NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Update on NIST Cybersecurity for Research Effort

Implementation of CHIPS & Science §10229

October 2023

Background: §10229

- CHIPS & Science Act signed into law August 2022, including *NIST for the Future Act* (Div B, Title II)
- **§10229, *Dissemination of Resources for Research Institutions***, directs NIST to disseminate and make **publicly available tailored resources** to help institutions of higher education in receipt of in excess of $50M/year in federal research funding identify, assess, manage, and **reduce cybersecurity risk related to conducting research**.
- Per statute, these resources should:
  - Be **generally applicable** and **usable** by a wide range of qualifying institutions;
  - Vary with the **nature** and **size** of the qualifying institutions, and the nature and **sensitivity** of the data collected or stored on the information systems or devices of the qualifying institutions;
  - Include elements that **promote awareness of simple, basic controls**, a workplace cyber security culture, and third-party stakeholder relationships, to assist qualifying institutions in mitigating common cybersecurity risks;
  - Include **case studies**, **examples**, and **scenarios** of practical application;
  - Be **outcomes-based** and can be implemented using a **variety of technologies** that are **commercial and off-the-shelf**; and
  - Be based on **international technical standards**.

§10229 Implementation Timeline

January - March 2023
(FY23 Q2)

Initial discovery exercise, conduct SME engagements

April-June 2023
(FY23 Q3)

Initial RFC and engagements with the higher ed and research security communities

July-September 2023
(FY23 Q4)

NISTIR 8481 developed and published for comment

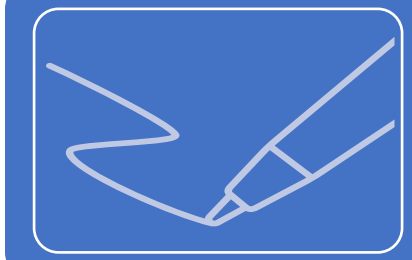
October-December 2023
(FY24 Q1)

Ongoing engagement with higher education communities

Finalize NISTIR 8481

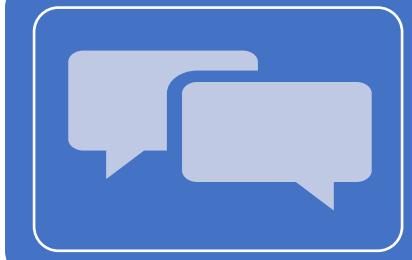
Community Engagement To-Date in 2023

Direct engagement with 20+ higher ed research institutions



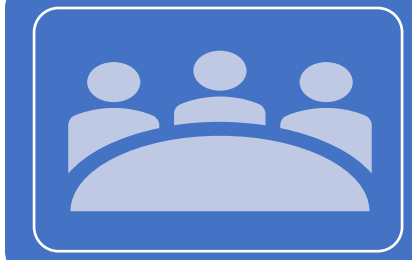
Request for Comment (RFC)

- Posted from April 2023 to June 2023
- Requested input on cybersecurity challenges for research, existing cybersecurity resources, and future resources to support the cybersecurity of research projects



One-on-one Meetings

- one-on-one discussions with individuals from universities, research security groups, and NIST program leads
- Held follow-up meetings to discuss cybersecurity for research programs or efforts



Virtual Group Discussion Session

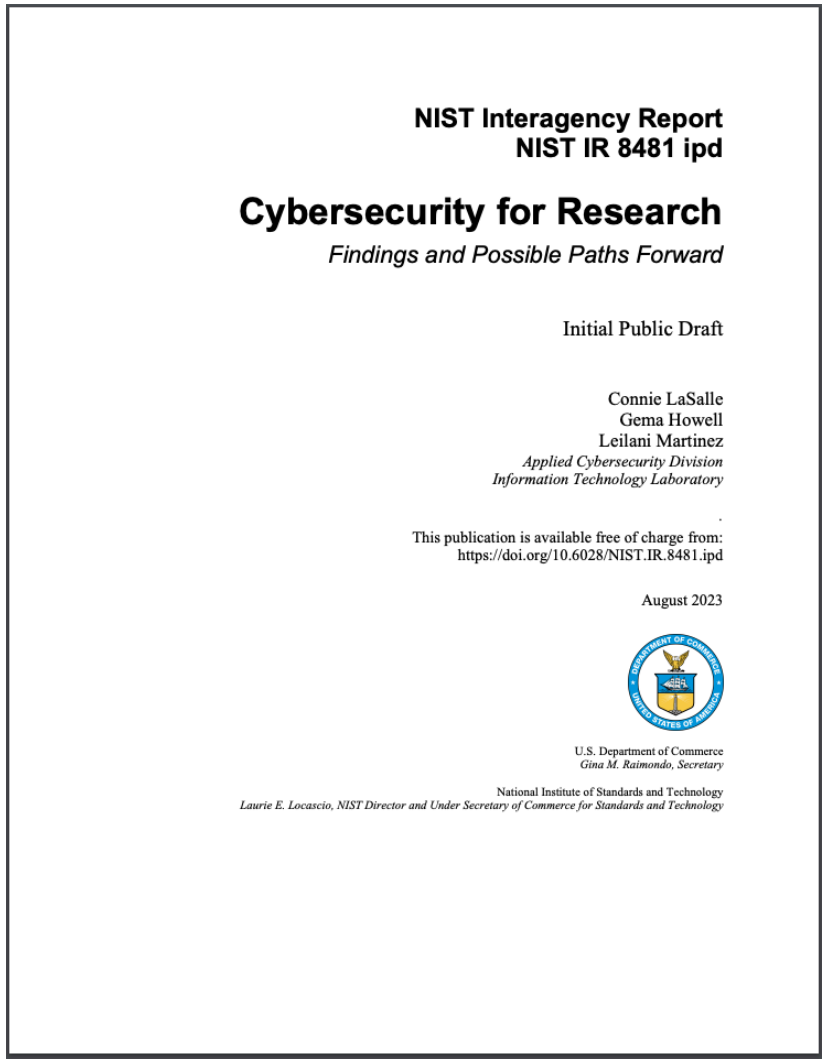
- Included attendees from research security groups and universities
- RFC questions were used to guide the conversation

Community Feedback Analysis

Request for Comment (RFC)

One-on-one Meetings

Virtual Group Discussion Session



NIST Interagency Report
NIST IR 8481 ipd

Cybersecurity for Research

Findings and Possible Paths Forward

Initial Public Draft

Connie LaSalle
Gema Howell
Leilani Martinez
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8481.ipd

August 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Key Questions Informing NISTIR 8481

1. What **common cybersecurity challenges and risks** does your institution face when conducting research?

2. Does your institution face **unique cybersecurity challenges and risks** associated with certain types of research, for example, microelectronics or other areas of science and technology?

3. **How** is your institution identifying, assessing, managing, and reducing cybersecurity risks related to conducting research?
    1. How do **NIST resources** support cybersecurity risk management in your institution?
    2. What **other resources** does your institution leverage to support cybersecurity risk management?

4. Are **existing resources** sufficient and effective? If not, why?

5. What **new resources** or areas of further research might address **common cybersecurity challenges** and **risks faced by faculty or researchers, students, academic or research affairs offices, and personnel with enterprise risk management responsibilities** (e.g., Chief Information Officers, Chief Information Security Officers, Chief Privacy Officers, Chief Compliance Officers, Chief Risk Officers, and others)?
    1. What role might NIST play in providing resources and research to address common cybersecurity challenges and risks faced by these communities?
    2. Who should be involved in the development of these resources and research (e.g., researchers with institutional affiliation, research cybersecurity subject matter experts, or other associations or groups)?

Summary of Feedback: Common Challenges & Risks

Awareness

Workforce

Culture clash

Limited cybersecurity budgets

Complicated requirements landscape

Rapid pace of innovation

Summary of Feedback: Unique Challenges & Risks

Biotechnology

Quantum Computing

Neural psychology

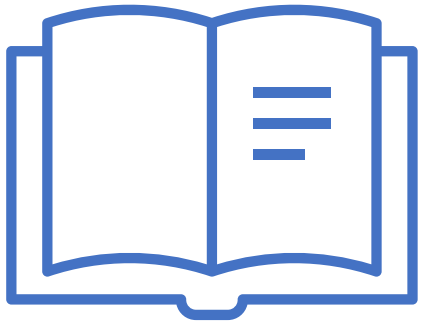
Optical science

Space research

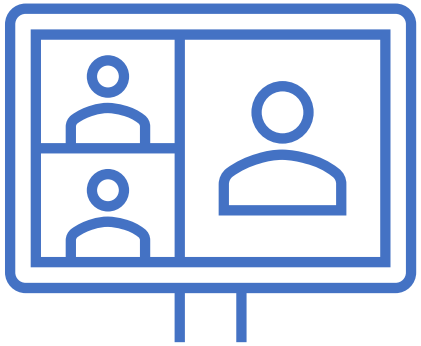
Engineering

Clinical research (in general)

Summary of Feedback: Future Work Suggestions

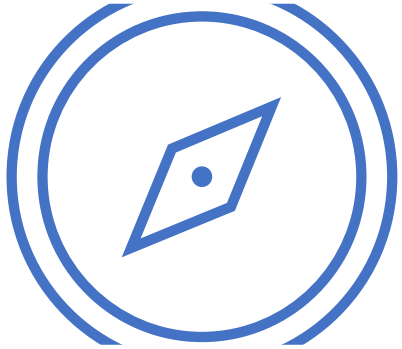


Targeted Cybersecurity Resources



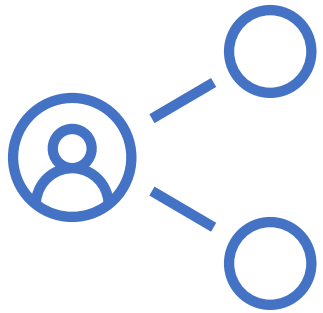
Collaborative Engagements

Trainings



Framework Guidance

Security Compliance Grant Guidance



Shared Services Support

Potential Next Steps for NIST

Community-specific Cybersecurity Resources

- Cybersecurity resources tailored to research security
- Cybersecurity resources for specific fields of study (e.g., clinical research, space research)

Coordination

- Coordinate with federal agencies to include consistent application of NIST guidance
- Sustain collaboration with high education cybersecurity and research communities

Capacity-building

- Support cybersecurity trainings for research
- Evaluate the National Initiative for Cybersecurity Education (NICE) Program role in building capacity in research cybersecurity

Appendix A. Existing Cybersecurity Resources

- NIST Resources
  - Cited by institutions
  - Other relevant cybersecurity risk management guidance
  - NIST guidance that demonstrations implementations and reference architectures that address relevant cybersecurity challenges
  - NCCoE projects that cover relevant topic areas

- Other Available Resources
  - Resources that exist to support a specific higher education institution and its community
  - R&E community resources from various groups and federal agencies

Areas Where We'd Like Feedback

See more in our Note to Reviewers (page ii):

- **Section 3.1: Cybersecurity Challenges and Risks**
  - Any potential gaps or nuance missed?

- **Section 4: Potential Next Steps for NIST**
  - Which areas would be most impactful?

- **Appendix A: Existing Cybersecurity Resources**
  - Thoughts on the list of resources and any specific resources that could be tailored to research

Questions?

Contact us: cyber4R&D@nist.gov