Evolving Information Technology & Innovation at NSF

Terry Carpenter
Chief Information Officer (CIO)

Linnea Avalone
Chief Officer for Research Facilities

October 26, 2023

NSF's Approach to Research Ecosystem Cybersecurity

- By design NSF generally avoids being prescriptive
- Cybersecurity is the responsibility of the awardee
- NSF's oversight responsibilities include ensuring due diligence w/regard to cybersecurity

<u>Principles Informing Expectations for Research Cybersecurity:</u>

- Must rapidly adapt with changes in policy, practices and adversary activity.
- Requires a programmatic approach in contrast to a handful of transactional practices.
- Must support protection of vital national assets.
- Requires engagement with facility leadership.
- Must provide sufficient and timely information about the planned and executed cybersecurity activities to comply with NSF oversight.

Research Facility Resilience

With the sophistication of modern, state sponsored or facilitated attacks, breaches of accounts and systems are inevitable. Resilience for a research facility consists of:

- Minimize the likelihood of successful attacks in general, and unsophisticated, opportunistic attacks specifically.
- Minimize the impact of even sophisticated attacks by constraining the 'blast radius' or ability to spread throughout a facility.
- Minimize the period of the disruption of scientific operations.
- Ensure the integrity of scientific data and artifacts despite the occurrence of a cybersecurity incident.

Zero Trust Architecture and Risk Management Frameworks help to guide partners to manage resilient facilities

Questions from the NIST ISPAB

- **Cybersecurity requirements for NSF research programs**
- Cybersecurity guidance, policy or programs that USG research agencies use or could use
- Issues that drove NSF efforts in this area
- General guidance being developed for research security

Cybersecurity Requirements for Programs with Facilities

Major facilities are not managed or operated by NSF

- Cybersecurity is a legal the obligation of the awardee (managing organization).
- NSF focuses on ensuring awardees have appropriate cybersecurity policies and practices
- NSF is updating cybersecurity expectations, requirements, and review process for major and mid-scale facilities.

Currently cybersecurity requirements for programs with facilities include:

- Awardees with research facilities are required to provide an initial cybersecurity plan w/in 90 days of an award.
- New guidance on what constitutes an acceptable cybersecurity plan may include,
  - Explicit statement of chosen standard or framework
  - Detailed cybersecurity risk register
  - Line itemed cybersecurity budget
- Cybersecurity performance is an element of each facility's formal review.

Cybersecurity Requirements for General Awardees

NSF Proposal & Award Policies & Procedures Guide (PAPPG)

II.D.2.i(ii) Plans for Data Management and Sharing of the Products of Research

Proposals must include a document of no more than two pages uploaded under "Data Management Plan" in the supplementary documentation section of Research.gov. This supplementary document should describe how the proposal will conform to NSF policy on the dissemination and sharing of research results (see Chapter XI.D.4), and may include:

- the types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project;
- the standards to be used for data and metadata format and content (where existing standards are absent or deemed inadequate, this should be documented along with any proposed solutions or remedies);
- policies for access and sharing including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements;
- policies and provisions for re-use, re-distribution, and the production of derivatives; and
- plans for archiving data, samples, and other research products, and for preservation of access to them

IX.C Research Security

In accordance with the Guidance for Implementation of National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, the Foundation requires the following post-award updates to current and pending support information after issuance of an NSF award:

- Post-award Disclosure of Current Support and In-Kind Contribution Information (includes biographical information on senior personnel)
- Update of Current Support in Annual and Final Project Reports (includes biographical information on senior personnel)

Questions from the NIST ISPAB

- Cybersecurity requirements for NSF research programs
- **Cybersecurity guidance, policy or programs that USG research agencies use or could use**
- Issues that drove NSF efforts in this area
- General guidance being developed for research security

NSF Research Cybersecurity – Programs & Investments

NSF funds a rich portfolio of programs that support research cybersecurity, for example

- CI-Compass, cyberinfrastructure and data management
  https://ci-compass.org
- TrustedCI, cybersecurity and cybersecurity program assessment
  https://www.trustedci.org
- Regulated Research Community of Practice, with participation by 270+ institutions
  https://www.regulatedresearch.org

NSF Research Cybersecurity Programs

- TrustedCI – NSF Cybersecurity Center of Excellence
  https://www.trustedci.org
  - Lead development of an NSF Cybersecurity Ecosystem with the workforce, knowledge, processes, and cyberinfrastructure that enables trustworthy science and NSF's vision of a nation that is a global leader in research and innovation.
  - Accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

- CICI - NSF CISE OAC Cybersecurity Innovation for Cyberinfrastructure
  - Supports research on securing scientific data, workflows and infrastructure in three focus areas: usable and collaborative security for science; reference scientific security datasets; and transition to cyberinfrastructure resilience
    https://www.nsf.gov/pubs/2023/nsf23517/nsf23517.htm

NSF Investments in ‘Research on Research Cybersecurity’

Office of Advanced Cyberinfrastructure investment examples:

- Cyber Reasoning System: Scientific binary vulnerability detection and auto patching (ASU)
- ARMOR: Computing / search on encrypted data in HPC (Augusta)
- SciAuth: Deploying Interoperable and Usable Authorization Tokens (UIUC)
- Vulnerability Detection in Configurable Scientific Computing (Utah)
- Open Science Chain for Protecting Integrity and Provenance of Research Data (UCSD)

Questions from the NIST ISPAB

- Cybersecurity requirements for NSF research programs
- Cybersecurity guidance, policy or programs that USG research agencies use or could use
- **Issues that drove NSF efforts in this area**
- General guidance being developed for research security

Issues that Drove NSF Research Cybersecurity Efforts

- Stewardship for critical national assets and recognizing the essential role cybersecurity plays in supporting our national and scientific competitiveness
- Growing concerns over national security implications for Federally funded research (as seen in NSPM-33 and the threat from foreign 'talent' programs)
- General recognition that due to the independence and heterogeneous nature of major facilities, greater coordination and normalization of practice was warranted.

- Resulted in
  - The JASON study that forms basis for our current efforts https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/index.jsp
  - Established the *Office of the Chief of Research Security Strategy and Policy*

Perspective on Different Cultures

Higher Education	Defense Industrial Base (DIB)
Core mission: education, research, public service (non-profit)	Profit motive
Open, peer reviewed science	Closed, intellectual property
Integrated teaching/research environments	Restricted staff and personnel
Highly decentralized administrative and research environments	Project / product focused
Fundamentally collaborative	Centralized span of control

Questions from the NIST ISPAB

- Cybersecurity requirements for NSF research programs
- Cybersecurity guidance, policy or programs that USG research agencies use or could use
- Issues that drove NSF efforts in this area
- **General guidance being developed for research cybersecurity**

General Guidance in Development for Research Cybersecurity

Research Infrastructure Guide (for major research facilities) Update in 2024

- Adds a new section on cybersecurity
  - Current draft: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf21107
- Recognition that cybersecurity must support and adapt to research workflows
- Focused on building resilience and identifying facility specific risks for tailored mitigation.

NSF Cybersecurity Advisor for Research Infrastructure

- New position at NSF in 2023
  - Reports to the Chief Officer for Research Facilities
  - Created in response to the JASON report of 2021 https://www.nsf.gov/news/special_reports/jasonreportcybersecurity/index.jsp
- Three tracks of responsibilities
  - Ensure completion of JASON report recommendations
  - Assist NSF in refining and maturing its cybersecurity posture for major facilities
  - Resource for program officers and research facility operators


NSF

TrustedCI – NSF Cybersecurity Center of Excellence

The Framework Core

- Designed to be applicable in any environment and useful for any organization
- **4 Pillars** make up the foundation of a competent cybersecurity program
  - Mission Alignment
  - Governance
  - Resources
  - Controls
- **16 Musts** identify the concrete, critical requirements for establishing and running a competent cybersecurity program

The Trusted CI Framework

Four Pillars. Sixteen Musts. An Architecture for Cybersecurity Programs

Mission Alignment

1. Organizations must tailor their cybersecurity programs to the organization's **mission**.
2. Organizations must identify and account for cybersecurity **stakeholders and obligations**.
3. Organizations must establish and maintain **documentation of information assets**.
4. Organizations must establish and implement a structure for **classifying information assets** as they relate to the organization's mission.

Governance

5. Organizations must **involve leadership** in cybersecurity decision making.
6. Organizations must formalize roles and responsibilities for cybersecurity **risk acceptance**.
7. Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
8. Organizations must ensure the cybersecurity program **extends to all entities** with access to or authority over information assets.
9. Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policy**.
10. Organizations must **evaluate and refine** their cybersecurity programs.

Resources

11. Organizations must devote **adequate resources** to address unacceptable cybersecurity risk.
12. Organizations must establish and maintain a cybersecurity **budget**.
13. Organizations must allocate **personnel** resources to cybersecurity.
14. Organizations must identify **external cybersecurity resources** to support the cybersecurity programs.

Controls

15. Organizations must adopt and use a **baseline control set**.
16. Organizations must select and deploy **additional and alternate controls** as warranted.

Different Cybersecurity Approaches

	Higher Education	DIB
Security Approach	Project-based security	Institutional based-security
Facilities	Open access	Designed to restrict
Export Control	Specific USML / CCL Controls	Broad facility-wide controls
Management	Decentralized	Centralized
Training	Specific training only for privileged access	Facility-wide training
Interpretive burden	Broad knowledge of all USML / CCL	Specific product knowledge of USML / CCL
Foreign Population	Large, from every country	Limited
Academic Freedom	Presumption everything is public	Presumption everything is restricted

U.S. Munitions List (USML)
Commercial Control List (CCL)