In 2020, NIH encouraged our InCommon partners to support federated MFA and identity assurance to help us meet federal requirements for easy and secure access to our systems. We shared three requirements.
Requirement 1

*Provide basic user information* about the people accessing NIH resources so that we can provision and manage efficient and secure access
Requirement 2

Implement strong multi-factor authentication (MFA) so that we can minimize risk to NIH IT resources
Requirement 3

Provide assurance that each person who logs in is who they say they are so that we can provide appropriate authorization to access NIH data.
The InCommon community delivered.
UPDATE ON MFA AND IDENTITY REQUIREMENTS

Where We’ve Been...

1. In 2020, NIH encouraged the InCommon partners to support federated MFA and identity assurance to help us meet federal requirements for easy and secure access to our systems. We shared three requirements.

2. In 2021, the electronic Research Administration (eRA) system became the first NIH system to require MFA (with no/low identity assurance) and the first to accept federated MFA or Login.gov.
Federated IdPs Using MFA at NIH Login Gateway

- September 15, 2021: eRA begins accepting federated MFA
- June 28, 2021: 37 Domains
- December 13, 2021: 174 Domains
- February 20, 2023: 204 Domains

Count of Domains
Thank you – for your efforts and support!
Let’s look at some more data.
Today there are... 350 institutions have implemented MFA using the REFEDS MFA profile for access to eRA.
Federated MFA for eRA by Top 40 NIH-Funded Members

% Logins Using InCommon vs Login.gov

Average: 10% InCommon

Highest NIH-Funded Institutions from Most Funding (Left) to Least (Right)
Federated Logins

Federated MFA Logins to eRA vs. Non-eRA Federated Logins

Total Number of Unique User Logins Between October 2022 – March 2023

- **eRA Logins**: 15,713
- **Non-eRA Logins**: 203,690

Key Takeaways:
- More people are using federated login than federated MFA, and more institutions are providing federated login than federated MFA.
- Many of those non-eRA systems will require MFA and identity assurance soon.
- Prepare to implement response signaling using the [REFEDS MFA Profile](https://www.refeds.org/profiles/mfa) and [REFEDS Assurance Framework](https://www.refeds.org/frameworks/assurance).
Done

- Reduced security risks for eRA
- Provided single sign-on options for researchers and faculty
- Leveraged research institutions’ investments in MFA

To Do

- Researchers may not know that they can log into eRA with their institution’s credentials
- Other NIH systems will require both MFA and identity assurance soon
UPDATE ON MFA AND IDENTITY REQUIREMENTS

Past is prologue

1. In 2020, NIH encouraged the InCommon partners to support federated MFA and identity assurance to help us meet federal requirements for easy and secure access to our systems. We shared three requirements.

2. In 2021, the electronic Research Administration (eRA) system became the first NIH system to require MFA (with no/low identity assurance) and the first to accept federated MFA or Login.gov.

3. In 2023, NIH continues to request that federation partners enable support for federated MFA and identity assurance.
How can you support us?
You can...

1. Support the [REFEDS MFA Profile](#) if you haven’t yet

2. Support the [REFEDS Assurance Framework](#)

3. Encourage [federated credential use](#) in your community
Don’t wait. **Lead now!**
Resources

- REFEDS MFA Profile
- REFEDS Assurance Framework
- REFEDS Research and Scholarship Category
- REFEDS Assurance Working Group
- REFEDS Assurance Framework Implementation Guidance for InCommon Participants
- Get NIH Ready
- Kantara Initiative’s Trust Status List of Component Services

For more information about MFA and identity assurance requirements, please contact help@incommon.org.