Getting Ready: Institutional Benchmarking Covering Topics of Interest in Research Security

February 26, 2025

Speakers:

#COGRFeb25

Allen DiPalma, Executive Director, Office of Research Security & Trade Compliance, (University of Pittsburgh)

Jennifer Donais, Assistant Vice President of Research Integrity and Compliance, (Chapman University)

Tam Dao, Assistant Vice President for Research Security, (Rice University)

Thomas Burns, Associate Dean for Research Affairs, (Johns Hopkins University)

Moderator:

Krystal Toups, Director, Contracts and Grants Administration (COGR)

COGR

Agenda

- Framing of Research Security and Cybersecurity Requirements
- Implementing Research Security in an ERI
- Perspectives on NSF Research Security Training Modules
- NIH Implementation Update for Data Management and Access Practices Under the Genomic Data Sharing Policy
- Panel Discussion and Live Poll Questions
- Q&A

University of Pittsburgh

Overview of Research Security and Cybersecurity Requirements

Allen DiPalma

Executive Director

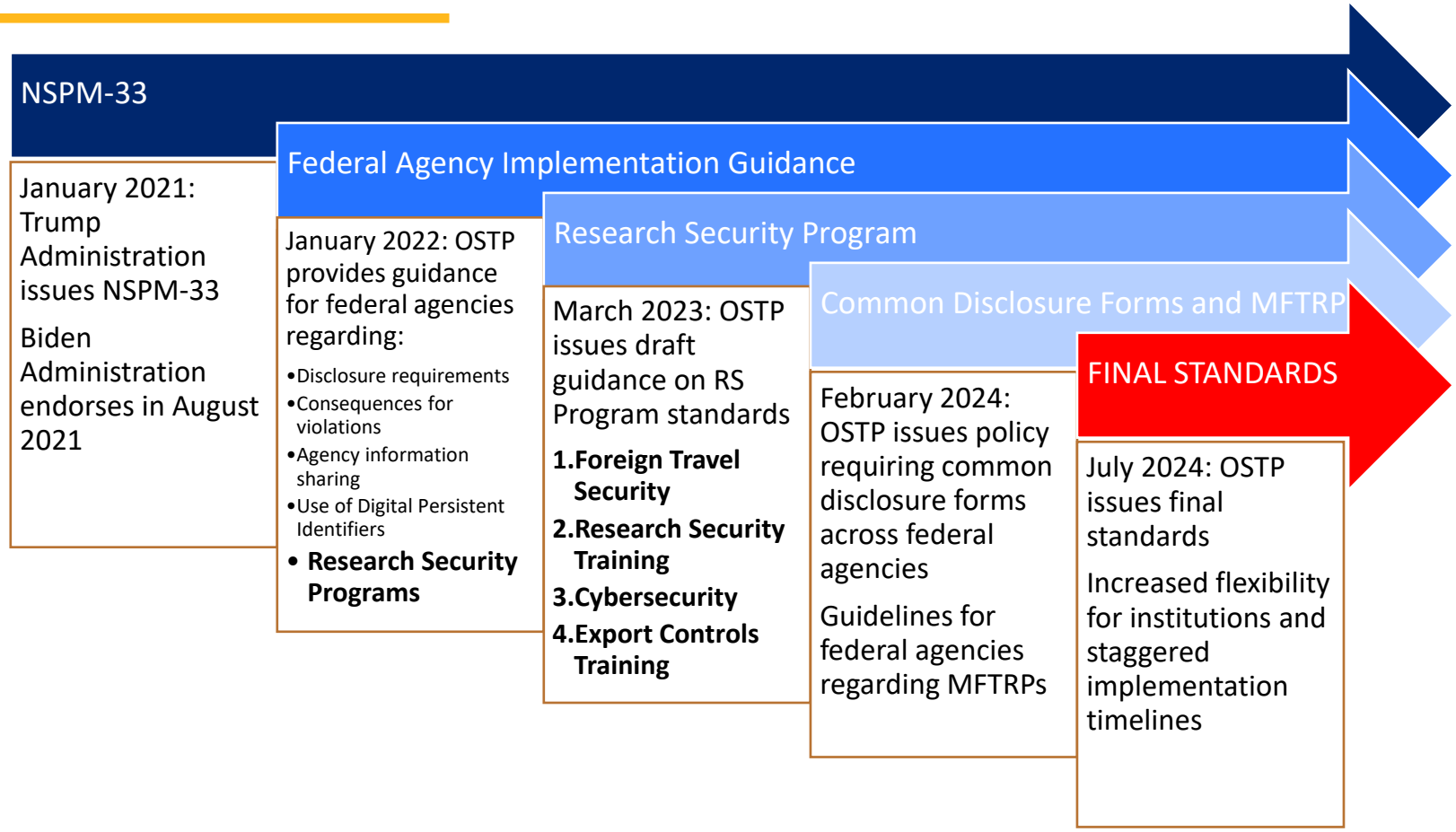
Office of Research Security & Trade Compliance

University of Pittsburgh Institutional Profile

- Private State Affiliated University in Pennsylvania founded in 1787
- 747 Degrees and Certificate Programs offered among its 5 campuses
- Over 10,700 degrees and certificates issued in 2024
- Undergrad Students = 24,570; Grad Students = 9,509
- Full-Time Faculty = 5,333
- Strong Biomedical Focus: Medical firsts include first polio vaccine and heart liver transplant
- FY 2024 research expenditures = $1.2 billion
- Fundamental Research supported by Policy
- Long-standing Openness in Research Statement

University of Pittsburgh

National Security Presidential Memorandum 33 (NSPM-33)



University of Pittsburgh

Research Security Program Implementation Timeline

July 9, 2024

OSTP releases a memo to the heads of federal research agencies entitled "Final Guidelines for Research Security Programs at Covered Institutions"

January 8, 2025

Within six (6) months of the date of the OSTP memo, federal agencies shall submit to OSTP and OMB plans for updating policies to ensure the guidance is reflected in the Research Security Programs Standard Requirements of each federal agency.

January 2025 – July 2025

Federal agencies shall implement updated policies no later than six (6) months after finalized plans have been submitted to OSTP and OMB.

January 2025 – July 2026

Covered Institutions shall have no more than eighteen (18) months after the effective date of federal agency plans to implement the requirements of the OSTP Research Security Program Requirements memo.

University of Pittsburgh

NSPM-33 & Cybersecurity

From 07/09/2024 OSTP Memo For the Heads of Federal Research Agencies

- "As the first element of the standardized requirement, federal research agencies shall require institutions of higher education to certify that the institution will implement a cybersecurity program consistent with the cybersecurity resource for research institutions described in the CHIPS and Science Act within one year after the National Institute of Standards and Technology (NIST) of the Department of Commerce publishes that resource."

- "For covered institutions that are not institutions of higher education, federal research agencies shall require covered institutions to certify that the institution will implement a cybersecurity program consistent with another relevant cybersecurity resource maintained by NIST or another federal research agency."

University of Pittsburgh

NSPM-33 Cybersecurity Requirements from 2022 NSPM 33 Implementation Guidance

System access	Network connectivity	Malicious code	Other
• Control system access by user, device (#1) • Control system access to transactions, functions (#2) • Identify accounts acting on behalf of users, devices (#5) • Verify identities of user accounts (#6)	• Control connections to and use of external systems (#3) • Monitor, control network connections (#7) • Separate network connections for public systems (#8)	• Protect from malicious code, software (#10) • Update malicious code protections timely (#11) • Scan systems and files for malicious code (#12)	• Control non-public on public systems (#4) • Correct system flaws, vulnerabilities timely (#9)

University of Pittsburgh

While We Wait… There are Some Clues

Similar Baseline Cybersecurity Requirements Currently Appear in:

- NSTC Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33)
- FAR Clause 52.204-21 “Basic Safeguarding of Covered Contractor Information Systems”
- DOD Cybersecurity Maturity Model Certification (CMMC) Level 1

Programs that Require Enhanced Cybersecurity Requirements through NIST SP 800-171

- Controlled Unclassified Information (CUI) Program Rules
- DOD Cybersecurity Maturity Model Certification (CMMC) Level 2
- NIH Controlled Access Genomic Data

Cybersecurity Challenges & Thoughts

- Cost of implementation across differing institutional frameworks.
- Data ownership and the requirement to save data to an institutionally managed system.
- Personal device access to institutional data and systems.
- Possible cybersecurity standard variations among federal agencies.
- Overall management of data and devices across campuses and research projects.

University of Pittsburgh

Research Security Training: Understanding the Overlap Between NSPM & CHIPS

Research Security Program (NSPM-33)	Research Security Training (CHIPS and NSPM-33)	Satisfying Requirements
• Applies to Covered Institutions: Research organizations awarded >$50M/year in total federal research funding must certify to a **research security program**	• Covered institutions are required to certify they have implemented a research security training program for all covered individuals listed on applications for federal R&D funding, whether they are employed by the institution • Includes subawards • Both CHIPS and NSPM-33 include different topic requirements	• Implement research security training; certify covered individuals have all completed this **<u>Two options:</u>** 1. NSF training modules 2. Non-federal training that covers (1) improper transfer of USG-supported R&D; (2) importance of international research and talent

University of Pittsburgh

Research Security Training: Topics Cited in NSPM & CHIPS

CHIPS and Science Act

- Cybersecurity
- Foreign influence risks
- Export control regulations
- Ensuring researchers are equipped to handle potential security challenges

NSPM-33

- Examples of illicit/illegal transfer of US government-supported R&D in the context of research, as described by federal agencies
- Importance of foreign contributions to US-based research, including attracting foreign talent to the US, as a core tenant of international leadership
- All CHIPS Act requirements

Research Security Training Challenges & Thoughts

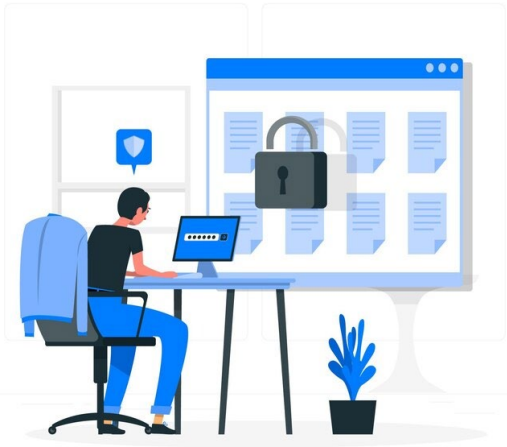
- Training Types: NSF Modules, Abridged NSF Modules, In-House Training, Third Party Training.
- Applicability of Training: Covered Personnel Only? Broader Applicability?
- Tracking Completion/Certifying Covered Personnel- how will you do that?
- Individual federal agency adoption and implementation.

University of Pittsburgh

Implementation of Research Security Requirements in an Emerging Research Institution

Jennifer A. Donais, MPA, CRA
Assistant Vice President for
Research Integrity & Compliance

CHAPMAN UNIVERSITY



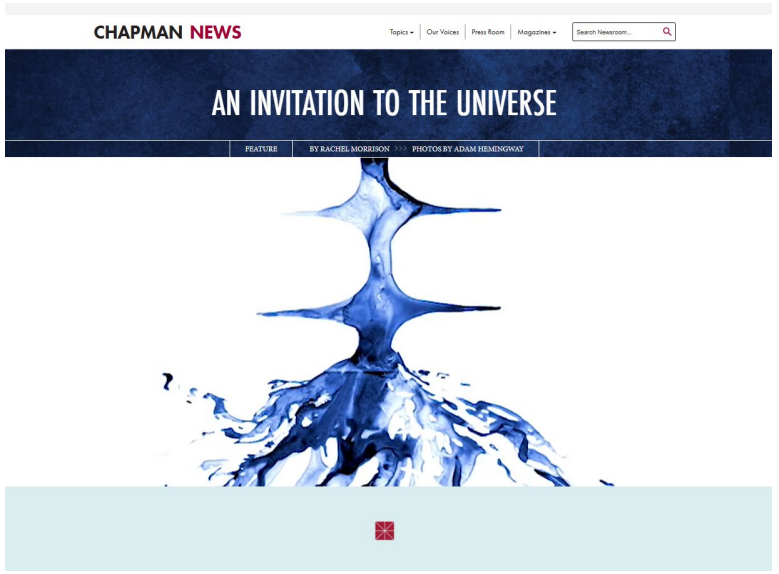
Introduction to Chapman University

- Achieved R2 status in 2018
- $42 million in R&D expenditures in FY2023 - $10 million in Federal
- 7 Doctoral programs (including computational/data science, education, physical therapy, health sciences, pharmacy, etc.)
- 57 Masters programs
- 2145 graduate students
- Diverse array of disciplines engaged in research, scholarly & creative activities
- Public & private sponsorship, including NIH, NSF, DOE, DOD, foundations, CA state, etc.

Chapman is known for…

Annual Economic Forecast

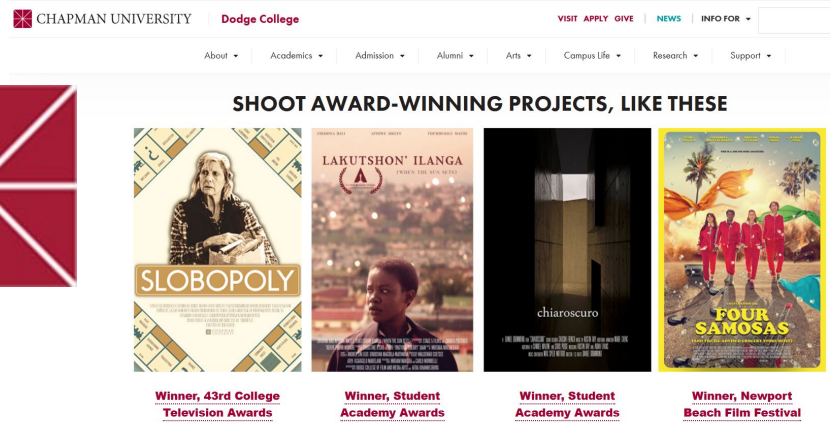
[Economic Forecast | Chapman University]



Art intersecting science

[LIA HALLORAN]

[Dodge College of Film & Media Arts]

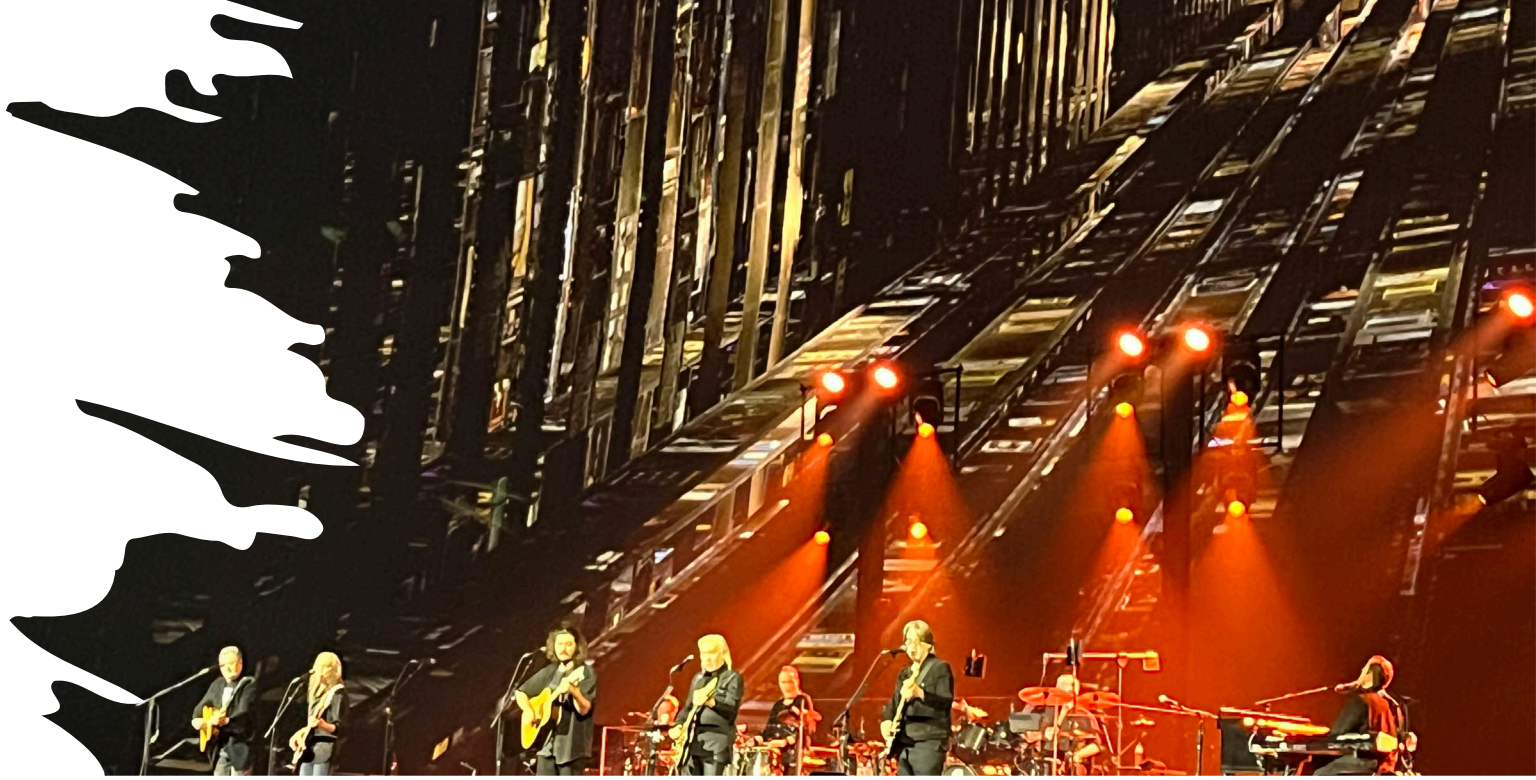


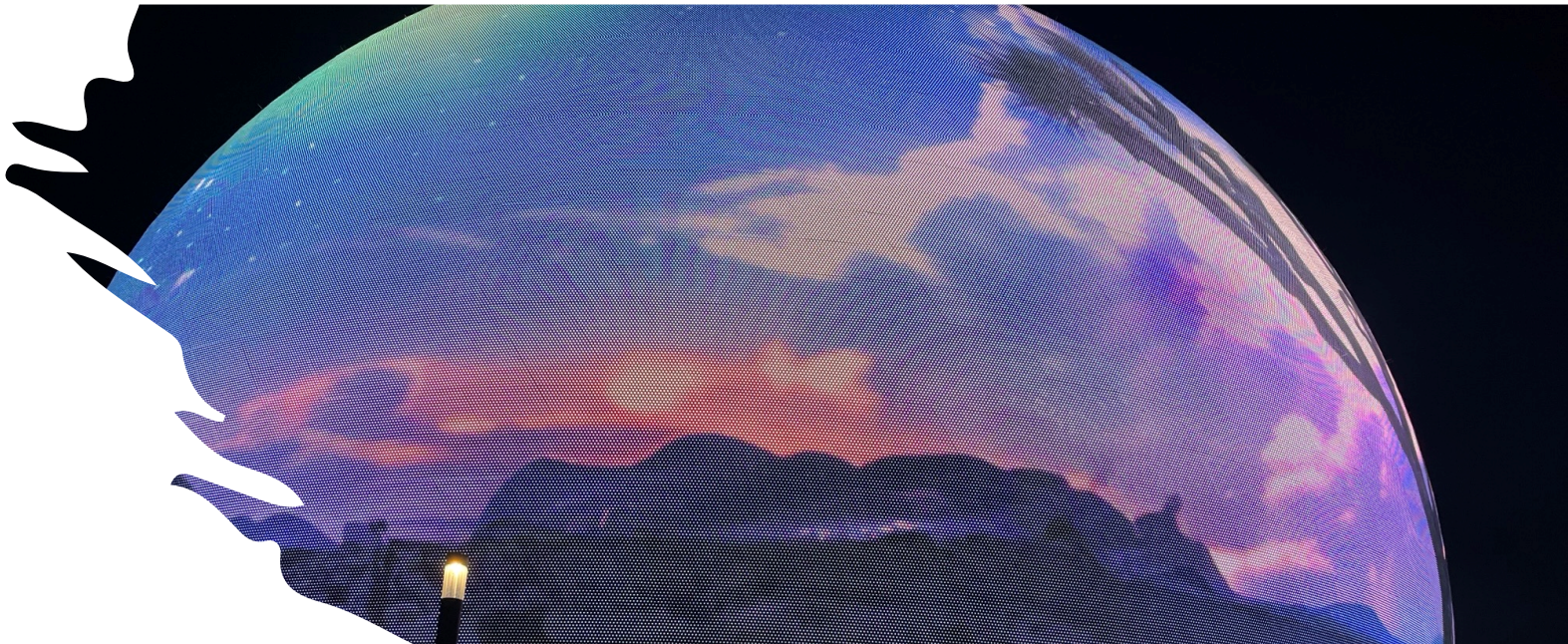
Survey of Fears

[The Chapman University Survey on American Fears | The Earl Babbie Research Center | Chapman University]

Key Components of a Research Security Program:

- Cybersecurity – NIST compliance, CUI
- Foreign travel security – registration, oversight
- Research security training – NSF requirement coming!
- Export control training – baseline understanding for research
- Insider threat awareness – red flags, vetting/screening
- Disclosure, disclosure, disclosure – when in doubt, let it out!





Challenges for small(er) institutions*

- Resource constraints – people & money
- Lack of expertise – generalist vs. specialist
- Administrative burden – same needed infrastructure for 2, 20 or 200 projects
- Technology gaps – lack of critical mass may impact options available for compliant computing
- Coordination & communication – surprisingly hard!

Question: Are these really so different from larger institutions' challenges?

*as identified by MS Co-Pilot

Other Challenges for Smaller Institutions*

- Complex research ecosystems - diverse and varied portfolios
- Collaborative nature of research – funded and unfunded
- Balancing open science with security
  - Academic culture
  - Open access publications
- Regulatory compliance – privacy, GDPR, export controls, etc.
- Cybersecurity risks – continuing assault by nefarious actors
- Faculty awareness & buy-in
- Data management & storage – lack of critical mass makes one-off solutions more likely (= less efficiency, higher cost per solution)
- Dynamic threat landscape – foreign policy, emerging technology, etc.
- Coordination across departments

Question: Are we missing any key challenges for either R1 or R2 recipients?

* As identified by ChatGPT

Experiences Thus Far

The Good

- Smaller size and scale of R2 research enterprise allows nimbleness that may be absent in larger recipient organizations
- Leadership commitment to growing and enhancing the University's research portfolio
- Positive perspectives on central OOR held by faculty – "boutique service opportunities"
- Great support to implement training on University platform, evaluate cybersecurity mandates, develop data security plans (good support services & team attitude)

The Bad

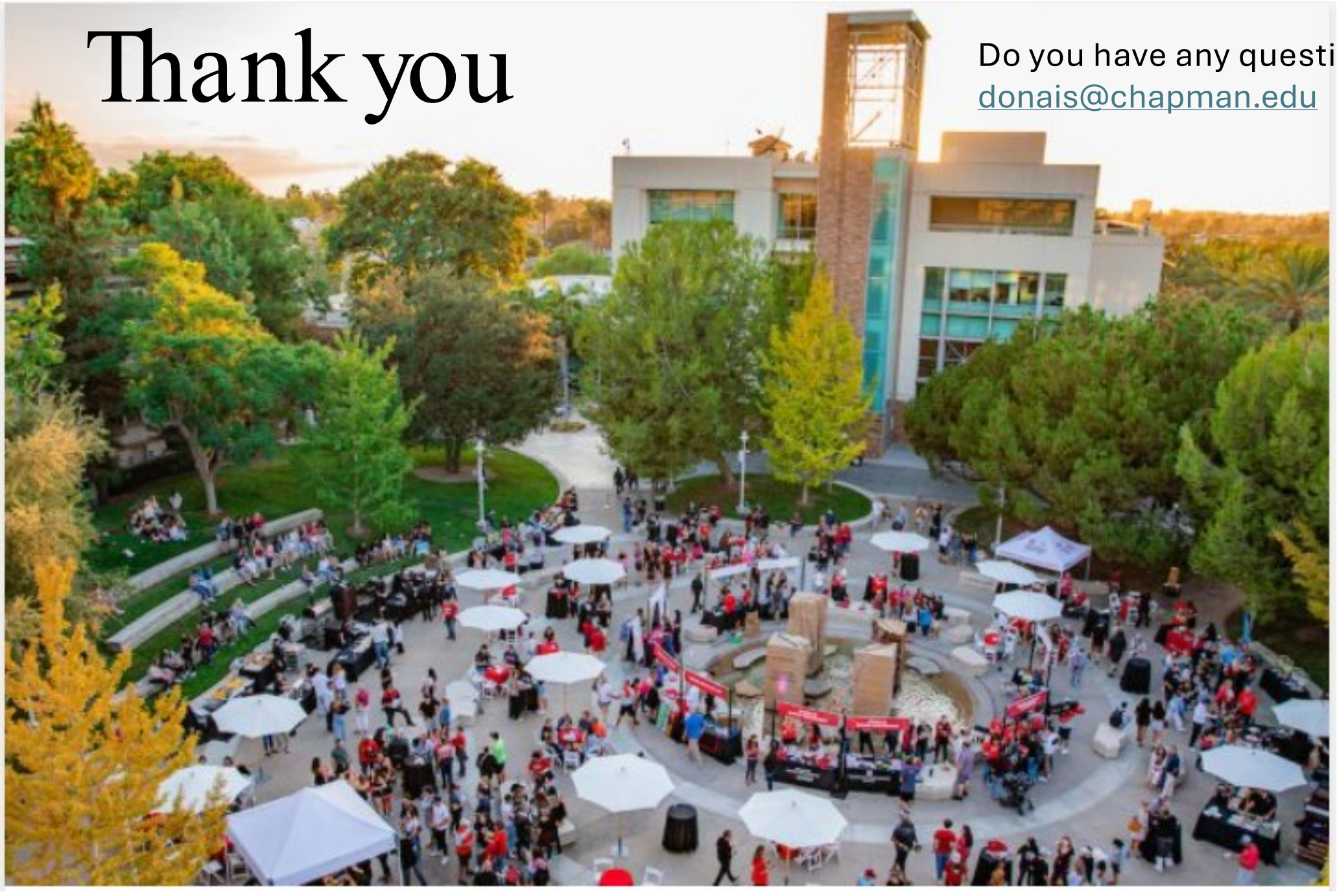
- Lack of understanding, lack of embracing, by investigators – "I do basic research that will be published!"
- Unfunded research activities may fly below the radar ("I'm not funded, so this doesn't apply to me.")
- Immature understanding of export controls & sanctions – "I'm not DOD funded!"
- Developing the culture of the research enterprise means we are often "building the airplane while flying it" - we love the instant use case to motivate & unclog the process!

The Ugly

- Ad hoc requests associated with specific awards, regardless of our covered entity status under CHIPS and Science Act (e.g., prime DOD award imposing research security plan requirement due to publications with authors from so-called countries of concern, including advisor from decades ago)

Question: Will lack of "covered status" differentiate R2s in terms of "IRL" requirements & burden?

Thank you



Do you have any questions?

donais@chapman.edu

Perspectives on NSF Research Security Training Modules: Insights from a Community Survey

Tam K. Dao
Assistant Vice President for Research Security
Baker Institute Rice Faculty Scholar

RICE

- 5K degree-seeking undergraduate students; 4K degree-seeking graduate students
- Asian Americans compose of 29 percent of the Class of 2026
- 218 million in awards. 130 million in Federal awards
- 850 full time faculty; 350 faculty in STEMS; 235 postdoctoral fellows

RICE UNIVERSITY

Core Research Competencies

Cradle of nanoscience & nanotechnology

Quantum Technologies

Artificial Intelligence & Future Computing

Space, Earth and Environment

Energy & Sustainability

Computational Sciences

Material Futures

Networks and Cyber

Advanced Biology

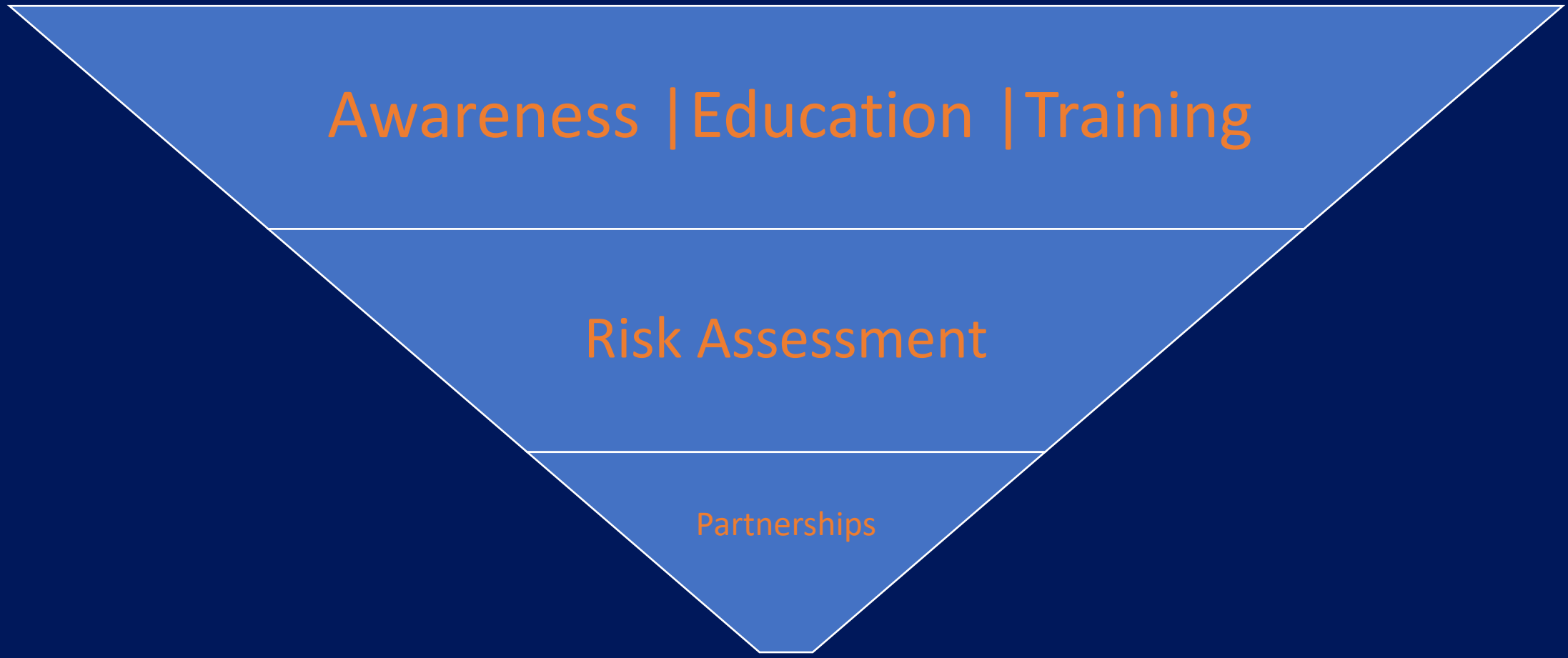
Science of Matter

Automation & Additive Manufacturing

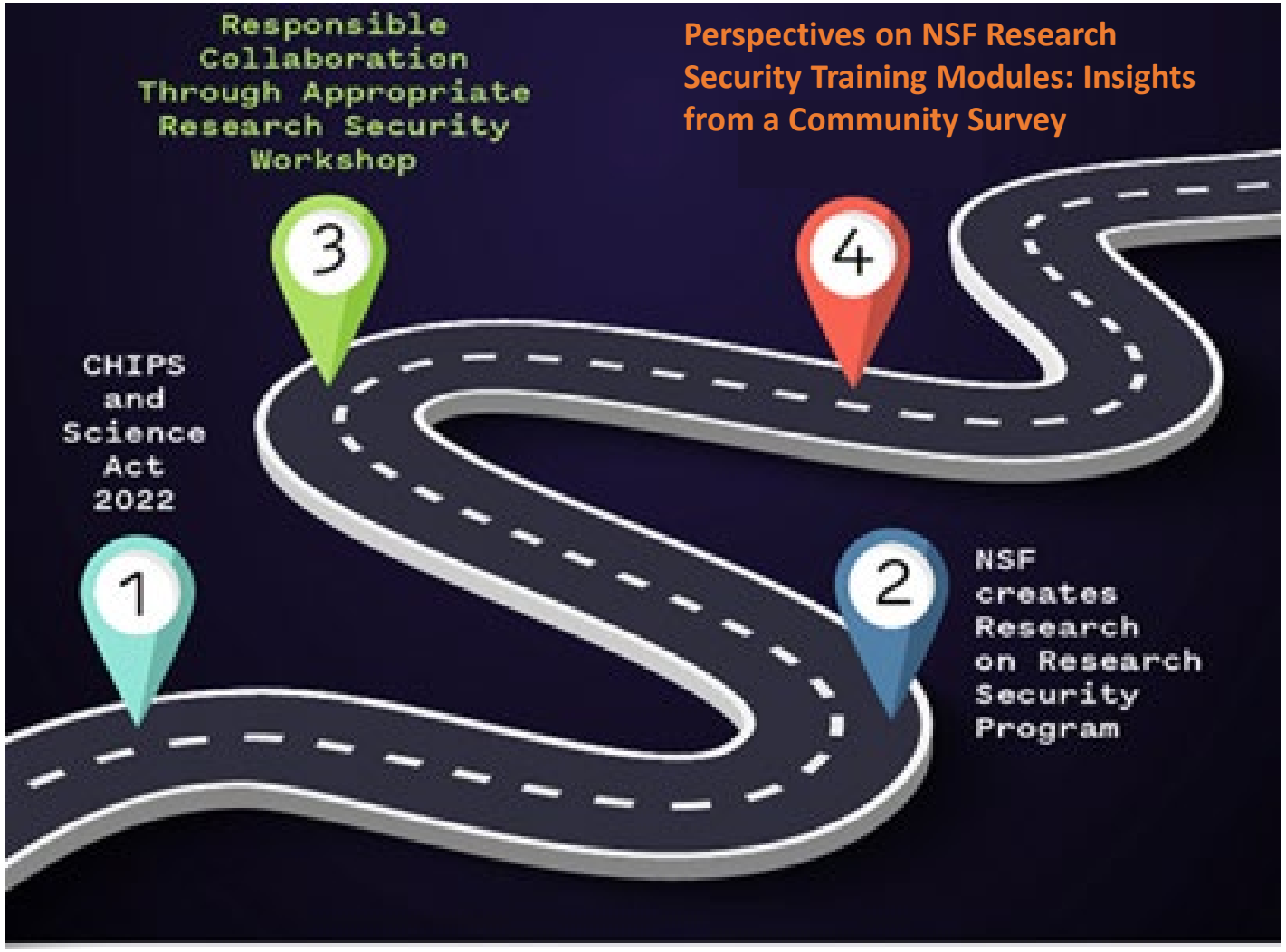
RICE

Office of Research Security

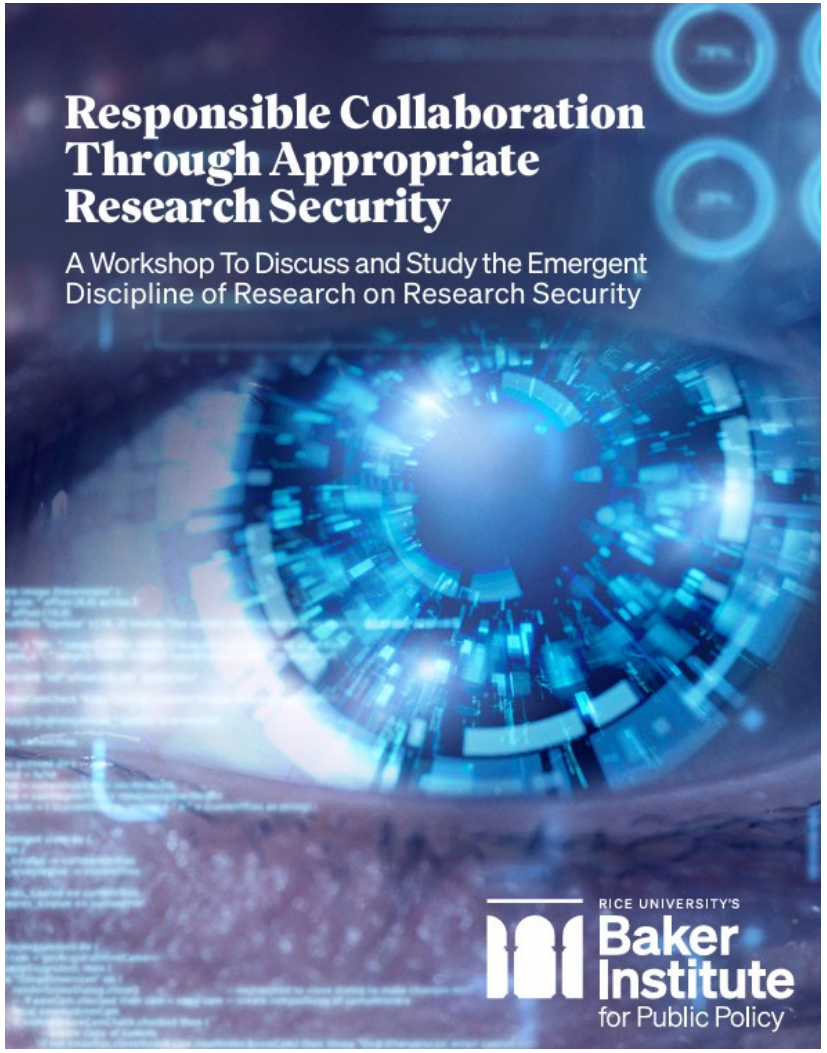
Goal is to safeguard the means, know-how, and products that originate from the Rice University research ecosystem against foreign and domestic adversaries.



RICE UNIVERSITY



Perspectives on NSF Research Security Training Modules: Insights from a Community Survey



RICE UNIVERSITY

Perspectives on NSF Research Security Training Modules: Insights from a Community Survey

Kenneth M. Evans[1,2], Tam K. Dao[1,2], Michael D. Shannon[2,3], Chris Bronk[2,4], Evan Roberts[5]
Claudia Neuhauser[4]

[1]Rice University
[2]Baker Institute for Public Policy
[3]IP Talons, Inc.
[4]University of Houston
[5] Society for Research Administrators International

RICE UNIVERSITY

Background

- CHIPS & Science Act, 2022
- NSF training modules 2024
- A focus group in May 2024 provided initial feedback, highlighting strengths and areas for improvement.

Study Objectives

- Identify trends in institutional adoption
- Evaluate comfort with learning objectives
- Assess the perceived necessity of the trainings
- Measure the perceived value and worthwhileness
- Evaluate training quality

RICE UNIVERSITY

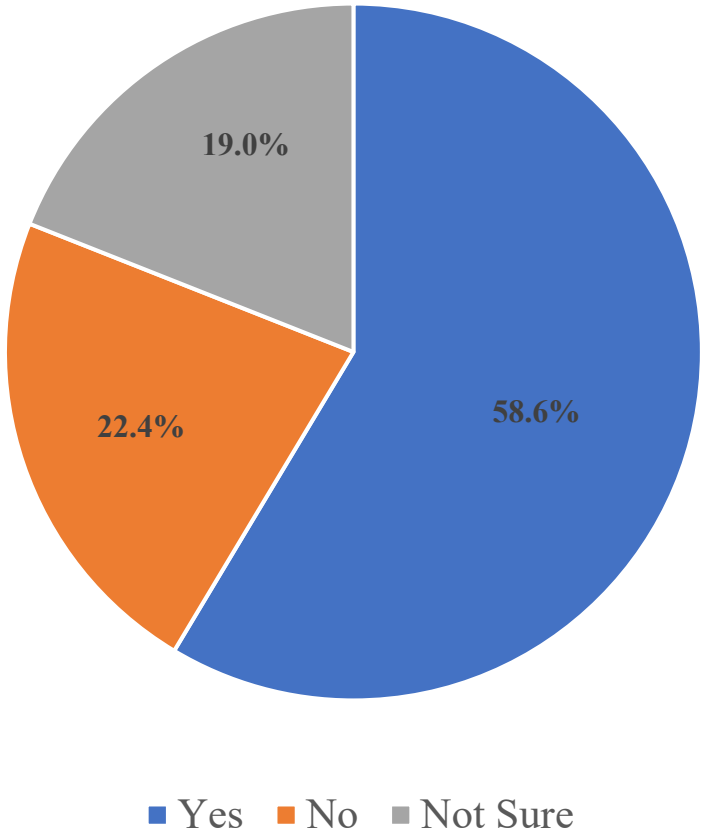
Methodology

- Survey distributed via professional organizations (e.g., SRAI, COGR, AAU, APS, AAAS).
- 175 respondents from diverse institutional backgrounds.
- Data analysis included descriptive statistics, chi-square tests, and Mann-Whitney U tests.

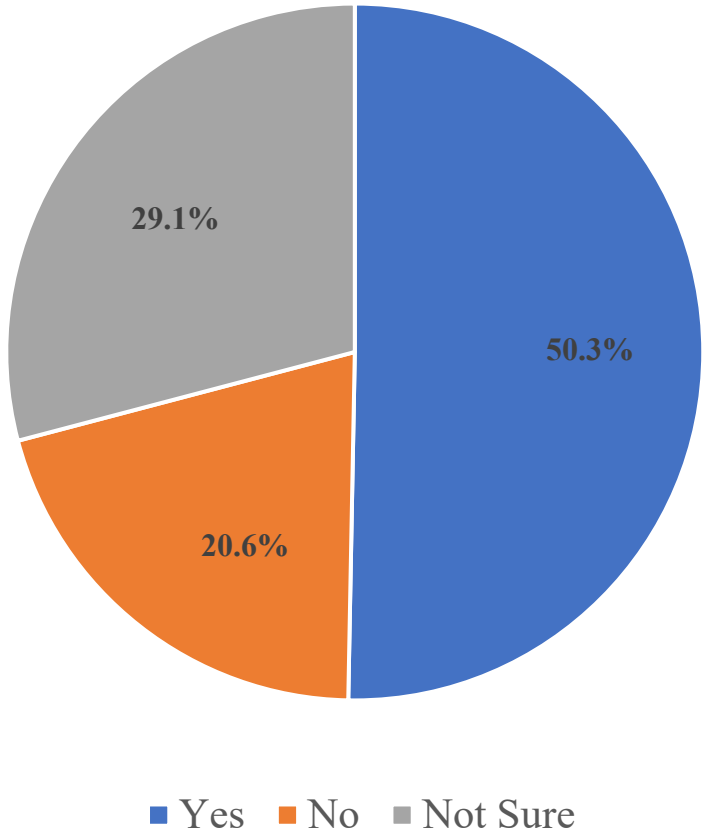
Participant Information

- 51.8% researchers, 28.2% research administrators, 15.9% institutional leaders.
- 52% from public higher education and 19.4% from private institutions.
- 79.9% affiliated with R1 institutions.

Does your organization administer required research security training?

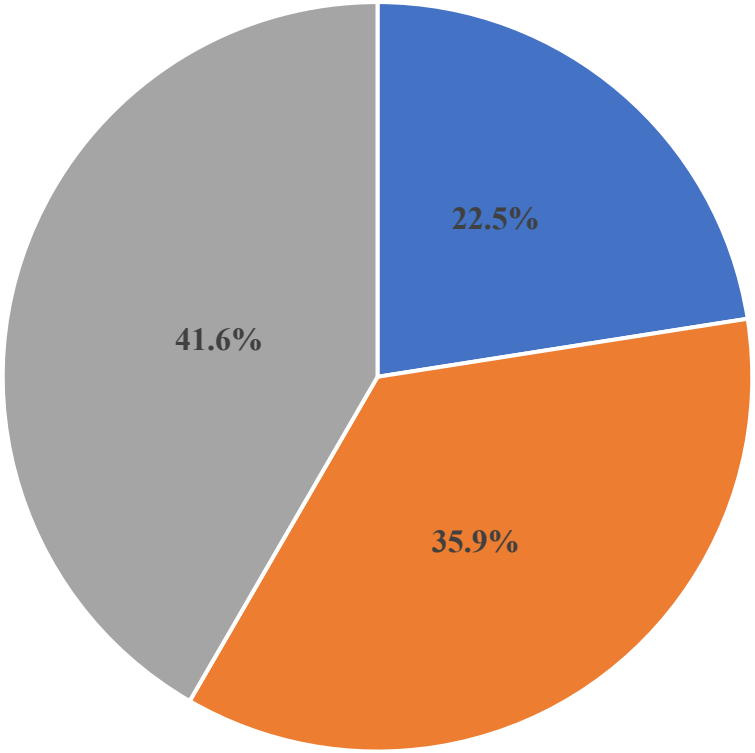


Does your organization have a formal research security program?

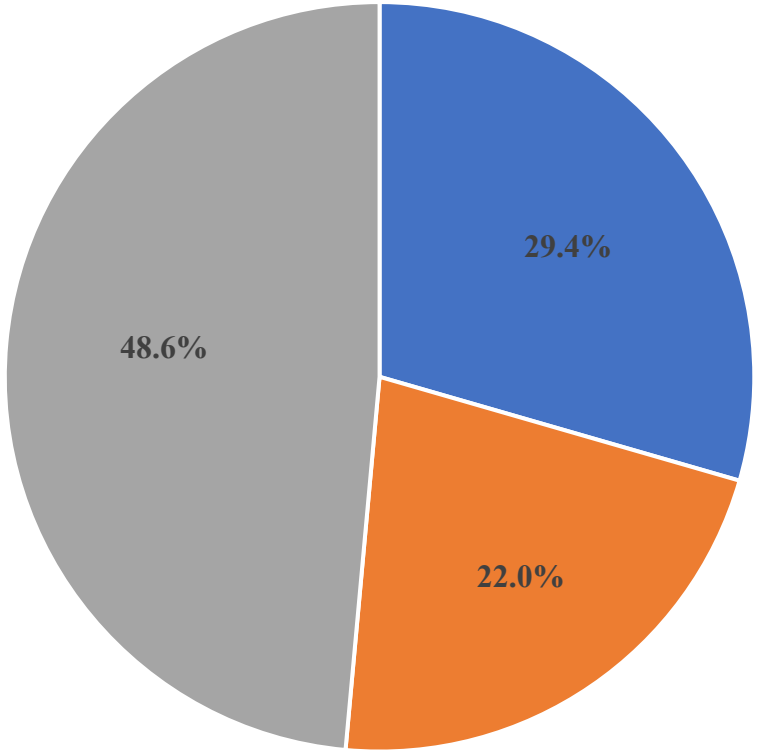


Big Picture

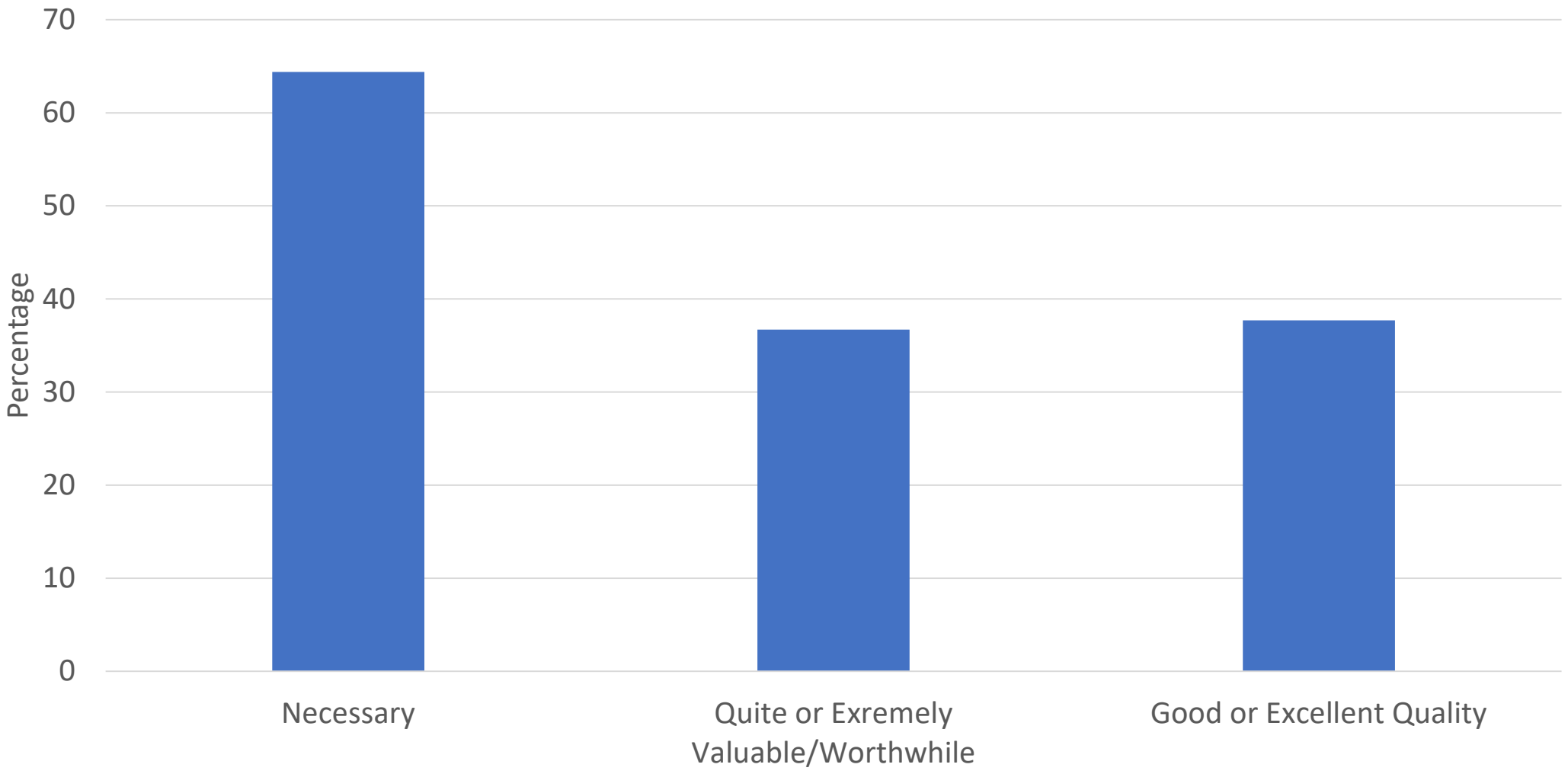
Implemented NSF research security training modules?

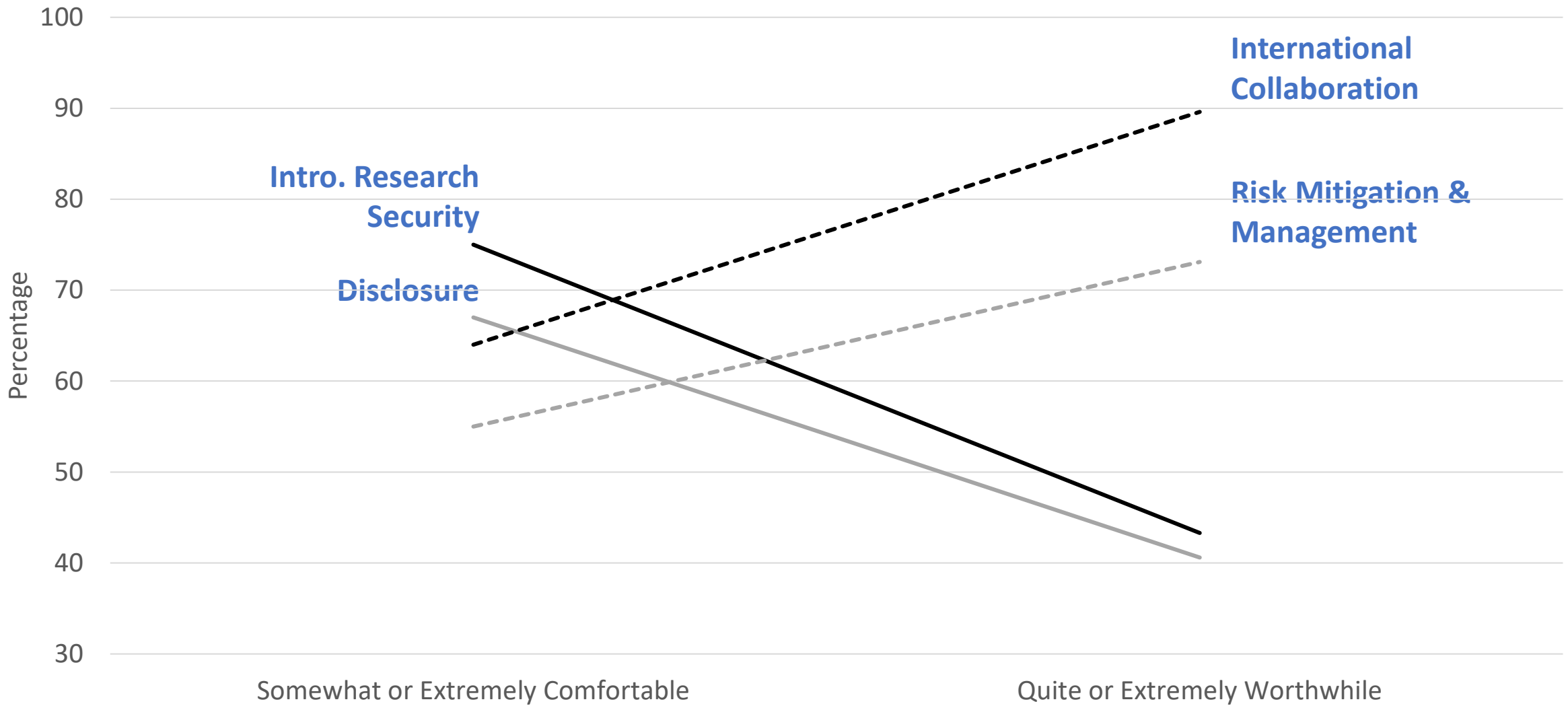


Considering implementing of NSF training modules?



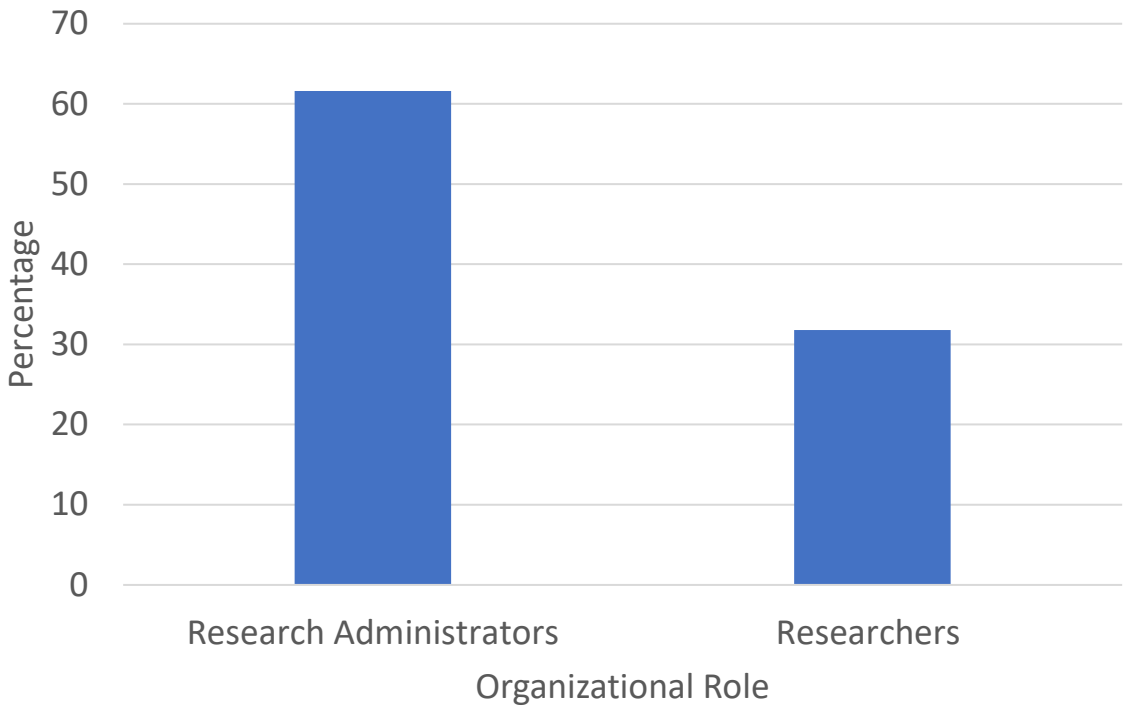
Big Picture


70
60
50
40
30
20
10
0
Percentage
Necessary
Quite or Exremely Valuable/Worthwhile
Good or Excellent Quality


100
90
80
70
60
50
40
30
Percentage
International Collaboration
Intro. Research Security
Risk Mitigation & Management
Disclosure
Somewhat or Extremely Comfortable
Quite or Extremely Worthwhile

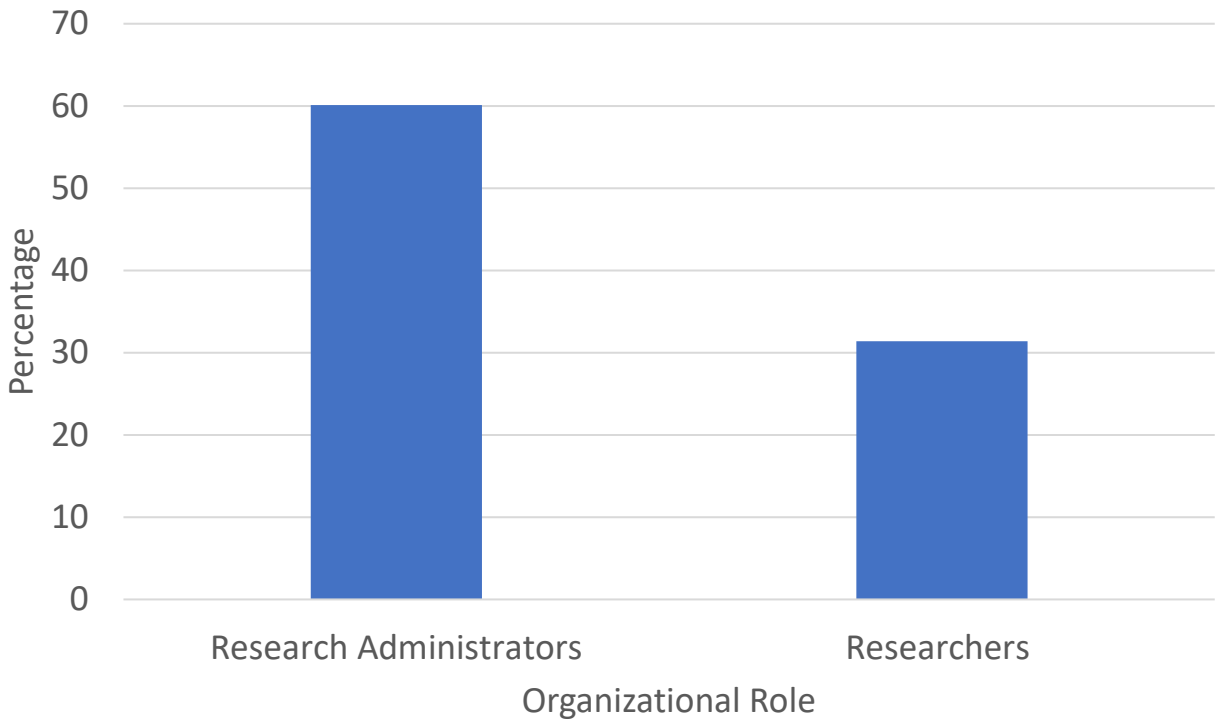
RICE UNIVERSITY

Necessity of Research Security Training



There was a significant association between an individual's role within an organization and their perspectives on the necessity of research security training, X^2 (2, N = 174) = 17.41, p < .001.

Knowledge of Research Security Program



There was a significant association between an individual's role within an organization and their awareness that their organization has a formal research security program, X^2 (2, N = 175) = 10.76, p < .005.

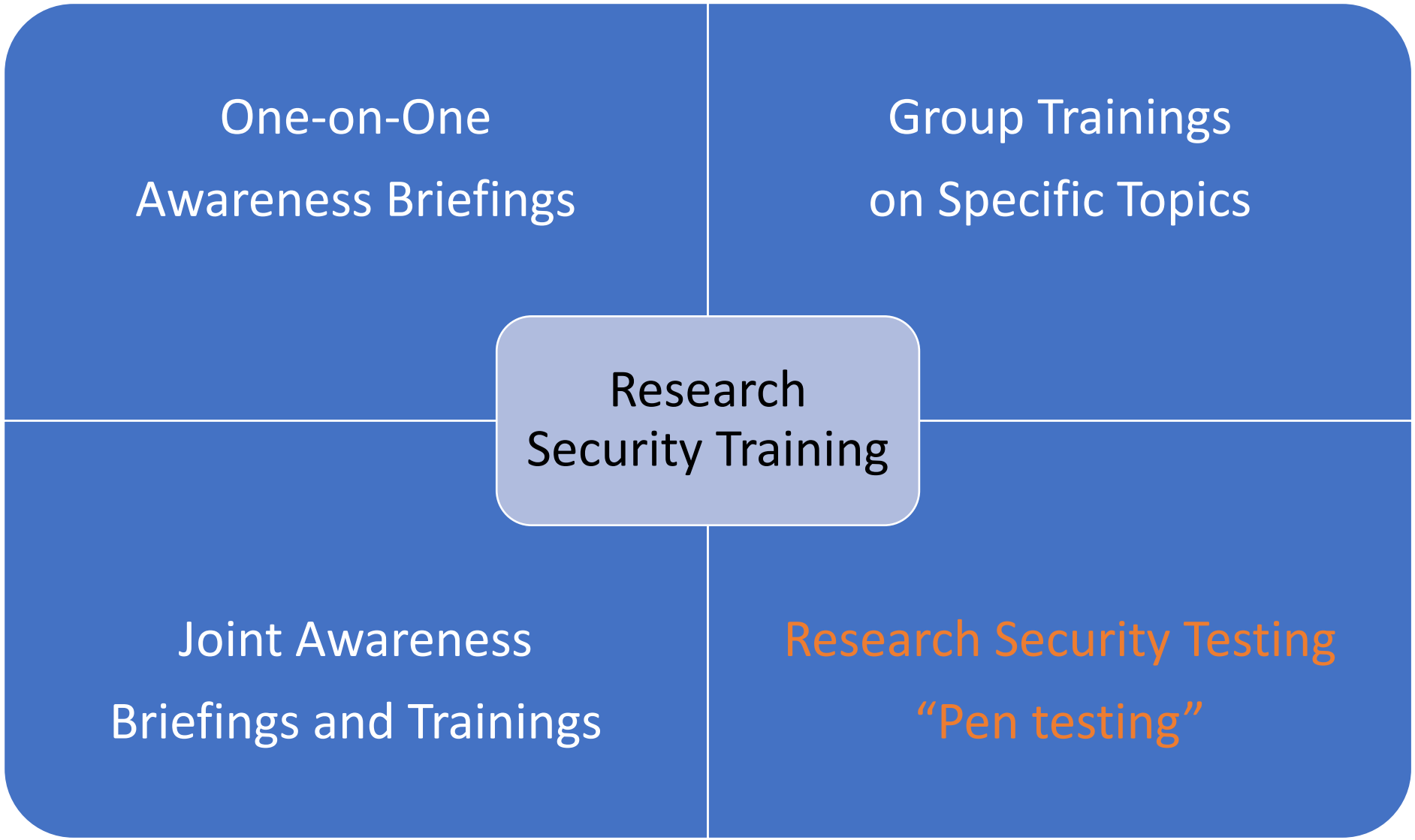
RICE UNIVERSITY

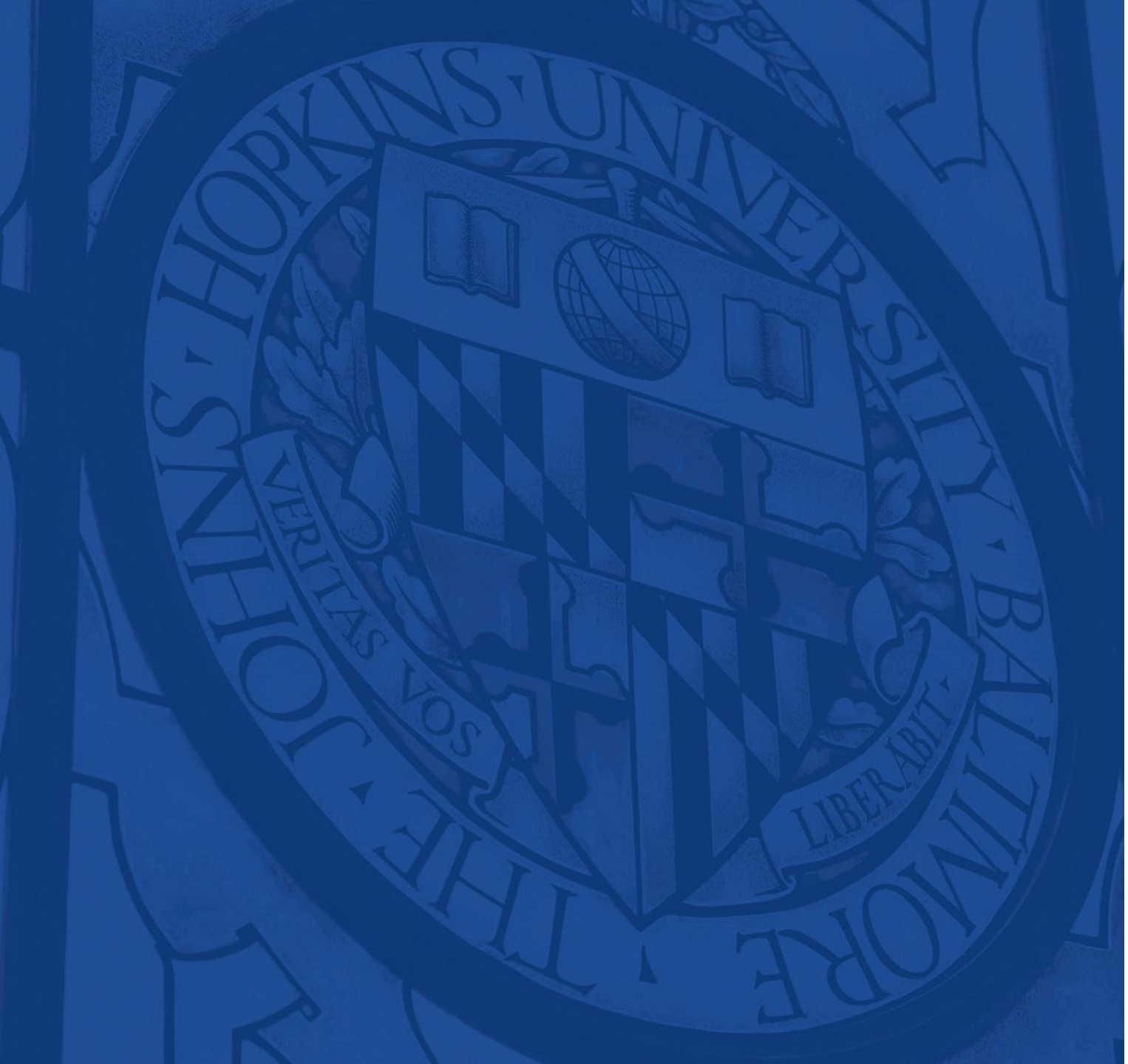
Study Objectives

- Identify trends in institutional adoption
- Evaluate comfort with learning objectives
- Assess the perceived necessity of the trainings
- Measure the perceived value and worthwhileness
- Evaluate training quality

Conclusion

- Low institutional adoption of NSF research security training modules.
- Respondents reported a good comfort level with the objectives.
- While the training is seen as necessary, it is not perceived as valuable or worthwhile.
- Perceived as too long and too slow.
- Interaction Effect


One-on-One
Awareness Briefings
Group Trainings
on Specific Topics
Research
Security Training
Joint Awareness
Briefings and Trainings
Research Security Testing
“Pen testing”



JOHNS HOPKINS
UNIVERSITY & MEDICINE

NIH Implementation Update for Data Management and Access Practices Under the Genomic Data Sharing Policy

Thomas Burns
Associate Dean for Research Affairs

JHU at a Glance

- 11 Schools and Divisions
- 3700 FT Faculty
- $3.3B federal R & D expenditures FY23
- $843M NIH funding FY23
- 2022-2023 Significant investment towards NIST compliance
- 2025 Research IT environment substantially compliant with NIST 800-171 Rev. 2/3

NIH Update to GDS data management & access practices

Effective January 25, 2025 and applies to:

- **NIH controlled-access human genomic data repositories and access systems**
  - Most widely used repository is the database of Genotypes and Phenotypes (dbGaP).
  - Institutions that generate large-scale human genomic data as a part of an award, and store it at their institution, cloud-service provider, or third-party IT system are **not in scope.**
- **Approved Users** of genomic data from NIH controlled-access repositories
  - **Required to secure data according to NIST SP 800-171 standard**, per NIH Security Best Practices for Users of Controlled-Access Data.
- **Developers** who test platforms, pipelines, analysis tools, and user interfaces that store, manage, and interact with human genomic data from NIH controlled-access repositories, and provide infrastructure development and repository maintenance
  - **The work must relate to developing or maintaining (one of the 20) NIH controlled-access data repositories – i.e., it is not classified as research.**
  - As of January 25, 2025, NOFOs, contracts, or Other Transactions, will indicate the applicability of the update and developer terms of access.
  - Data Security Training required for Approved Developers

Approved Users

- Approved Users who **submit a new or renewed data access request** are expected to secure data according to updated NIH Security Best Practices
  - Attest to NIH that the system storing and using human genomic data downloaded from these repositories complies with NIST SP 800-171. **NIH does NOT consider this data CUI.**
  - If choosing a third-party IT system and/or Cloud Service Provider for data analysis and/or storage, provide NIH with an attestation that the third-party system is compliant with NIST SP 800-171.
  - Non-U.S. users that are unable to attest to the NIST SP 800-171 may attest to the equivalent ISO/IEC 27001/27002 standard.
- The attestation may vary and is included in the existing data access request process. The PI's and institution's ability to attest is informed by a self-assessment.

JHU Implementation Plan

- Identification and alignment of stakeholders
  - Research Administration, Faculty, Research IT, IT Security, IRBs, Libraries, Purchasing
- Communication on singular central NIST 800-171 compliant environment
- Review of researcher local environments
- Identify existing and likely approved users
  - dbGaP renewals
  - Awards/proposals with “developer work”
- Procedures for researcher and institution attestations
- Identify necessary deviations & develop PoA&M for partial/planned implementations.

Research IT Environment at JHU

- IT@JH has established a suite of storage and compute environments for research, to meet the NIST SP 800-171 standard (Rev. 2/3)
  - **Includes**: **Discovery HPC and SAFESTOR Storage now,** soon: SAFER and JH Clouds (Azure & AWS)
  - **Status**: Complete for Rev 2 by 1/25/25 (with added components soon after); in progress for Rev 3.
  - **Support**: IT Security checklist assessment and PoA&M for reference/inquiries; User rules of behavior; Onboarding materials and facilitation for researchers; Language for grants and data management plans.
  - **Goal**: Finalize implementation and conduct a formal audit to solidify the solution.

- The Research IT environment integrates with institutionally managed infrastructure and services with a set of cybersecurity policies and controls that also meet the NIST SP 800-171 standard: identity and authentication, access control, network protection, audit logging and monitoring, incident response, etc.

Data Access/Attestation Process

- The NIH process for genomic data access requests is expected to remain the same, with the addition of a PI attestation to meeting the updated NIH Security Best Practices for Users of Controlled-Access Data.
- Institutional official sign-off will continue to be required.
- Approved Users (and Developers) of NIH controlled-access repository data will be required to manage the data in an approved Johns Hopkins NIST SP 800-171 compliant environment.
- Faculty are strongly encouraged to begin the process of security evaluation as soon as possible to ensure there are no delays in renewing their agreements.
- Research Administration will be unable to submit an application or a request for data access to NIH without verification of the secure environment.
- IRB protocols, grant applications, and data management plans might need to indicate the use of approved NIST SP 800-171 environments.

Changes in Researcher Experience

- **Data movement in/out of the environment more controlled**:
  - Data/file transfers mostly mediated through Globus (a collaborative file transfer system, with connectors to many cloud storage services) and Azure Data Factory (an ETL data ingest tool).
  - Access to external sites restricted: denied by default, with an allowed list to specific repositories and APIs (e.g., Open OnDemand, GitHub)
- **Activity** in and around the environment logged and monitored for deviations and inquiries.
- Data and audit log retention reflect institutional policies and research-specific mandates.
- Researchers follow policies to ensure their part of the compliance
  - **Approve and review user access lists regularly.**
  - **Avoid moving data out of the environment** (e.g., not upload data to GitHub).
- **Some workflows will need to be adapted** – we will work with researchers and improve overtime.

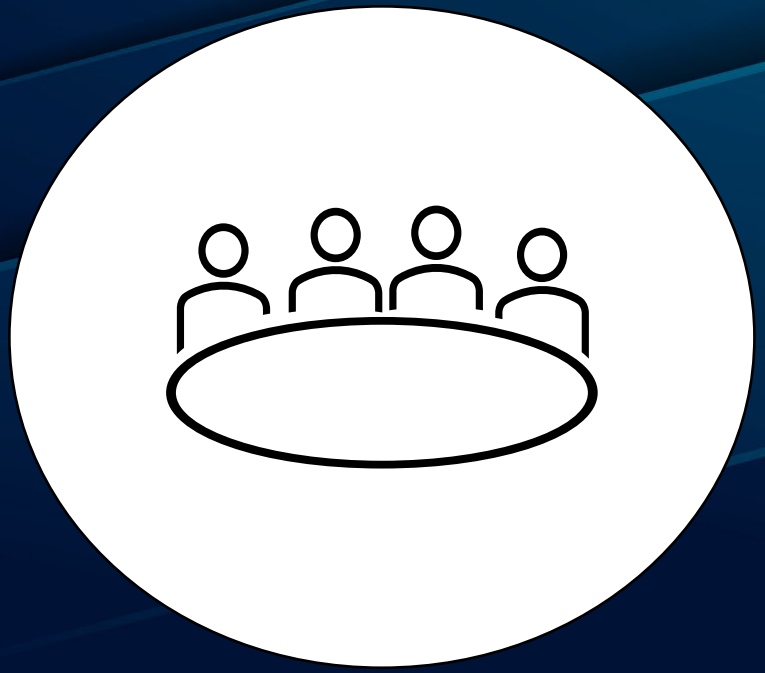
On a comforting note…

- All research institutions will be applying these standards per updated NIH GDS policy.
- Most federally funded research will soon be requiring this level of research security, with a clear convergence towards this particular NIST standard.
- Using approved research IT environments will increase research protection and free up time for researchers to focus on their projects.

Successes and Challenges

- Critical support from institutional Research IT and IT Security teams
- Early identification of affected researchers/environments
- Challenges with single environment approach
  - Researchers can opt to use Research IT or seek review of local cluster by CISO
  - Use of PoA&M when necessary
- Concern around alignment with enterprise information security infrastructure and patterns.
- Successful proactive approach in communicating with researchers

Panel Discussion



Poll Question #1

#COGRFeb25

How would you describe your institution's readiness regarding research security training?

A. We are actively developing our research security training.

B. We are in the process of implementing our research security training.

C. Our research security training is fully implemented, with active participation.

D. We are still assessing how best to implement a training program

E. I don't know

COGR

Poll Question #2

#COGRFeb25

How would you best describe your institution's approach to research security training?

A. Using the NSF-provided research security training modules as-is.

B. Using abridged NSF Modules (developed by UMichigan, Stanford, Duke and The Ohio State University)

C. Taking a hybrid approach, combining NSF modules with institution-specific training

D. Using a third-party vendor solution (e.g., CITI) for research security training.

E. Using a fully customized, internally developed research security training program.

F. Other (please specify in the chat).

COGR

Poll Question #3

#COGRFeb25

What is your institution's readiness for implementing cybersecurity measures for research security?

A. We're largely in a holding pattern, awaiting further guidance.

B. We're in the development and planning stages.

C. We're actively implementing our cybersecurity measures.

D. We're ready! Our cybersecurity program is fully implemented

E. I don't know

COGR

#COGRFeb25

Poll Question #4

Has your institution received a notice from the NIH to apply new security standards (e.g., NIST 800-171) to controlled-access data?

A. Yes
B. No
C. I don't know

COGR