NIST Interagency Report
NIST IR 8481 ipd

# Cybersecurity for Research

## *Findings and Possible Paths Forward*

Initial Public Draft

Connie LaSalle
Gema Howell
Leilani Martinez

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

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

# 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*

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

**NIST Technical Series Policies**
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

**Publication History**
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added upon final publishing.]

**How to Cite this NIST Technical Series Publication:**
LaSalle C, Howell G, Martinez L (2023) Cybersecurity for Research: Findings and Possible Paths Forward. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8481 ipd. https://doi.org/10.6028/NIST.IR.8481.ipd

**Author ORCID iDs**
Connie LaSalle: 0000-0001-6031-7550
Gema Howell: 0000-0002-0428-5045
Leilani Martinez: 0009-0005-9715-7649

**Public Comment Period**
August 31, 2023 – October 31, 2023

**Submit Comments**
cyber4R&D@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

**All comments are subject to release under the Freedom of Information Act (FOIA).**

## Abstract

Unmanaged cybersecurity risks can wreak havoc on a community. This is no less true for the U.S. scientific research ecosystem, particularly members of the higher education research community, which can be characterized by its fundamentally open, collaborative culture and web of highly decentralized administrative and research environments. Securing the digital resources that contribute to a thriving higher education research enterprise requires consideration of the threats and vulnerabilities relevant to the community as well as unique mission contexts, cultures, and motivations. This resource is intended to enable institutions of higher education to identify, assess, manage, and reduce cybersecurity risks related to conducting research, as described in Section 10229 of the CHIPS and Science Act.

## Keywords

access control; cybersecurity; cybersecurity awareness and education; cybersecurity risk management; controlled unclassified information (CUI); digital identity; higher education; information security; National Initiative for Cybersecurity Education (NICE); NIST Special Publication 800-53; NIST Special Publication 800-171; NIST Risk Management Framework; nonfederal systems; research and education (R&E); research cybersecurity; research security; risk management; safeguarding science; security; workforce.

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

## Note to Reviewers

NIST is specifically interested in feedback on the following sections:

- **Section 3.1: Cybersecurity Challenges and Risks**

  Through the findings presented in Section 3.1, NIST hopes to document and drive awareness of the cybersecurity challenges and risks that institutions of higher education face when conducting research, as well as the parallel systemic problems and unique considerations associated with this community that increase the complexity of managing cybersecurity risks. Please provide feedback on the challenges, risks, and summary narrative offered in this document, NIST IR 8481, and alert us to any potential gaps or nuance that may have been missed.

- **Section 4: Potential Next Steps for NIST**

  A list of potential next steps for NIST was derived from feedback received through engagement with the research community and higher education cybersecurity community about their cybersecurity challenges, existing resources that they have found helpful, and desired new resources. Section 4 proposes three areas in which NIST could play a role:

  1. Community-specific cybersecurity resources
  2. Coordination
  3. Capacity building

  Please provide feedback on these areas, noting which would be most impactful.

- **Appendix A: Existing Cybersecurity Resources**

  NIST IR 8481 is a publicly available document that includes a list of existing cybersecurity resources that can be disseminated and used to help institutions of higher education identify, assess, manage, and reduce cybersecurity risks related to conducting research. The list of resources includes items that are currently available for Research Security Officers, Chief Information Security Officers, cybersecurity teams, and others who are responsible for managing risks related to conducting research.

Beyond this list of existing cybersecurity resources, NIST is seeking input on:

1. NIST resources on this list that could be tailored for an audience of researchers who do not have a background in cybersecurity
2. NIST resources on this list that could be adapted to align with the research and education environment

## Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: cyber4R&D@nist.gov

## Table of Contents

## Acknowledgments

The authors would like to thank those who contributed feedback to NIST's April 2023 Research for R&D Request for Comment, as well as those who actively participated in one-on-one sessions and community dialogue with NIST on the topic of research cybersecurity.

# 1. Introduction and Background

Research performed by higher education spans many sectors and areas of expertise. Contributions made by members of this community not only advance our understanding of the world around us but can also be commercialized to yield national economic benefits for countries with well-established research-to-market pipelines. Because of this, the research community has been victim to cyber espionage by nation-state actors. The pursuit of intellectual property and economic advancement through cyber espionage is an ongoing threat to the U.S. research ecosystem that — alongside other contemporary cybersecurity risks like ransomware — must be managed in a way that is cognizant of the unique mission contexts, cultures, and motivations of higher education research communities.

Additionally, the past few years have seen an overwhelming embrace of remote work across many sectors of the American economy. Even before the COVID-19 pandemic, the factors contributing to a "work from anywhere" mentality were in place, including a rise in cloud computing capabilities, greater availability of high-speed internet, improved connectivity in rural and underserved urban areas, and shifting workforce expectations around work-life balance. This trend toward distributed collaboration was accelerated for many by the unexpected and immediate move in 2020 away from on-site or on-campus work supported by enterprise-secured networks, on-premises compute infrastructure, and enterprise-managed devices toward at-home work supported by home networks, collaboration tools, and cloud-based environments by default.

The evolving cybersecurity threat landscape is of great concern to higher education, as well as the White House and Congress. In August of 2022, the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022 was enacted. It included Section 10229, which directed NIST to create resources like this one to aid qualifying institutions of higher education in identifying, assessing, managing, and reducing cybersecurity risks while conducting research.

## 1.1. Purpose

The purpose of this document is to provide the higher education community with an initial voluntary resource that can be leveraged to manage cybersecurity risks that are specific to conducting federally funded research. Specifically, this resource seeks to document and cultivate a common understanding of the state of cybersecurity across higher education research environments and is intended to help institutions of higher education identify, assess, manage, and reduce cybersecurity risks related to conducting research, as described in Section 10229 of the CHIPS and Science Act (Pub. Law 117-167).

## 1.2. Scope and Audience

This publication is intended to be used by members of the higher education community, particularly those responsible for managing cybersecurity risks associated with conducting research, such as Vice Presidents of Research, Research Security Officers, Chief Information Security Officers, higher education IT, cybersecurity and privacy professionals, and research performers. The audience of this publication also includes policymakers and organizations that

fund research, who may play a role in constructing and overseeing the implementation of cybersecurity requirements for this community.

# 2. Approach

This section provides an overview of the approach used to conduct the study that assisted in the development of this document, NIST IR 8481. Common cybersecurity challenges and desired resources were identified in consultation with higher education institutions and members of the research security community. This was accomplished through four main tasks: initial discovery, community engagement, feedback analysis, and initial resource development.

## 2.1. Initial Discovery

Preliminary research was conducted to identify relevant federal agencies, associations, institutions of higher education, subject-matter experts with research security equities, and programs across NIST focused on cybersecurity and privacy risk management, cybersecurity workforce development, and research security, including NIST's own research security program. Engagement with the appropriate parties was essential to ensure that adequate information was gathered related to the cybersecurity challenges, current resources, and future cybersecurity resources that can assist the research community.

## 2.2. Community Engagement

After identifying the relevant groups, including associations representing 2000+ colleges, universities, and related organizations, a series of consultations and open engagements was conducted, resulting in direct engagement with over twenty research institutions. Conversations and feedback have increased NIST's understanding of the current higher education research landscape and variations in research infrastructure. Three forms of engagement were used: one-on-one meetings with subject-matter experts, a request for comment, and research community dialogue.

One-on-one meetings were scheduled with individuals from universities, research security groups, and the leaders of relevant NIST programs. Each meeting consisted of brief introductions, an overview of the NIST directive in the CHIPS & Science Act, and a general discussion about the topic of cybersecurity for research. Many of these meetings resulted in referrals to additional contacts. Some discussions led to follow-up meetings to review programs or efforts within an organization that relate to the topic of cybersecurity for research.

A discussion session was hosted virtually to gain verbal thoughts and input about relevant cybersecurity challenges for research projects, information about existing resources, and thoughts on future resources. The listening session included attendees from different research security groups and universities. The Request for Comment (RFC) questions noted below were shared with attendees and used to guide the conversation.

An RFC was posted in April 2023 and open for public feedback until June 30, 2023. The RFC was posted to allow the public to give formal and written input about relevant cybersecurity challenges for research, information about existing cybersecurity resources, and thoughts on future resources to support the cybersecurity of research projects. The questions asked were categorized into the following three areas.

1. **Questions related to: *Cybersecurity Challenges and Risks***
    - What common cybersecurity challenges and risks does your institution face when conducting research?
    - 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?
2. **Questions related to: *Current Methods and Resources***
    - What other resources does your institution leverage to support cybersecurity risk management?
    - Are existing resources sufficient and effective? If not, why?
3. **Questions related to: *Recommendations for Future Work***
    - 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)?
        - What role might NIST play in providing resources and research to address common cybersecurity challenges and risks faced by these communities?
        - 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)?

## 2.3. Feedback Analysis

After the close of the RFC, analysis of feedback began. Written comments from the RFC were gathered into a spreadsheet. Information received from initial discovery, one-on-one meetings, the RFC, and the discussion session were compiled and discussed during several working sessions.

Analysis of the overall feedback helped identify common themes that would result in options for initial and potential future resources. As an initial resource, this document, NIST IR 8481, was developed to share the summarized findings and describe potential next steps for future resources to support the cybersecurity of research.

# 3. Summary of Feedback

Through a series of direct engagements with higher education cybersecurity and research security communities, as well as through comments received in response to NIST's April 2023 RFC, several takeaways have emerged regarding the status of research cybersecurity across higher education.

While institutions of higher education face many of the same cybersecurity challenges and risks as other communities, various factors make this community and their research practices unique. In particular, the top-down, command-and-control model of cybersecurity risk management that works for many enterprises in the public and private sectors does not translate well to the complex, highly distributed, and diverse web of functions, missions, and cultures that constitute the higher education community. Beyond the common challenges that plague the cybersecurity field as a whole (e.g., budget constraints, workforce shortages, and the ongoing need to keep up with a rapidly evolving technology landscape), cybersecurity professionals in higher education must also be prepared to address a heterogeneous set of risks across distinctive contexts of research, from neural psychology to space research. Despite these and other challenges, institutions report some early successes in operationalizing cybersecurity risk management strategies in partnership with researchers and offered specific recommendations to advance the state of cybersecurity across the research community.

The following subsections describe the risks, challenges, current cybersecurity risk management methods, and recommendations provided to NIST from institutions of higher education, including members of this community with specialized experience in securing research activities.

## 3.1. Cybersecurity Challenges and Risks

First, NIST sought to understand the common cybersecurity challenges and risks that institutions face when conducting research. The following themes emerged through feedback:

- **Awareness.** General cybersecurity awareness is lacking among researchers and institutional administrators. The cost of entry to gain that knowledge is high given the amount of time required to learn and the lack of tailored trainings, and there are limited incentives for researchers to bridge the awareness gap.
- **Workforce.** Research institutions face IT security workforce challenges, such as not having enough personnel, lacking qualified security personnel, and insufficient support or funding to develop research cybersecurity professionals with specialized experience. Along with limited security personnel, other challenges include high turnover and struggles to retain staff. Workforce retention can be challenging because of competition with industry and burnout due to the broad set of mission areas that the staff must support (e.g., teaching, learning, research, and community impact). Institutional cybersecurity teams are often not empowered or equipped to support bespoke cybersecurity support requests from researchers.
- **Culture clash.** A compliance culture can permeate higher education administrative teams in place of a risk management one. In parallel, centralized enterprise IT security management approaches do not translate well to highly distributed research environments. "One-size-fits-all" cybersecurity requirements imposed through research

agreements (e.g., grants, data use agreements, and contracts) can inhibit the efficient allocation of limited resources and create operational challenges, such as authentication requirements for research equipment that cannot accommodate authentication measures or physical access requirements imposed on principal investigators who are not responsible for or authorized to make physical access control decisions. Requirements in research agreements may not reflect or account for the unique characteristics of research environments, which can complicate compliance. Additionally, there are limited incentives in place to motivate researchers to take on the additional burden of security. For instance, the cost of securing certain types of devices, such as microscopes or some Internet of Things (IoT) devices, is prohibitively high and is not always perceived as a value-add by researchers.

- **Limited budgets for cybersecurity.** Institutions often struggle to provide the resources needed to establish and operate secure research environments. Funding is limited for secure research environments that require internal research networks, and building a specific research network is cost prohibitive. Agreement-based funding streams often do not support the measures required to secure data and equipment during and after project completion. Overall, the funding model for research, largely based on individual grants and contracts, is insufficient to develop and maintain effective research cybersecurity.
- **Complicated requirements landscape.** Higher education institutions must navigate a diverse regulatory environment given the broad set of functions they manage and the wide-ranging topics of research in which they engage. Cybersecurity requirements can be difficult to decipher, may vary widely across research agreements depending on the organization imposing them, and may not address the relevant risks for a given project, which can lead to confusion and inconsistent interpretations.
- **Rapid pace of innovation.** The rapid pace of technological innovation has had implications for three areas of concern for cybersecurity risk management in a research context: researchers with niche tool stacks that need to be protected, security professional capabilities, and the technologies available to adversaries. There is an ongoing need for tools to support modern and evolving research, which puts pressure on the security workforce to not only understand the tools but stay abreast of modern cybersecurity protections. Despite this need, intelligence handling (e.g., collection, analysis, dissemination, ingestion, and taking action) is a significant gap for this community, worsened by the fact that adversaries also benefit from technological advancements and do not face the same budget challenges as the higher education cybersecurity community. These factors, combined with the already steep learning curve security professionals must tackle to reach a baseline level of proficiency in cybersecurity risk management, further exacerbate the challenges enumerated above.

> ***"Our normal operations work in a deficit of funding and people."***
>
> *– Higher education respondent from the April 2023 Request for Comment*

Beyond these common cybersecurity challenges and risks faced by institutions, feedback indicated that the following fields of study present unique cybersecurity challenges and risks:

- Biotechnology
- Quantum computing
- Neural psychology
- Optical science
- Space research
- Engineering
- Clinical research in general

Challenges and risks that arise from these specific fields include:

- The handling of specialized, sensitive, and/or regulated data, such as protected health information (PHI), controlled unclassified information (CUI), and data related to International Traffic in Arms Regulations (ITAR), which may require additional controls, reporting, or education regarding usage
- The need for inter-institutional and international collaboration, which may require additional investments in identity and access management to appropriately support research while protecting confidentiality
- The distributed accountability for cybersecurity, which is reinforced through research agreement language and institutional processes, politics, and cultures
- The unique characteristics and configurations of the research equipment involved and the lack of secure storage and other tools that meet regulatory and contractual requirements
- The lack of institutional capacity to support required research tools (e.g., Research Electronic Data Capture, or REDCap)

## 3.2. Current Methods and Resources

NIST also sought to better understand how institutions currently identify, assess, manage, and reduce cybersecurity risks related to conducting research, including the extent to which existing resources provided by NIST and other organizations support risk management activities. The institutions that provided feedback to NIST reported the use of defense-in-depth and risk-based approaches that generally emphasize strong governance and the implementation of both administrative and technical controls.

Governance often involves collaboration between IT/cybersecurity and sponsored research offices, and governance processes intended to support risk identification and management include the consideration of research data, which helps to foster risk-based approaches to cybersecurity in research contexts. Administrative controls can include policies, processes, efforts to instill a culture of cybersecurity risk management, and ongoing education for faculty, researchers, students, and administrators.

Technical controls can include the continuous monitoring of networks and systems, log collection and analysis, the management of secure storage systems, strong authentication, endpoint management, and elevated security for high-risk systems. Some respondents also said

that they rely on sharing threat information and best practices with similar research and education (R&E) institutions.

Respondents cited use of the NIST Risk Management Framework (RMF), NIST Special Publication (SP) 800-171, and SP 800-53 for general cybersecurity risk identification and management purposes, which then inform institutional approaches for risk management in research contexts. One respondent noted that available NIST resources allow for agility in mitigating cybersecurity risks and considering the unique cultural, statutory, and historical needs of the institution. Respondents also cited resources from others in the higher education community. See Appendix A for a non-exhaustive list of available resources.

Regarding the sufficiency and effectiveness of available resources, feedback indicated that institutions are challenged less by the availability of cybersecurity risk management resources and more by cultural, workforce, budgetary, policy, and other operational barriers that prevent effective and consistent operationalization of cybersecurity risk management strategies across research contexts.

Respondents indicated that because research cybersecurity — including the development of research cybersecurity professionals — has not been prioritized, the burden of frontline IT/cybersecurity often falls to research staff, including graduate students or other partners and contributors whose affiliation may not be with the institution or whose participation may be transient. Current cybersecurity resources largely speak to an audience of IT/cybersecurity professionals, and while general cybersecurity education materials and awareness trainings exist, they have not been designed with researchers in mind.

## 3.3. Recommendations for Future Work

The final question in the RFC requested feedback on potential new resources and areas of further research that might address common cybersecurity challenges and risks. The following thematic areas emerged from comments and community engagement:

- **Targeted cybersecurity resources.** Cybersecurity guidance is available to address several topic areas, including specific attacks (e.g., social engineering, phishing, ransomware, supply chain) and security risk management practices. However, tailoring existing cybersecurity guidance for use by researchers who do not have a cybersecurity background could be particularly useful in facilitating engagement between researchers and cybersecurity professionals within and across research institutions. Resources could be developed that are specific to particular fields of research and could emphasize the risks, impacts, and importance of applying cybersecurity within the research context.
- **Collaborative engagements.** Collaboration between groups and communities can provide opportunities for information sharing, innovation, and efficient problem solving. The feedback emphasized the importance of collaborating with existing research communities and the need for more collaboration with Federal Government entities.

  There are several groups that are addressing some of the challenges faced by the research community. Working with these existing groups can help bolster awareness, engagement, and collaboration across the higher education research and cybersecurity communities. Some of the existing groups include:

- EDUCAUSE Higher Education Information Security Council (HEISC)
- NSF-funded Regulated Research Community of Practice (RRCoP)
- Trusted CI: The NSF Cybersecurity Center of Excellence
- REN-ISAC
- The National Laboratories

With regard to research, government agencies can play different roles (e.g., grantor, guidelines provider, resource distributor). Through collaboration with the research community, government agencies can better align their guidance, resources, and grants to the research environment.

- **Trainings.** Training provides individuals with the opportunity to grow their knowledge base, improve their skills, and become more effective in a particular field. Training resources designed for researchers and their teams could raise awareness about the importance of cybersecurity, particularly cybersecurity's value in preserving data integrity. With information about the impact and importance of secure research, researchers may be more willing to work with their institution's security officers to ensure limited impact on their research experiments. Training could take the form of online training, webinars, and conferences that focus on the cybersecurity tools available to support secure research.
- **Guidance for frameworks.** Frameworks are intended to provide structured guidance for building upon a system or a concept. Feedback did not specifically request more frameworks but rather further development of existing frameworks for institutional planning and implementation of research cybersecurity services. Tailoring certain frameworks to support research environments could help ease the integration of cybersecurity while simplifying the process and minimizing operational overhead.
- **Grant guidance for security compliance.** Frameworks and other structured guidance are sometimes used to create complex compliance requirements for grantees interested in applying or participating in specific research opportunities, which may be unrealistic for higher education research institutions. The research community expressed the need for effective grant writing guidance that considers security, compliance, and research environments hosted at higher education institutions.
- **Shared services support.** To meet cybersecurity needs or compliance requirements, research institutions need access to cybersecurity capabilities and services (e.g., secure enclaves, security operations centers or SOCs, data protection tools, etc.). Some institutions may not have the resources or funding to maintain a robust cybersecurity program on their own. It is in the public interest to ensure that scientific exploration remains open and accessible and that research opportunities are not limited to those institutions with the most robust in-house cybersecurity risk management and research compliance capacities. There are risk management models that support a thriving research ecosystem and achieve cybersecurity objectives without passing most of the burden onto individual performers and their host institutions. For example, organizations with well-established programs and services can help support the cybersecurity needs of smaller or disadvantaged research institutions. Funding organizations can also manage

462 common research infrastructures and services to more consistently apply cybersecurity
463 protections across the community. Increasing awareness of available shared service
464 opportunities and developing trusted cybersecurity services can help mitigate limited
465 cybersecurity budgets for many institutions.

466

# 4. Potential Next Steps for NIST

To help qualifying institutions of higher education identify, assess, manage, and reduce cybersecurity risks related to conducting research, NIST could pursue the following activities:

- Community-specific cybersecurity resources
    - Determine whether additional cybersecurity resources can be tailored for a general audience, such as a repeatable process that can be applied per research activity or project.
    - Determine whether additional cybersecurity resources can be tailored for specific fields of study, particularly those areas highlighted as having unique cybersecurity challenges (e.g., clinical research settings in general, biotechnology, quantum computing, neural psychology, optical science, space research, engineering). Examples of this type of work are referenced under the National Cybersecurity Center of Excellence (NCCoE) bullet in Appendix A.1.
- Coordination
    - Coordinate with other federal agencies on cybersecurity for research contexts, and promote consistent application of NIST guidance.
    - Identify mechanisms to sustain NIST's institutional collaboration with the higher education cybersecurity and research communities, build on progress, and identify gaps where additional focus from NIST would be appropriate and mission-aligned.
- Capacity-building
    - Identify opportunities to advise on content that could support cybersecurity trainings customized for a research context and audience.
    - Evaluate the role that the National Initiative for Cybersecurity Education (NICE) Program could play in building capacity in research cybersecurity.

# Appendix A. Existing Cybersecurity Resources

The higher education research community is encouraged to consider how existing cybersecurity resources could be leveraged to support the identification, assessment, management, and reduction of cybersecurity risks related to conducting research.

## A.1. NIST Resources

Some institutions cited specific NIST resources for managing cybersecurity risks, including:

- SP 800-37r2 (Revision 2), *The Risk Management Framework* (RMF): https://csrc.nist.gov/projects/risk-management/about-rmf
- SP 800-53r5, *Security and Privacy Controls for Information Systems and Organizations*: https://doi.org/10.6028/NIST.SP.800-53r5
    - SP 800-53Ar5, *Assessing Security and Privacy Controls in Information Systems and Organizations*: https://doi.org/10.6028/NIST.SP.800-53Ar5
- SP 800-171r2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*: https://doi.org/10.6028/NIST.SP.800-171r2
    - SP 800-171r3 ipd (initial public draft) is available and in progress: https://doi.org/10.6028/NIST.SP.800-171r3.ipd

Additional NIST resources may be relevant to support cybersecurity risk management in research contexts, including:

- The Cybersecurity Framework: https://www.nist.gov/cyberframework
- The Privacy Framework: https://www.nist.gov/privacy-framework
- Getting Started with Cybersecurity Risk Management: Ransomware: https://csrc.nist.gov/files/pubs/other/2022/02/24/getting-started-with-cybersecurity-risk-management/final/docs/quick-start-guide--ransomware.pdf
- NIST Interagency Report (IR) 8374, *Ransomware Risk Management: A Cybersecurity Framework Profile*: https://doi.org/10.6028/NIST.IR.8374
- SP 800-30r11, *Guide for Conducting Risk Assessments*: https://doi.org/10.6028/NIST.SP.800-30r1
- SP 800-223 ipd, *High-Performance Computing (HPC) Security: Architecture, Threat Analysis, and Security Posture*: https://doi.org/10.6028/NIST.SP.800-223.ipd
- SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*: https://doi.org/10.6028/NIST.SP.800-218
- The Research Data Framework (RDaF): https://www.nist.gov/programs-projects/research-data-framework-rdaf
- SP 800-63, *Digital Identity Guidelines*: https://doi.org/10.6028/NIST.SP.800-63-3
    - Revision 4 ipd is in progress: https://pages.nist.gov/800-63-4/

- National Cybersecurity Center of Excellence (NCCoE) projects and practice guides demonstrate how NIST guidance can be implemented and provide reference architectures to address cybersecurity challenges:
    - Trusted Cloud: VMware Hybrid Cloud IaaS Environments: https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments
    - Mobile Device Security: Bring Your Own Device: https://www.nccoe.nist.gov/mobile-device-security/bring-your-own-device
    - Data Security: https://www.nccoe.nist.gov/data-security
    - Cybersecurity of Genomic Data: https://www.nccoe.nist.gov/projects/cybersecurity-genomic-data
    - Cybersecurity for the Space Domain: https://www.nccoe.nist.gov/cybersecurity-space-domain

## A.2. Internal Support Provided by Institutions of Higher Education

Institutional resources may be available to researchers and their affiliates through institution-specific guidance documents, planning tools, trainings, and managed technology services. For example:

- University of California, Irvine OIT Service Catalog, Research Category: https://www.oit.uci.edu/services/research/
- University of Colorado at Colorado Springs Guidance Cookbook: https://oit.uccs.edu/security/ResearchComplianceResources
- University of Delaware Secure UD Research Security Plan Tool: https://www1.udel.edu/security/research/
- University of Georgia Office of Research: https://research.uga.edu/research-security/controlled-unclassified-information/
- University of Michigan Research Information Security Oversight (RISO) Program: https://research-compliance.umich.edu/research-information-security/controlled-unclassified-information-cui
- Indiana University SecureMyResearch Initiative: https://cacr.iu.edu/projects/SecureMyResearch/index.html
- Oklahoma State Research Compliance and Data Services Resources: https://research.okstate.edu/faculty-resources/research-compliance-overview.html https://research.okstate.edu/faculty-resources/research-data-services.html
- Texas A&M University Secure Technologies for Aggie Research (STAR) Platform: https://it.tamu.edu/star/
    - Data Classification Tool: https://it.tamu.edu/community/tools/data-classification.php

- TAMUS Secure Enclave: https://it.tamu.edu/services/academics-and-research/research/available-research-resources/

## A.3. Research and Education Community Resources

Resources and services may also be available through other members of the R&E community and federal agencies. For example:

- Higher Education Community Vendor Assessmenct Toolkit (HECVAT), developed jointly by the Higher Education Information Security Council (HEISC) Shared Assessments Working Group, Internet2, and REN-ISAC: https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit#tools
- Trusted CI Framework, Implementation Guide for Research Cyberinfrastructure Operators, templates, and other tools: https://www.trustedci.org/framework
- Indiana University-hosted OmniSOC: https://omnisoc.iu.edu/index.html
- Research & Education Networks Information Sharing and Analysis Center (REN-ISAC): https://www.ren-isac.net/
- National Institutes of Health (NIH) Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability (STRIDES) Initiative: https://cloud.nih.gov/about-strides/

## Appendix B. Selected Bibliography


- AAU and APLU (2020). University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus. Available at https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf
- AAU (2020) AAU Science and Security Resources. Available at https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Science-and-Security-Resource-Document.pdf
- CHIPS and Science Act of 2022, Pub. L. No. 117-167 (2022). https://www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf
- Cybersecurity & Infrastructure Security Agency (2023) Advanced Persistent Threats and Nation-State Actors: Helping cybersecurity defenders protect against and respond to APTs. Available at https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors
- Congressional Research Service (2022) Federal Research and Development (R&D) Funding: FY2023. Available at https://crsreports.congress.gov/product/pdf/R/R47161
- Congressional Research Service (2022) Federal Scientific Integrity Policies: A Primer Available at https://crsreports.congress.gov/product/pdf/R/R46614
- Director of the National Counterintelligence and Security Center, National Security Presidential Memorandum/NSPM-28, The National Operations Security Program, 13 January 2021, Washington DC, 2021.
- Flagg M and Arnold Z (2021). A New Institutional Approach to Research Security in the United States: Defending a Diverse R&D Ecosystem. Available at https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states/
- Forum of Incident Response and Security Teams (FIRST) (2019) Common Vulnerability Scoring System version 3.1 Specification Document, Revision 1. Available at https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf
- General Services Administration (2022) Advanced Persistent Threat Buyer's Guide. Available at https://www.gsa.gov/system/files/APT_Buyers_Guide_v2_July_2022.pdf
- Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800- 30r1
- Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2
- Joint Task Force (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology,

Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

- Mandiant (2023) Advanced Persistent Threats (APTs). Available at https://www.mandiant.com/resources/insights/apt-groups
- MITRE (2023). ATT&CK Groups. Available at https://attack.mitre.org/groups/
- National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6
- National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/privacy-framework/privacy-framework
- National Initiative for Cybersecurity Education (2020) NICE Framework Resource Center. Available at https://www.nist.gov/nice/framework
- National Science and Technology Council, "Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise," Subcommittee on Research Security, Joint Committee on the Research Environment, 2021.
- National Science and Technology Council, "Critical and Emerging Technologies List Update," Executive Office of the President of the United States, 2022.
- National Science and Technology Council, "Guidance for Implementing National Security Presedential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government Supported Research and Development," Subcommittee on Research Security, Joint Committee on the Research Environment, 2022.
- Oldehoeft, A (1992). Foundations of a Security Policy for Use of the National Research and Educational Network. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (NISTIR) 4734. https://doi.org/10.6028/NIST.IR.4734
- Petersen, R., Santos, D., Smith, M., Wetzel, K., Witte, G. (2020). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181-1. Available at https://doi.org/10.6028/NIST.SP.800-181r1
- SBIR and STTR Extension Act of 2022, Pub. L. No. 117-183 (2022).
- Shankar A. and Drake W. (2022). *Effective Cybersecurity for Research*. Available at https://library.educause.edu/-/media/files/library/2022/6/researchcybersecurity.pdf
- The MITRE Corporation (2019) ATT&CK. Available at https://attack.mitre.org
- The White House, "National Security Presidential Memorandum - 33 on United States Goverment-Supported Research and Development National Security Policy," trumpwhitehouse.gov, 2021.

663 • Tiffert G. et. al. (2020). Global Engagement. Rethinking Risk in the Research
664 Enterprise, ed Tiffert G. (Hoover Institution Press, Stanford, CA). Available
665 at https://www.hoover.org/sites/default/files/research/docs/tiffert_globalengagement_full
666 _0818.pdf.
667 • National Institute of Standards and Technology (2023). Cybersecurity for R&D Request
668 for Comment. Available at https://www.nist.gov/cybersecurity/cybersecurity-rd-request-
669 comment