National Institutes of Health
Center for Information Technology

Identity & Access Management

Jeff Erickson, Chief of NIH Identity and Access Management
Sumit Nanda, Technical Lead, NIH Identity and Access Management

December 2022

Contents | Identity & Access Management (IAM)

NIH Center for Information Technology

What is Identity & Access Management?

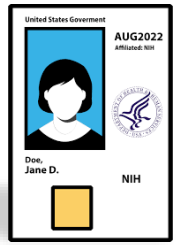
A suite of products and services that ensure NIH staff and research collaborators have **seamless, secure access** to the data and resources they need.

Identity Management

Example: *NIH Enterprise Directory*

How an agency **collects, verifies, maintains, and terminates** digital identities of people and things

Credential Management



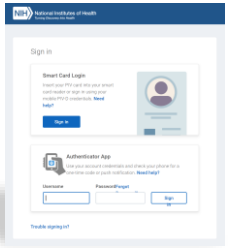
Example: *PIV Card*

How an agency **issues, manages, and revokes** credentials such as PIV cards, passwords, tokens, and certificates that individuals use to prove their digital identities online

Federation

How an agency **facilitates** the secure exchange of data about people and things by accepting external credentials for access to its systems and applications

Access Management



Example: *NIH Login*

How an agency **authenticates** credentials and **authorizes** appropriate access to protected services

Governance

How an agency **establishes** and **uses** standards for data about people and things, and how it **aligns** with Federal standards and policies

Why Do We Provide IAM Services? | Identity & Access Management

NIH Center for Information Technology

1

Protect People and Resources

NIH achieves the right balance of security, compliance, and ease of use to protect staff and intellectual property.

2

Reduce Complexity and Increase Efficiency

NIH procures the services it needs so our institutes and centers don't need to recreate or reproduce those capabilities.

3

Provide Transparent and Intuitive Experience

People get the access they need and expect in ways they understand and can use.

By the Numbers | Identity & Access Management

The metrics below demonstrate the impact our services have on the NIH community.

40K+	**Simplifies the login experience for all 40K+NIH staff members**
1 million	**Processes more than 1 million authentication requests per month for external and federated researchers and collaborators**
27	**Supports all 27 NIH Institutes and Centers to conduct day-to-day business and meet program goals and objectives**
24x7x365	**Provides 24x7x365 support to ensure robust operations of enterprise IT services and systems**
196	**Streamlines the login experience for grantees at 150+ extramural institutions**
38%	**Self-service capabilities - reduces the rate of password changes requiring a call to the Service Desk by 38%**
11K+	**Provides 11K+ members of the NIH community with a backup login mechanism**
400+	**Improves the security of 400+ public-facing NIH sites and applications by enabling MFA**

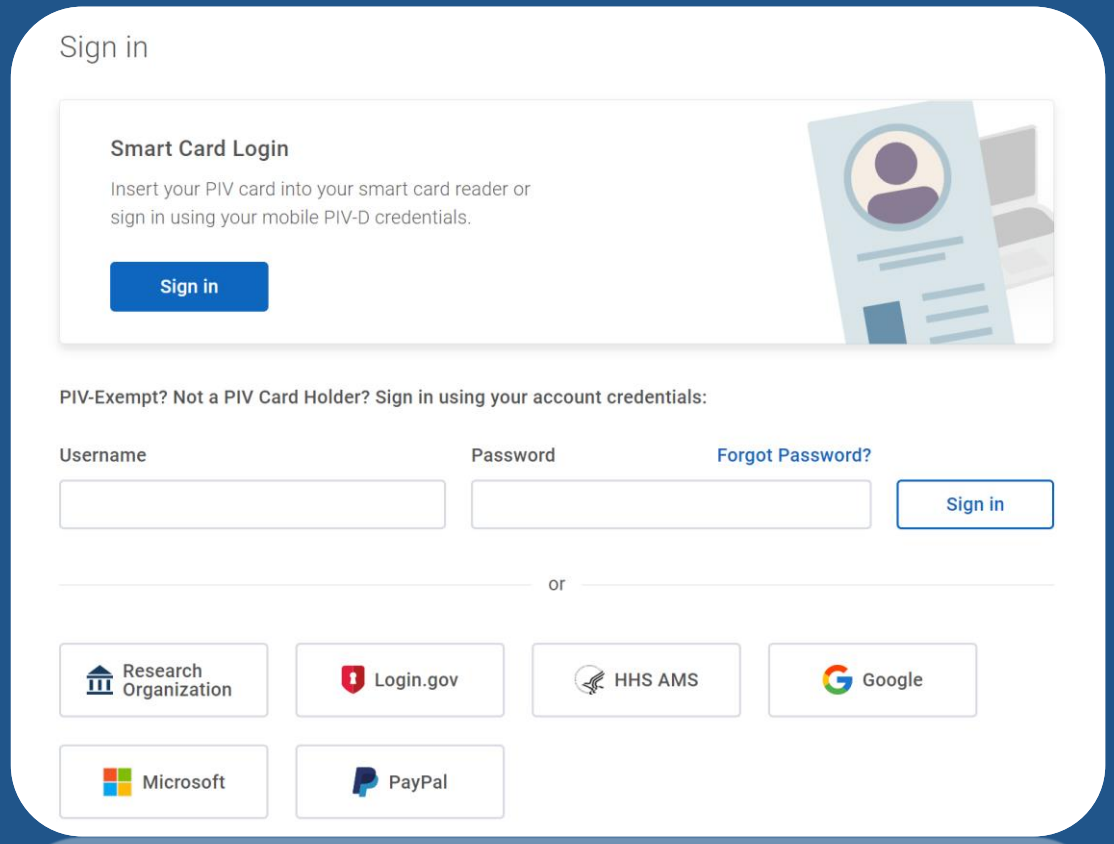
IAM SERVICES

IAM Services Spotlight:
NIH Login &
Researcher Auth Service (RAS) Services

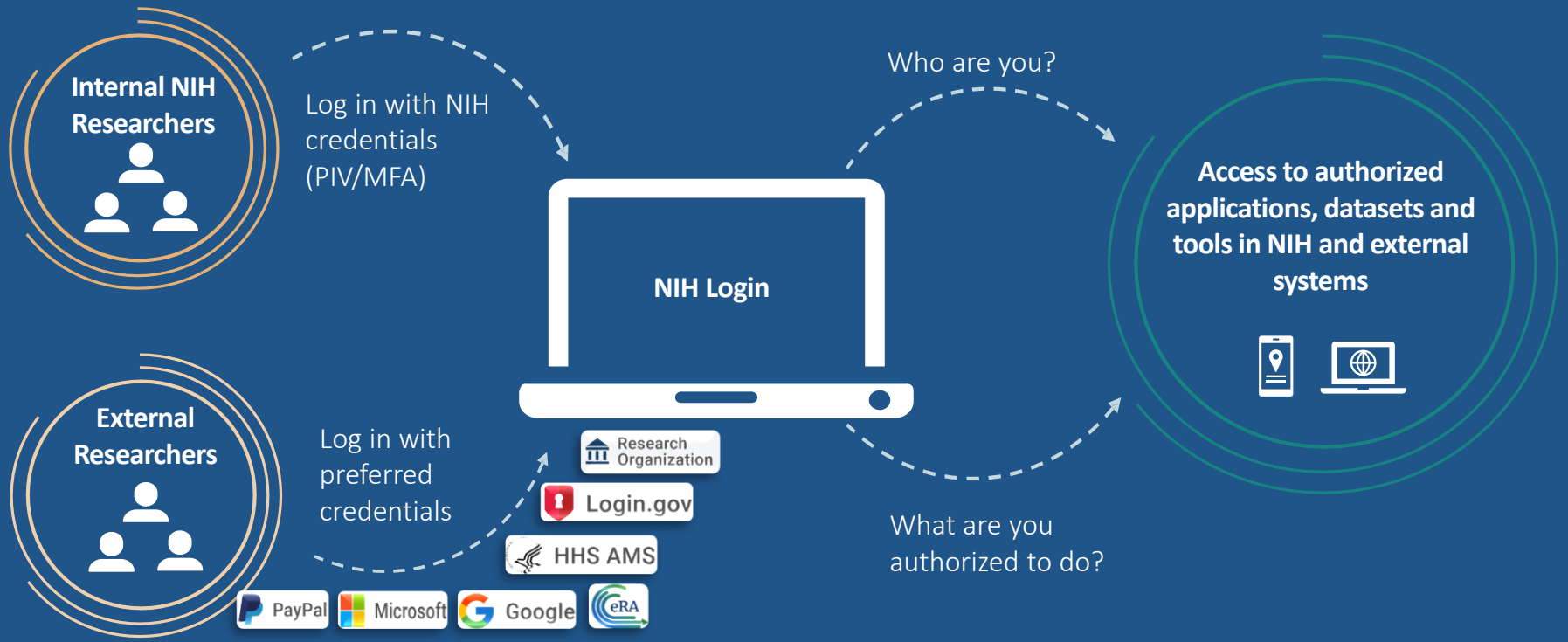
What is NIH Login Service?

The National Institutes of Health (NIH) Login Solution is an NIH Identity and Access Management service offered by the Center for Information Technology (CIT) to **provide centralized authentication and Single Sign On (SSO) capability for web-based applications**.

The NIH Login is a **"one-stop shop" which allows logins** from all of NIH staff, Electronic Research Administration (eRA) Commons, Department of Health and Human Services (HHS) employees, and various federated partners.



NIH Login | Identity & Access Management



Researcher signs in with preferred credentials

Researcher has option to link and manage their identities in RAS

Enforced multi-factor authentication for platforms that require a higher level of assurance

Authorizations based on NIH Data Access Committee decisions are provided to partner systems

What is RAS Service?

NIH Researcher Auth Service (RAS) is a unified, efficient, and secure authentication and authorization service that enables streamlined access by researchers to NIH-funded data resources across multiple systems and provides standardized methods of logging and auditing such access.

With RAS Service, **researchers can log in once** and then have their appropriate authentication and authorization information travel with them as they move between platforms.

NIH Center for Information Technology

RAS Service | Identity & Access Management

CUSTOMER PAIN POINTS

- Researchers login with duplicative credentials or provide consent to share their personal information **multiple times** to access data located in different cloud environment. It takes weeks to reflect user's access to data in distributed systems, thereby prolonging research to months
- Researchers do not have a unified authentication experience
- Lack of federated audit framework to monitor user activities across distributed data ecosystem
- Lack of dynamic method to capture and transmit authorization decisions
- Researchers cannot link their university credentials to access NIH data ecosystem
- No secure way for authorization permission and audit activities to be federated
- Cloud compute charge back model to researching institutes for NIH data ecosystem access

ENTERPRISE SOLUTION USING VARIOUS INDUSTRY STANDARDS

OAuth/OIDC	NIST	GA4GH	Data Privacy
✓ **Authorization Code Flow (B2C use-case)** ✓ **Client Credential Grant Type (B2B use-case)**	✓ **Privacy Framework** ✓ **800-53 Security Controls** ✓ **800-57 Part 1 Key Management** ✓ **800-63-3 Digital Identity Guidelines**	✓ **Authentication and Authorization Infrastructure** ✓ **Passports and Visas** Abiding to GA4GH, the product can contribute to and integrate into an international data ecosystem Allows researchers to run long-term analyses without re-authenticating	✓ **Consent Management** ✓ **NIH Privacy Policy** ✓ **M-10-22** Ensures there is an accurate level of protection involving the collection, use, and cross-border sharing of people's personal data

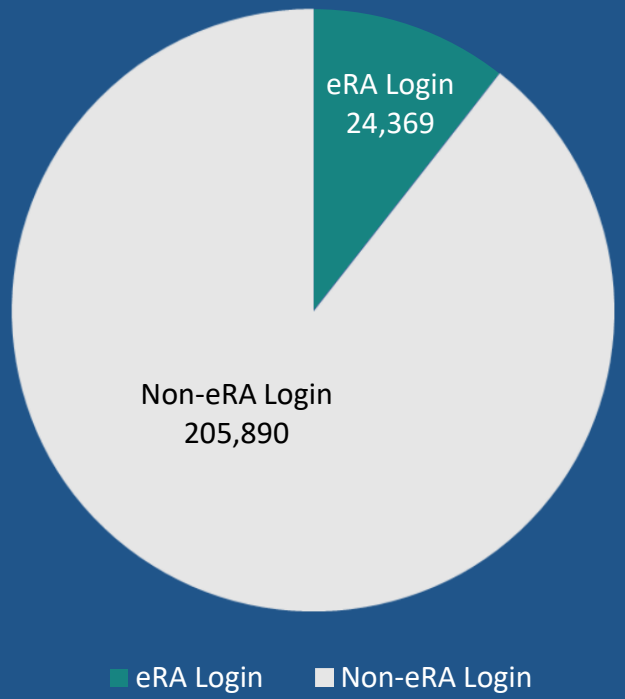
OpenID · NIST National Institute of Standards and Technology U.S. Department of Commerce · Global Alliance for Genomics & Health Collaborate. Innovate. Accelerate. · General Data Protection Regulation

CIT SERVICES

Federated Logins

eRA Login vs Non-eRA Login

Total Number of Unique Logins Between May – November 2022



196

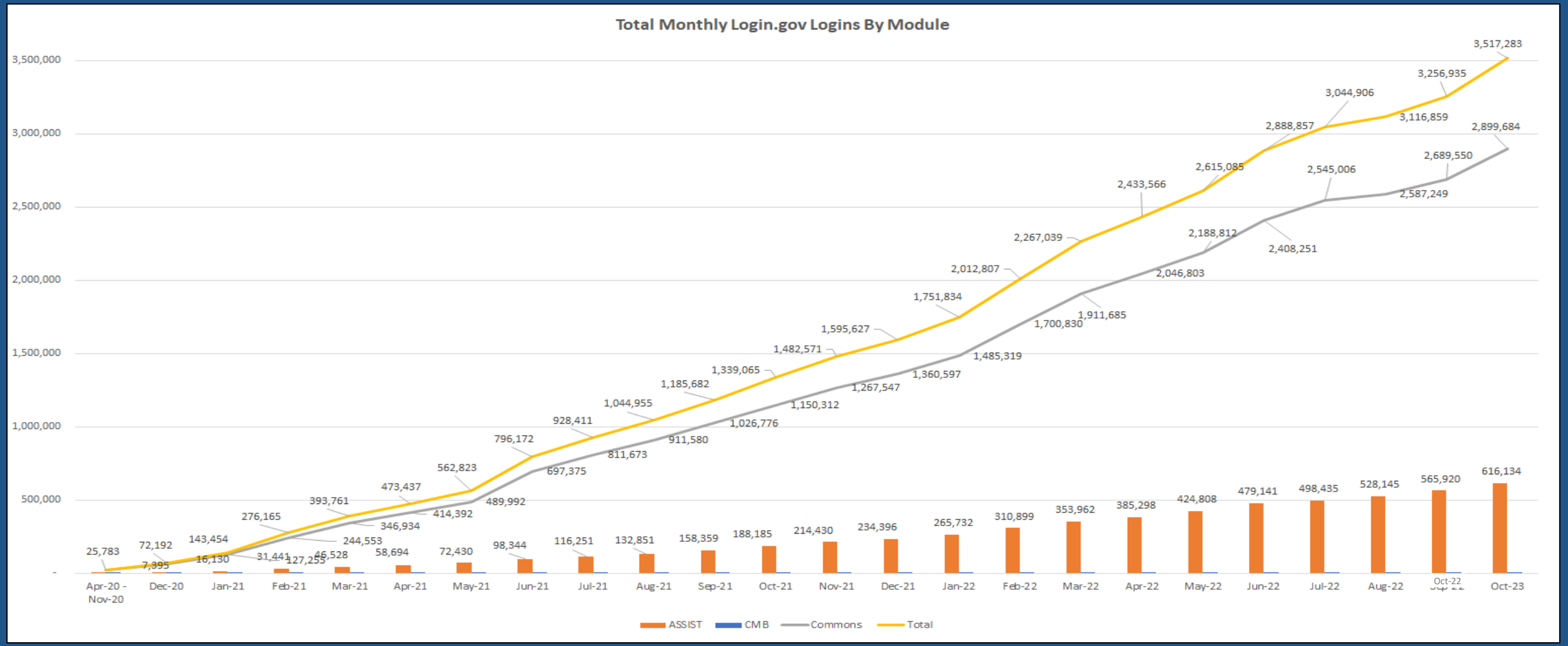
FEDERATED ENTITIES HAVE SUPPORTED THE REFEDS MFA PROFILE FOR eRA

1,350

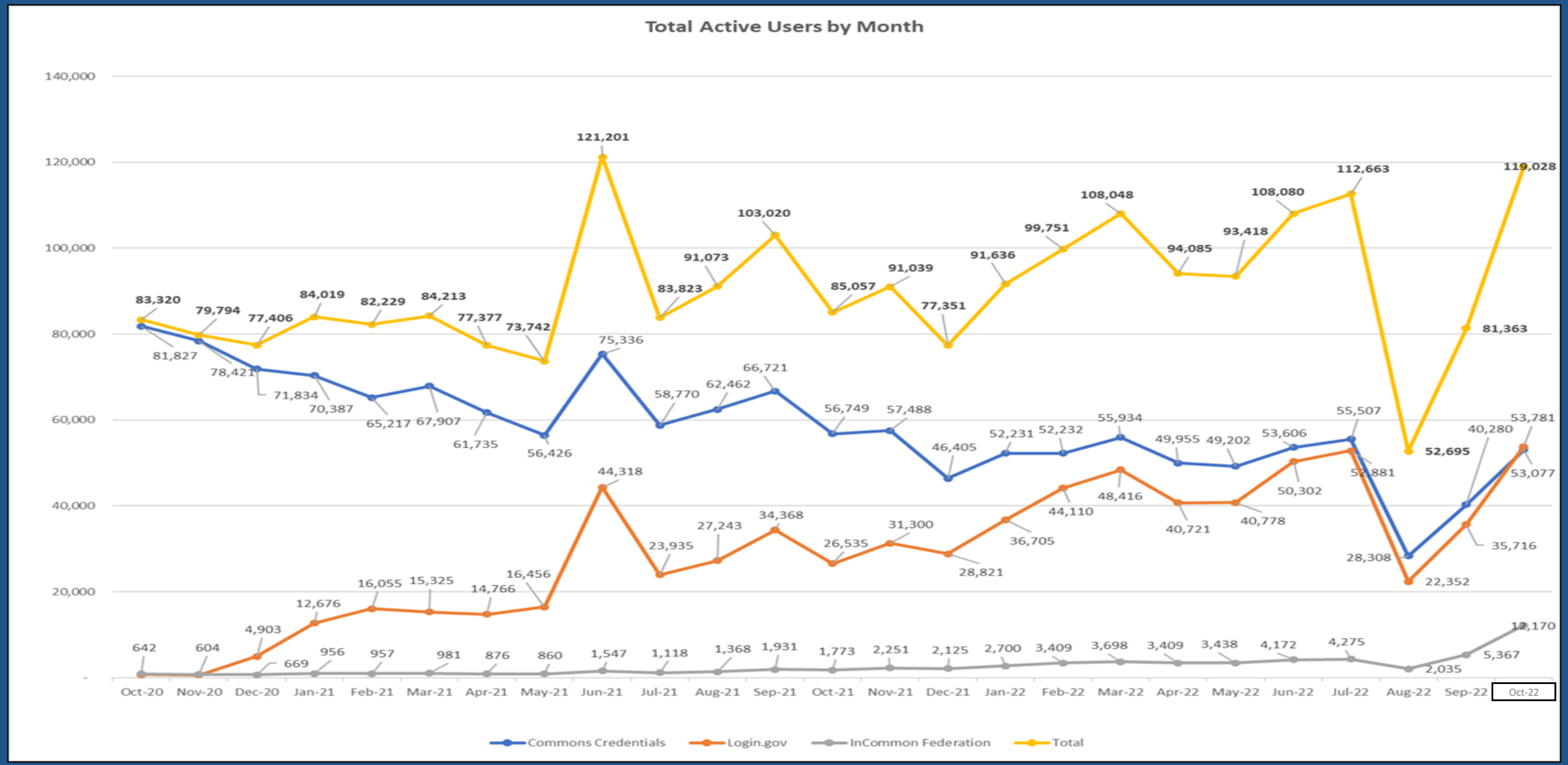
FEDERATED ENTITIES HAVE LOGGED IN TO NON-eRA APPLICATIONS WITH SINGLE FACTOR AUTHENTICATION

Key Takeaway: Federated partners should prepare to implement MFA and response signaling using the REFEDS MFA Profile

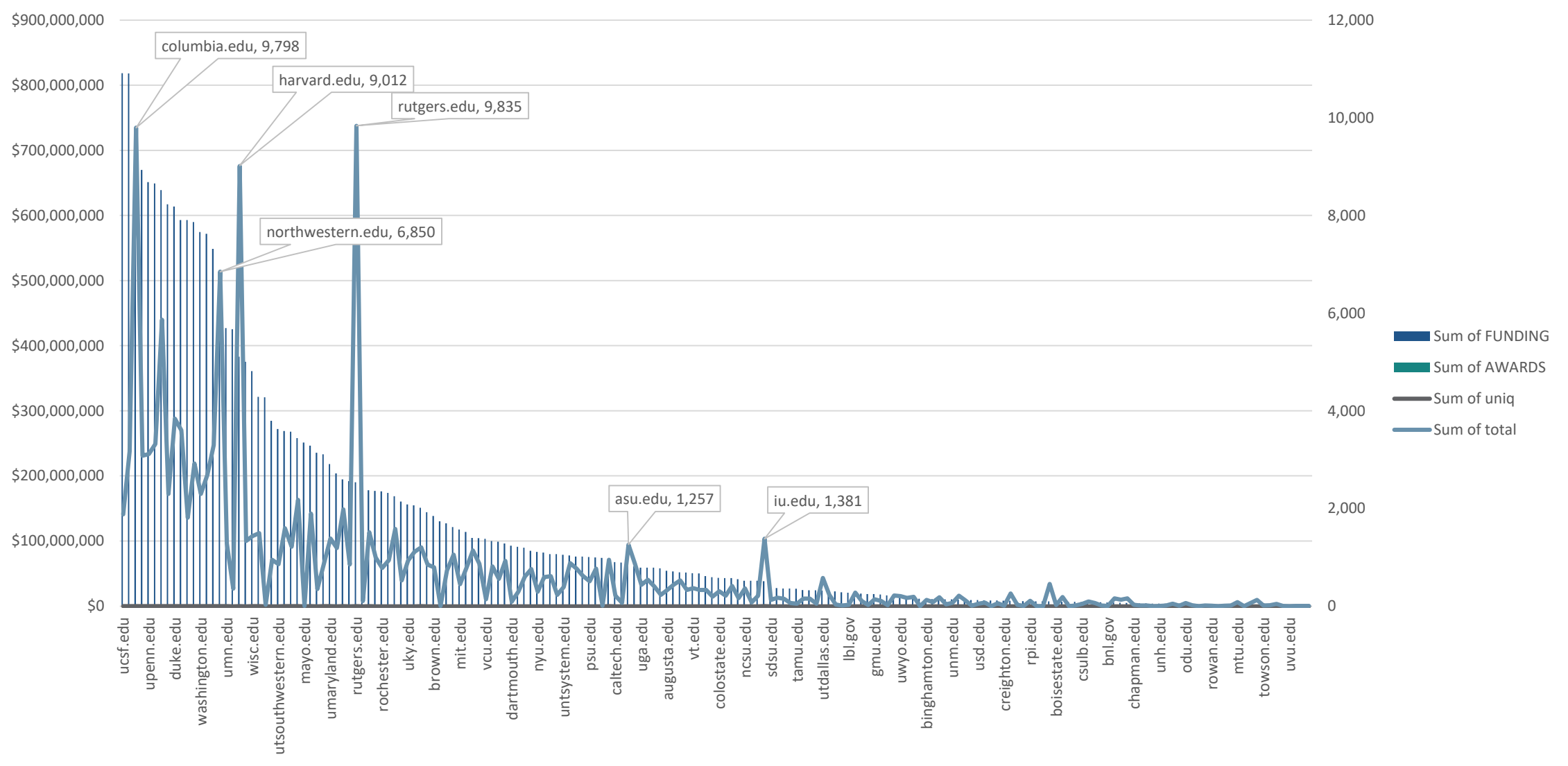
Federated logins to eRA with Login.gov



Federated logins to eRA with different credentials



Federated MFA logins to eRA relative to funding



Current challenges with federated MFA

- Must have:
  - Identity Assurance & Authenticator Assurance
    - Increasing adoption of federated identity assurance + federated phishing-resistant MFA
  - Organizational affiliation
- Constraints
  - Cost (ours and yours)

CIT SERVICES

Contact | Identity & Access Management

For more information about CIT's Identity & Access Management offerings, contact NIHLoginSupport@mail.nih.gov or visit https://auth.nih.gov

Questions?