U.S. NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 25-011

Dear Colleague Letter: Multifactor Authentication Implementation for Research.gov

Date: October 11, 2024

Dear Colleagues:

As part of our 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, effective on **October 27, 2024**, the U.S. National Science Foundation (NSF) is implementing multifactor authentication (MFA) for Research.gov. With the growing number of cyber threats, traditional password-only security is no longer sufficient. MFA provides an added layer of security and helps to ensure that only authorized users can access Federal resources online.

How does this change impact the external research community starting on October 27?

Effective on **October 27**, all external users must first complete a one-time MFA enrollment process and use the selected MFA method to sign into Research.gov. The MFA options for each user depend on their assigned role in Research.gov. Users with financial or administrative roles must use a phishing-resistant MFA method. Other users can select a phishing-resistant or regular MFA method; however, NSF strongly recommends that all users choose a phishing-resistant MFA. All Research.gov users must set up a primary MFA sign-in method to access 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). Users will be required to use MFA each time they sign into Research.gov.

Users can continue using Login.gov to sign into Research.gov if a phishing-resistant MFA is used. InCommon Federation users can continue to use their organization-issued credentials to sign into Research.gov if the participating organization requires MFA for systems access.

What is MFA and how does it work?

MFA is a layered security measure that requires two or more authentication methods to verify

a user's identity. MFA will increase the security of the Research.gov portal because even if one authentication method such as a password becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will be prevented from accessing Research.gov.

Here are the three main types of MFA and examples of each:

- **Something You Know** – PIN, password, or one-time passcode (OTP)
- **Something You Have** – Physical object such as a mobile device, laptop, USB device, key, or smart card
- **Something You Are** – Biometric authentication such as a fingerprint or face scan

For more information about MFA and phishing-resistant MFA, please see More than a Password: Protect Yourself from Malicious Hackers with Multifactor Authentication published by the Cybersecurity & Infrastructure Security Agency.

Training Resources

Training resources including how-to guides and frequently asked questions (FAQs) will be available on the new About Signing Into Research.gov page on Research.gov Help on **October 27**. This new page will assist the research community to quickly enroll in MFA and learn how to sign into Research.gov with the selected MFA method.

Questions? If you have IT system-related questions, please contact the NSF IT Service Desk at 1-800-381-1532 (7:00 AM - 9:00 PM ET; Monday - Friday except federal holidays) or to rgov@nsf.gov.

Thank you for your partnership with NSF and for your assistance to strengthen the security of Research.gov.

Regards,
Terry L. Carpenter
Office Head and Chief Information Officer
Office of the Chief Information Officer
U.S. National Science Foundation