National Institute of Allergy and Infectious Diseases

Internet2 Community Exchange

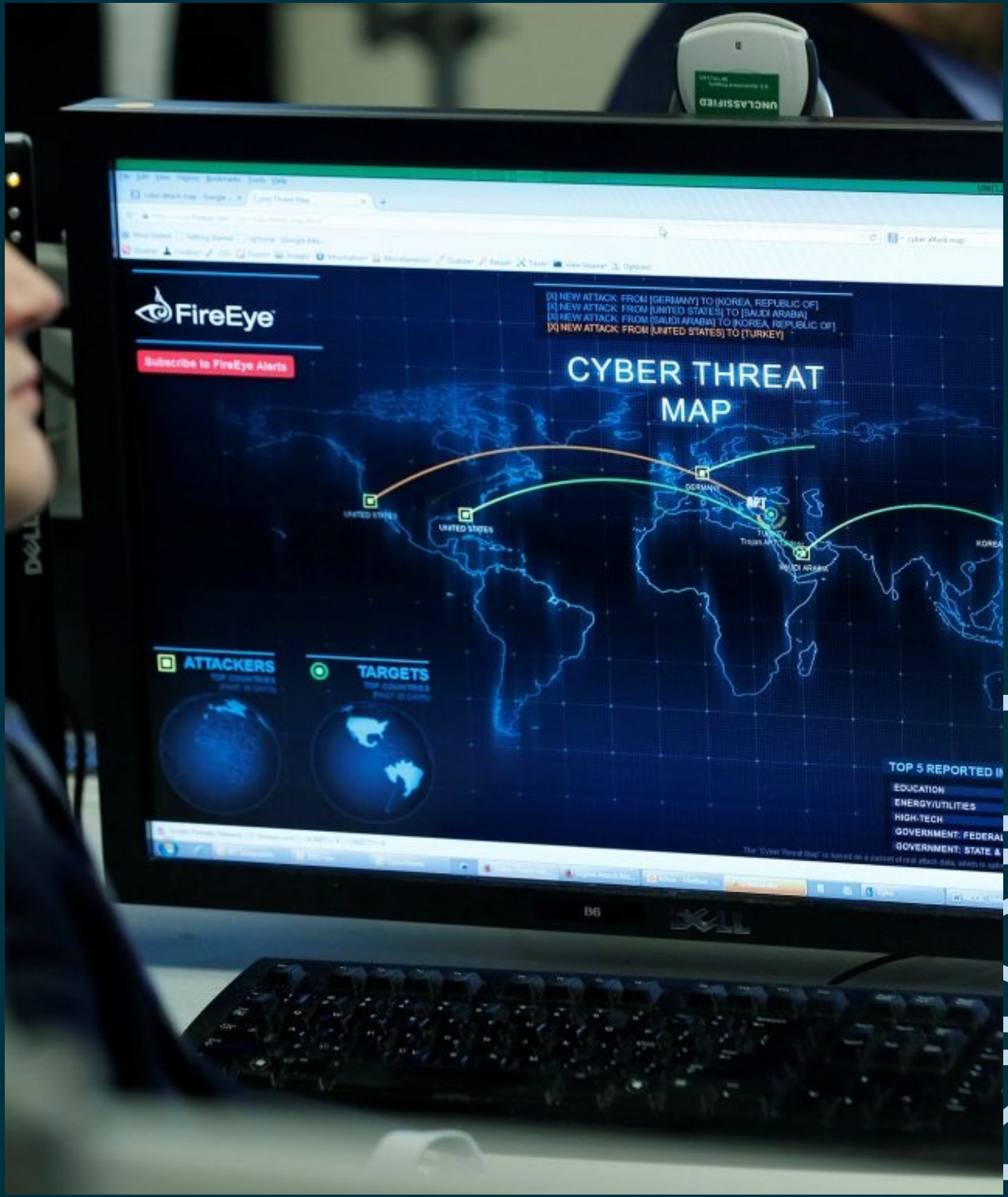
Federation Mindedness in Cybersecurity Incident Response

May 2023

Michael Tartakovsky
Chief Information Officer & Director
Office of Cyber Infrastructure & Computational Biology

The Ongoing War in Cyberspace: Chilling Impact On Research

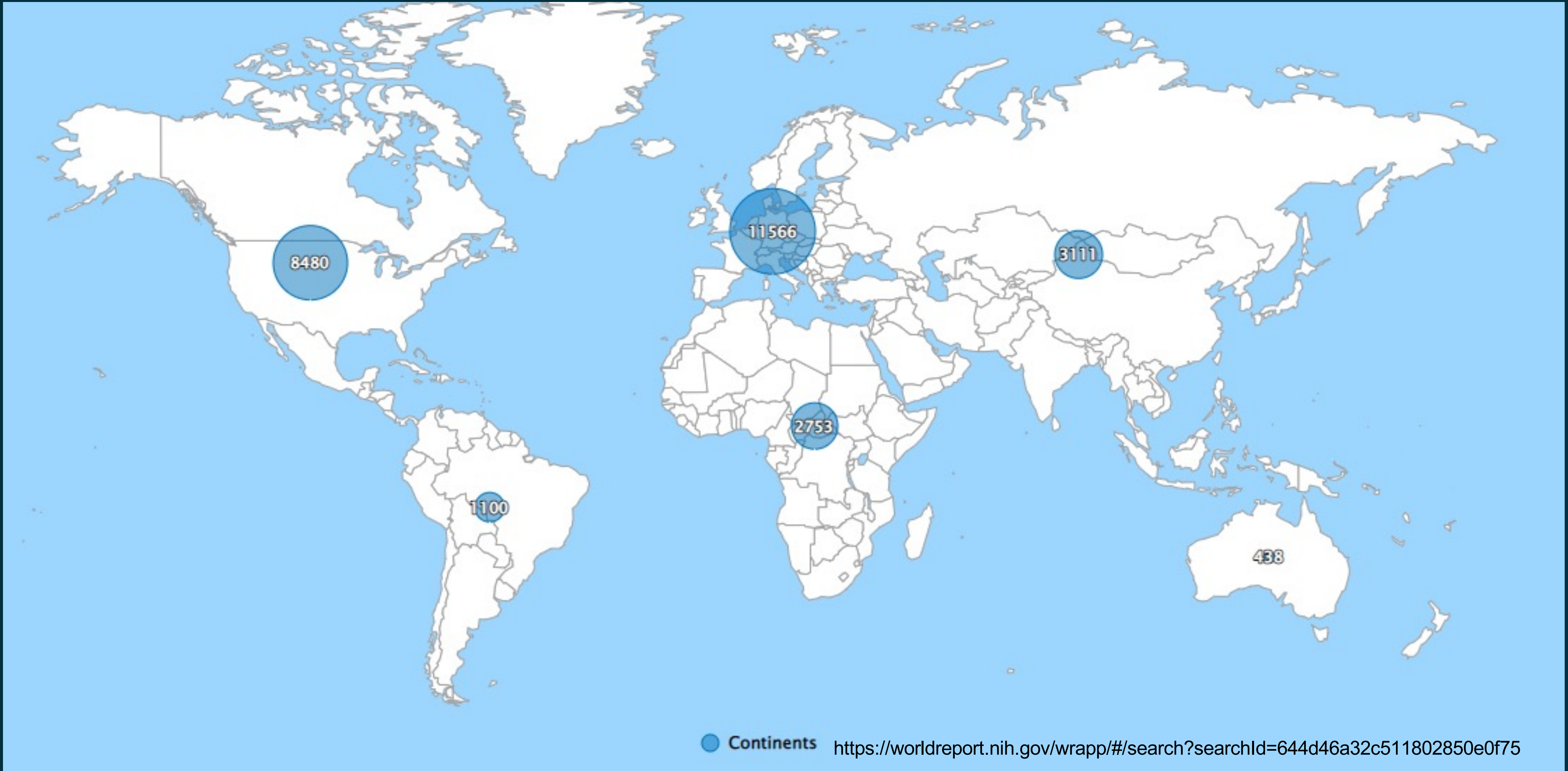
Cyber warfare is a growing threat to research and development, as malicious actors seek to disrupt and steal valuable data. Cyber security experts are working hard to protect research from these attacks.



NIH National Institutes of Health

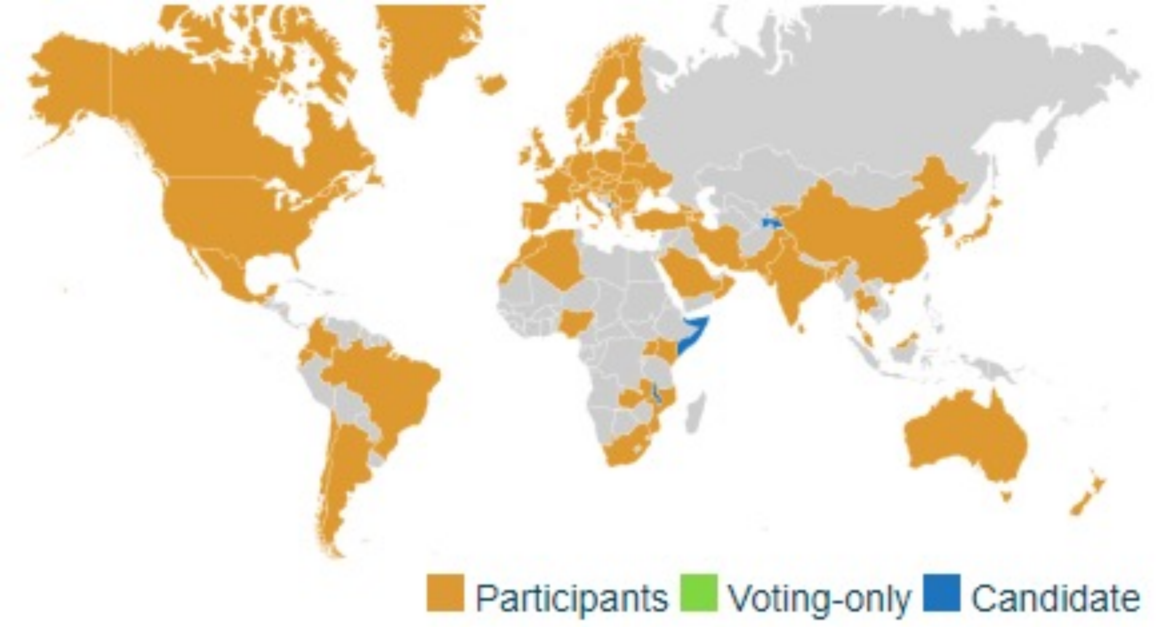
NIAID

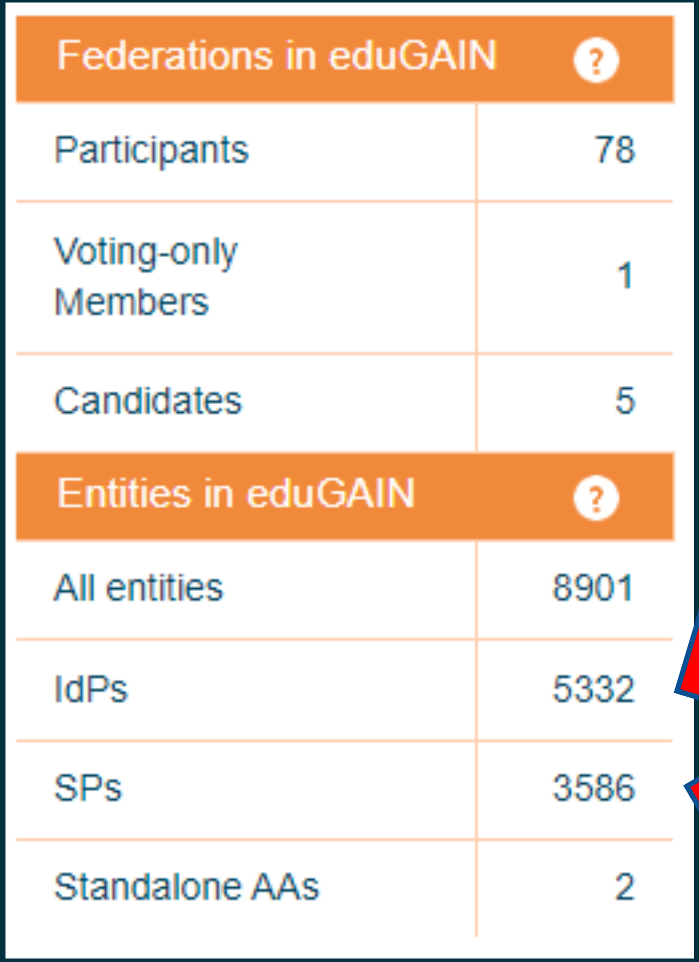
NIH is part of a big community = 27,448 Research Orgs



https://worldreport.nih.gov/wrapp/#/search?searchId=644d46a32c511802850e0f75

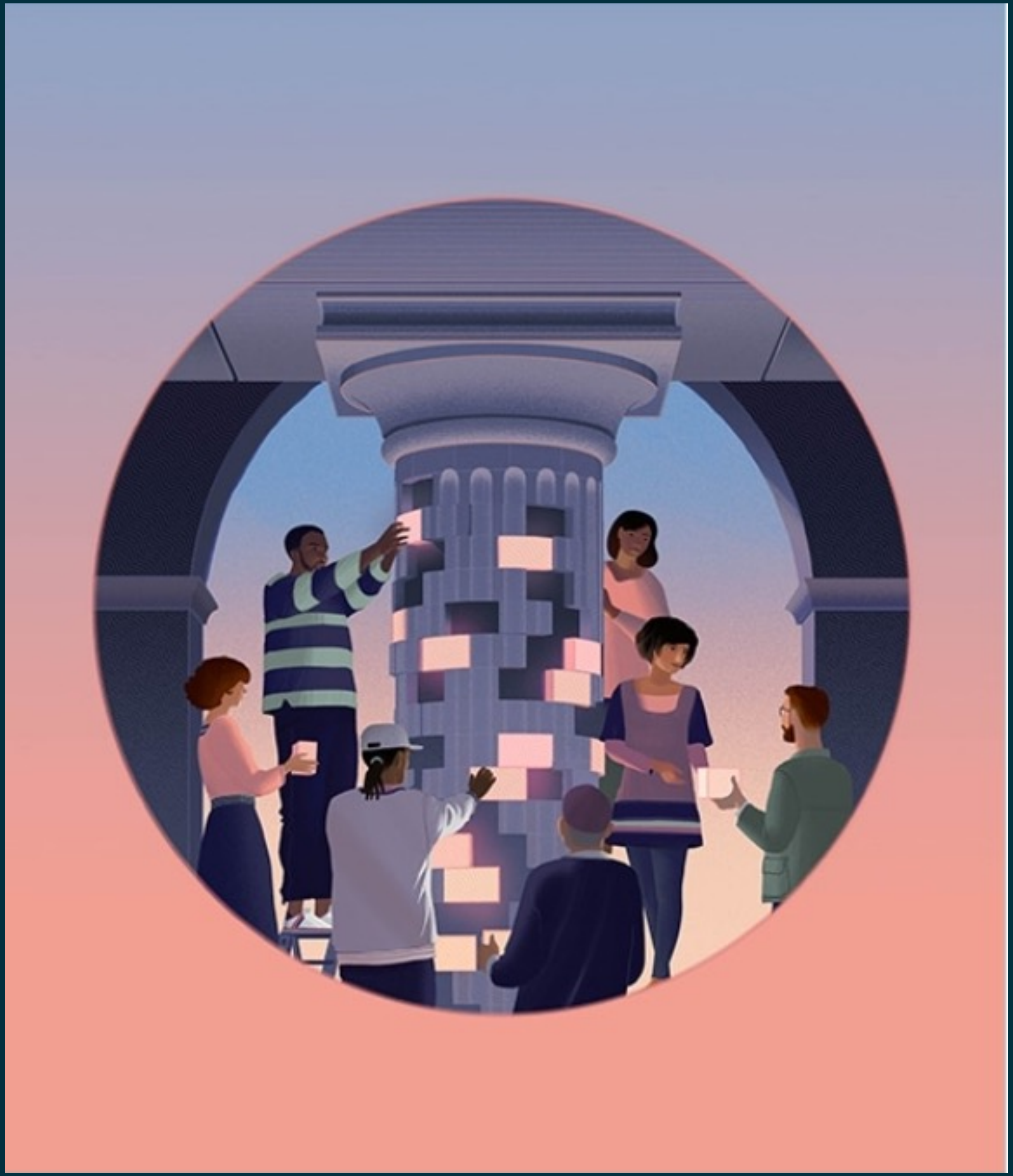
How can federation members trust each other?





Federations in eduGAIN ?	
Participants	78
Voting-only Members	1
Candidates	5

Entities in eduGAIN ?	
All entities	8901
IdPs	5332
SPs	3586
Standalone AAs	2



Building Trust Without Audits

Trust between institutions is essential for successful collaborations and partnerships. Without audits, it can be difficult to ensure that trust is maintained.

Audit frameworks don’t scale globally for R&E

NIH National Institutes of Health

NIAID

The Psychological Experience of *Tabletop Exercises*: Boosting Receptivity and Increasing Empathy

Wargaming is a powerful tool for developing empathy and receptivity to new ideas. Through its immersive stories and engaging gameplay, players are able to gain a unique perspective on the world around them.

NIH National Institutes of Health

NIAID

P. P. Perla, E. D. Mc Grady, WHY WARGAMING WORKS, (available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a619256.pdf).

Building Trust Through Exercises

Team Building Exercises

Team building exercises are activities that help build trust and collaboration among team members.

Trust Falls

Trust falls are a popular team building exercise that involves one person falling backward into the arms of their teammates.

Icebreakers

Icebreakers are activities that help people get to know each other better and build trust.

Group Discussions

Group discussions are a great way to build trust by allowing everyone to share their thoughts and ideas.

NIH National Institutes of Health

NIAID

Changing Our Incident Response Culture for Multilateral Cooperation

Steps	Benefits
Create a multilateral incident response team	Increased collaboration and communication between teams
Develop a shared understanding of incident response processes	Improved response times and accuracy
Establish a culture of learning and improvement	More effective responses to future incidents

NIH National Institutes of Health

NIAID

*Adapted from 'Creating a Multilateral Incident Response Culture' by the SANS Institute

Changing Our Incident Response Culture for Multilateral Cooperation

NIAID Tested Internally first

- How do you validate credentials of other institution’s IRT?
- How do you separate the valid IRT messages from the noise?

- Following Traffic Light Protocol for sharing data required exercise facilitator intervention

- Revealed need for routine refresher training and more practice – particularly to address turnover!
  → we need to change our security response culture to include a federation mindedness

- Practice across the federation and the global federated community

2022 InCommon Exercise revealed similar observations

Phase 1 – 19-23 Sep
Communications Test

Some security contact info out of date or not working.
Takeaway: Organizations need routine self checks.

Phase 2 – 14-22 Oct
Participating Organization
Exercise Training

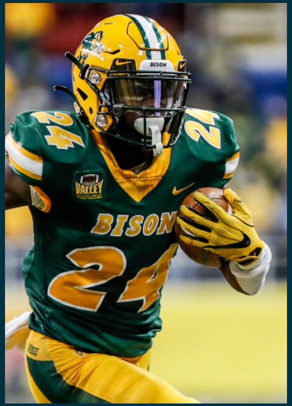
Uneven ability to validate security contacts in metadata.
Takeaway: Security response teams need refresher training.

Phase 3 – 14-18 Nov
Distributed Tabletop
Exercise

Security team and IAM teams not always integrated. Some security response teams not aware of Sirtfi procedures/federation context.
Takeaway: Need more practice to ensure security teams familiar Sirtfi's expectations and InCommon federation.

Who Showed Up (2022)

CA Poly State University-San Luis Obispo



North Dakota State University

Rice University

University of Illinois

NIH National Institute of Allergy and Infectious Diseases

NIH National Institutes of Health

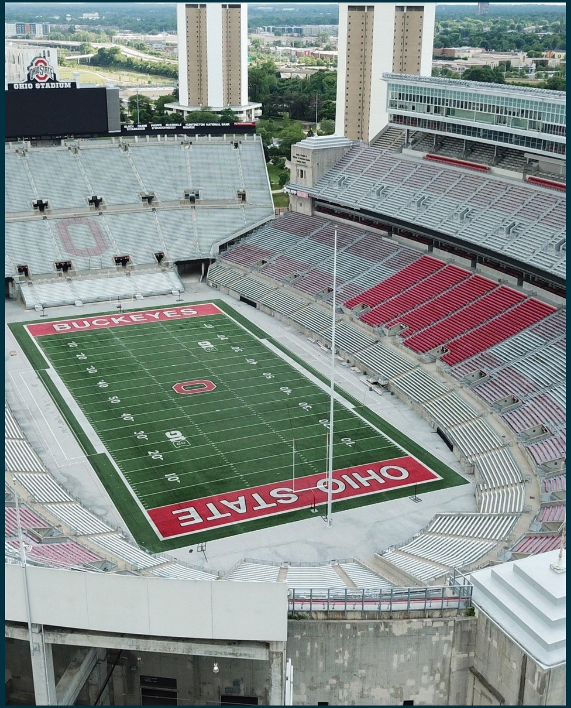
OCLC

CILogon

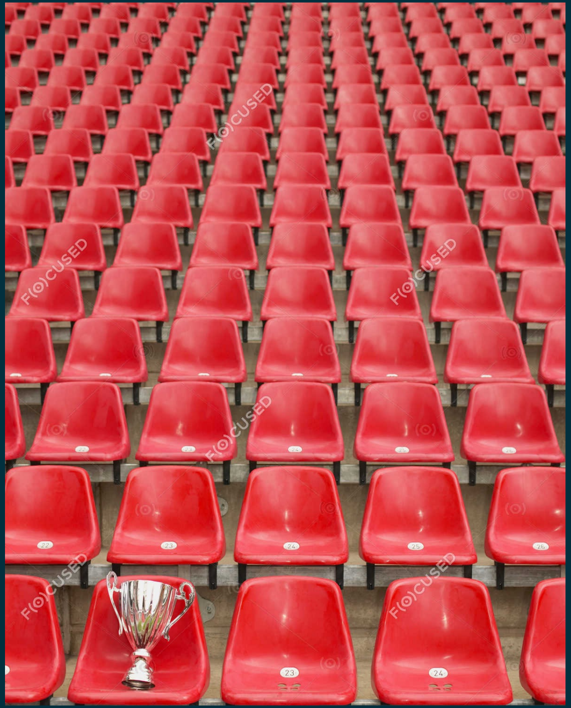
NON SOLUS ELSEVIER

LIGO

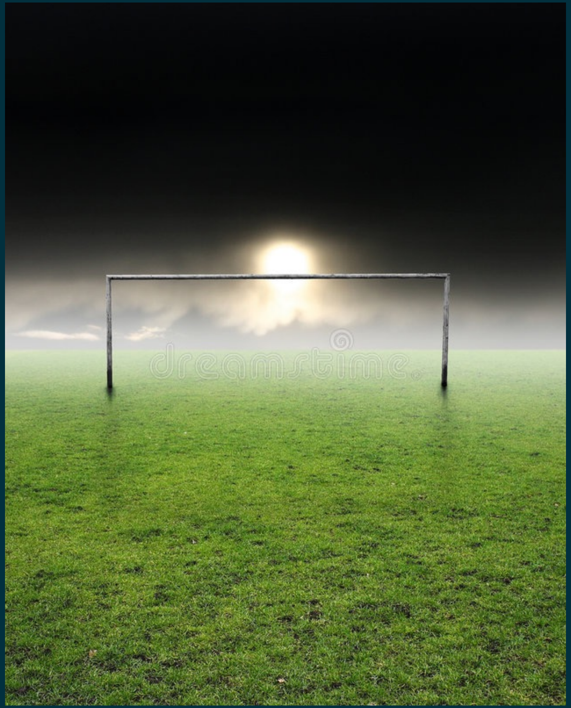
Where is Everyone?



United States
146 Universities are
“R1”



United States
133 Universities are
"R2”



Global
1797 R&S IdPs in 50
federations

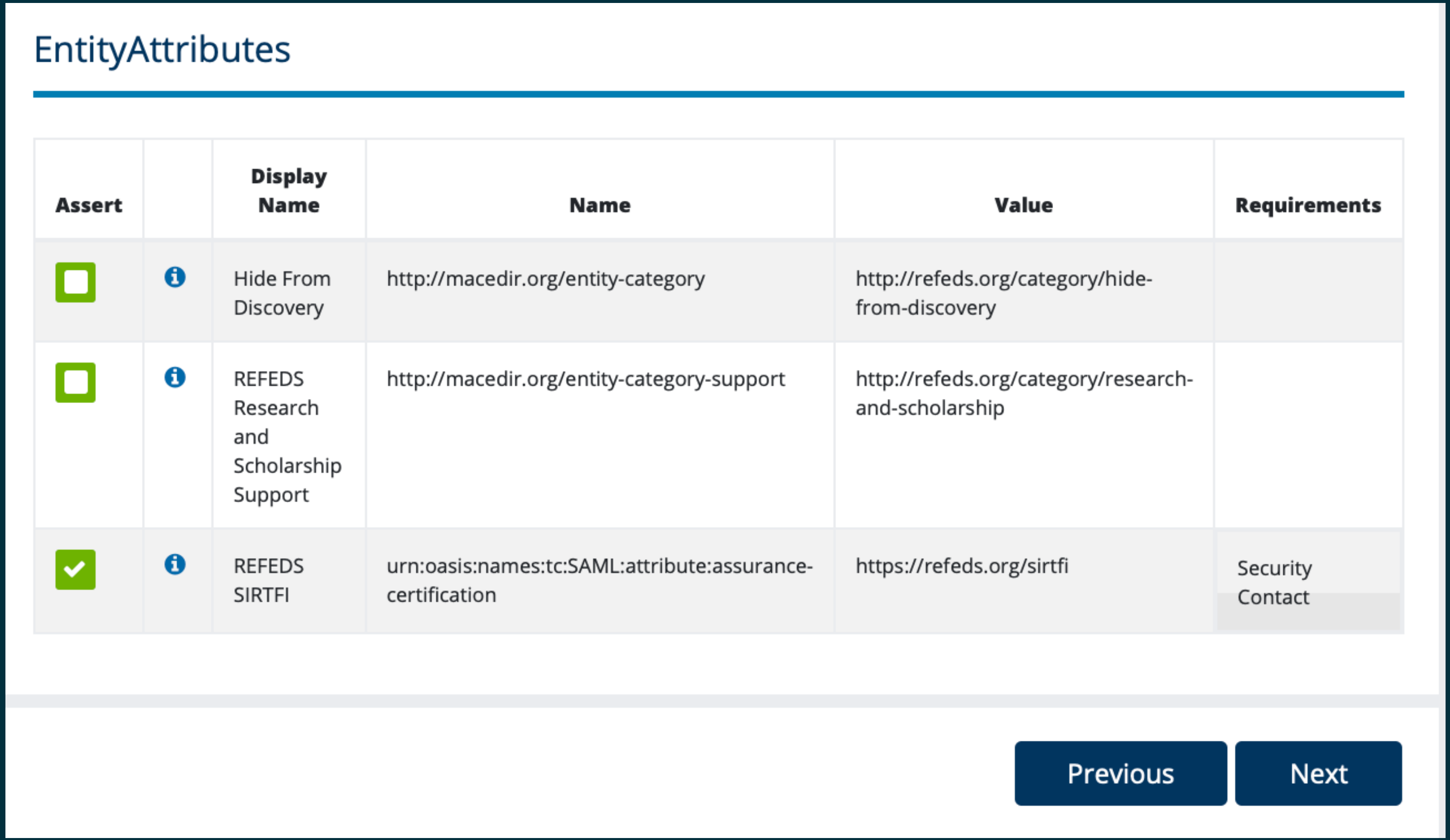
Global
349 R&S SPs in 30
federations

Only 10 showed up!!

NIH National Institutes of Health

NIAID

REFEDS Sirtfi, US InCommon your staff checked the box...



EntityAttributes

Assert		Display Name	Name	Value	Requirements
□	ℹ	Hide From Discovery	http://macedir.org/entity-category	http://refeds.org/category/hide-from-discovery	
□	ℹ	REFEDS Research and Scholarship Support	http://macedir.org/entity-category-support	http://refeds.org/category/research-and-scholarship	
☑	ℹ	REFEDS SIRTFI	urn:oasis:names:tc:SAML:attribute:assurance-certification	https://refeds.org/sirtfi	Security Contact

Are you ready?

NIH National Institutes of Health

NIAID

In Summary

- Science needs better credentials
- Your researchers and students need more robust credentials to use tools at the NIH and at other research orgs
- Credentials aren’t enough you need to participate in the incident response exercises
- InCommon is planning 2023 events – look for the call to participate this Summer for a November exercise.

NIH National Institutes of Health

NIAID

Thank You!

Questions and feedback can be directed to
Mike Tartakovsky

MTARTAKOVS@niaid.nih.gov

Acknowledgements

2022 Sirtfi Exercise Planning Working Group, Core Team

- Kyle Lewis, Prabha Manda, Tom Barton, Mark Baumgartner,
  Jon Vasquez, Jim Basney, Ercan Elibol

2022 Tabletop Exercise Participating Organizations

1. CA Poly State University-San Luis Obispo
2. CILogon
3. Elsevier
4. Laser Interferometer Gravitational-Wave Observatory (LIGO)
5. National Institute of Allergy and Infectious Diseases (NIAID)
6. National Institutes of Health (NIH)
7. North Dakota State University (NDSU)
8. Online Computer Library Center Inc (OCLC)
9. Rice University
10. University of Illinois