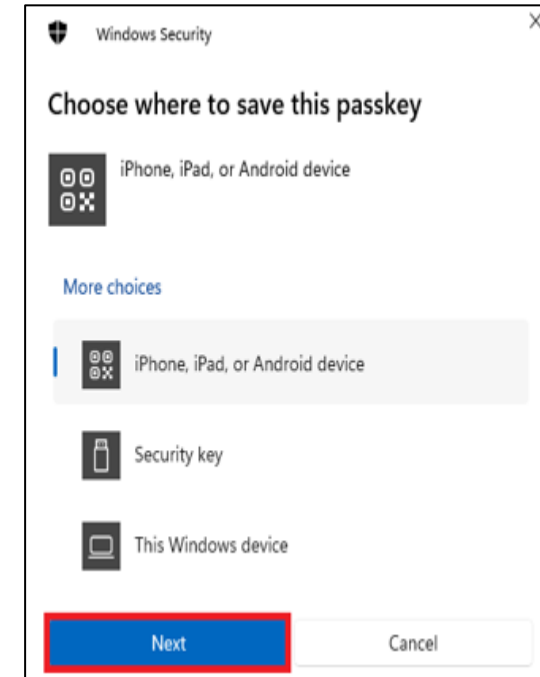
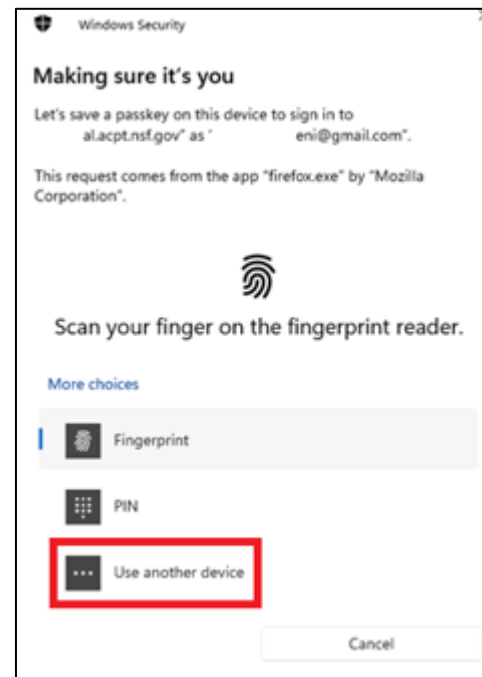
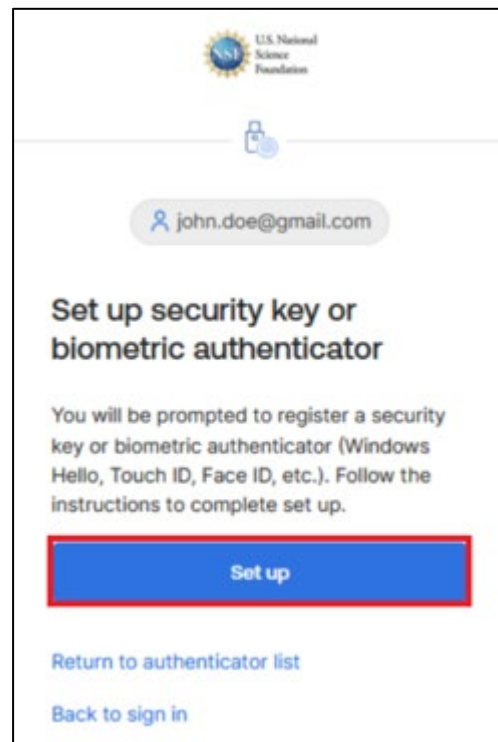
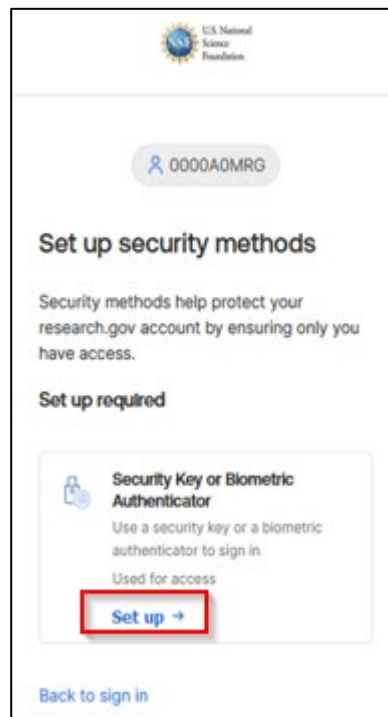
Passkey setup for privileged users (users with an administrative or financial role in Research.gov);

**Step P7** Select setup from Security Key or Biometric Authenticator.

**Step P8** Select set up in the next screen

**Step P9** Select Use another device if you don't see iPhone, iPad or Android Device. Select iPhone, iPad or Android device and select next.

Steps highlighted in green must be completed each time a user signs into Research.gov





# Research.gov New MFA Screens

Passkey setup for privileged users (users with an administrative or financial role in Research.gov):

## Step P10

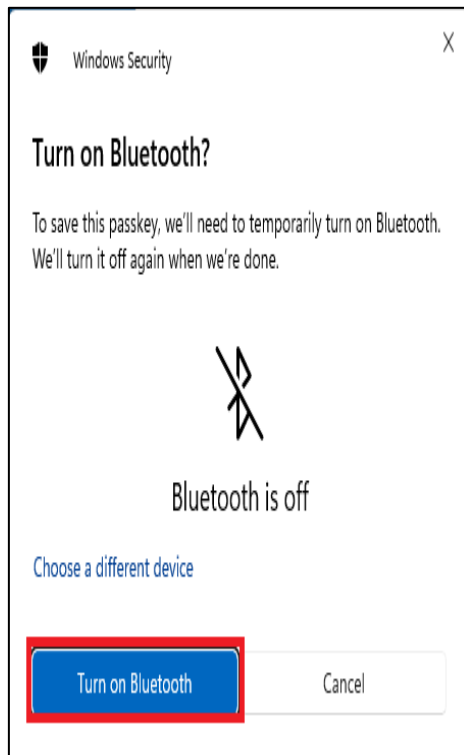
Please turn on your Bluetooth if it is not turned on.

## Step P11

Use your mobile device to scan the QR code on your laptop

## Step P12

Once the QR code is scanned, you will see a "Use Passkey" message. Tap the Use Passkey message. Once set-up is complete, you should see the screen below on your system. Follow the prompts on your mobile device. Your mobile device will require you to sign in using the same unlock feature on your phone.



Steps highlighted in green must be completed each time a user signs into Research.gov