Cybersecurity at NSF Major Facilities
Executive Summary

Contact: Gordon Long — glong@mitre.org

JSR-21-10E

October 2021

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102-7508
(703) 983-6997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
October 2021	Technical	

4. TITLE AND SUBTITLE

Cybersecurity at NSF Major Facilities Executive Summary

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER
1321JAPM

5e. TASK NUMBER
PS

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
JASON Program Office
7515 Colshire Drive
McLean, Virginia 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

JSR-21-10E

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Science Foundation, Office of Director
2415 Eisenhower Avenue
Alexandria, Virginia 22314

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

JASON was charged by the NSF to understand their current approach to managing cybersecurity at its major facilities, to assess the major risks associated with inadequate or overly-constraining cybersecurity requirements, and to recommend any changes deemed appropriate in NSF's policy or procedures.

The issue to be addressed is the degree to which NSF should maintain or modify its present approach to oversight of cybersecurity. These are the largest scientific installations that NSF supports.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. James Ulvestad
UNCL	UNCL	UNCL	UL	10	**19b. TELEPHONE NUMBER** *(include area code)* 703-292-7165

1 EXECUTIVE SUMMARY

Cybersecurity is a significant and growing concern across the public and private sector. Database breaches are commonly in the news, and phishing emails frequently appear in our inboxes. In 2021, sophisticated ransomware attacks threatened gas supply to the US East Coast and shut down the computer systems of thousands of small to medium size businesses. In response to these threats, organizations are adding layers of cybersecurity, such as firewalls, encryption, and multi-factor authentication. These measures, however, have significant costs, including increased friction for users. With threats real and growing, finding the appropriate balance between security, cost, and burden to users is a continual challenge.

National Science Foundation (NSF) major facilities are critical scientific platforms used by a wide range of scientific communities to collect and distribute scientific data. They are the largest class of investments made by the agency, but across this class, they are very diverse. Facilities may be comprised of distributed sensors, or may be a single telescope. They may be run by a single institution or by many institutions. New facilities are being built today, while others are almost 50 years old. Operating budgets vary by more than an order of magnitude.

A key feature that distinguishes NSF major facilities from other federal science facilities is that NSF is not typically the owner nor the operator. Instead, NSF oversees the cooperative agreements that are the primary mechanism by which the major facilities are funded.[1] The operators, personnel and users of these NSF-funded facilities are not federal government employees. Because of this oversight model, NSF's involvement with cybersecurity

[1] US Antarctic Program is the exception, supported via contract. See Section 5.1.1.

issues to date has been limited in scope and detail; facility operators have had the responsibility for assessing risks and implementing controls.

JASON was charged by the NSF to understand their current approach to managing cybersecurity at its major facilities, to assess the major risks associated with inadequate or overly-constraining cybersecurity requirements, and to recommend any changes deemed appropriate in NSF's policy or procedures.

This study was informed by four days of briefings and additional virtual meetings between January and July 2021 with NSF staff, major facility leadership and information technology staff, DOE and NASA laboratory cybersecurity managers, NIST cybersecurity professionals, and the FBI. Documents from NSF, major facilities, and other public sources were also an important source of information.

JASON makes the following findings and recommendations on cybersecurity at NSF major facilities.

Findings

1. In common with other federal science facilities, NSF major facility data are to be openly shared; confidentiality is not a primary goal. Instead, the principal cybersecurity concerns are data availability and integrity, continuity of service, and in some cases, physical safety.

2. Though successful high-consequence attacks have yet to be reported, NSF major facilities regularly experience cyber attacks. New types of attacks also merit consideration: ransomware; coordinated attacks, especially Advanced Persistent Threats (APT); and supply-chain techniques that might use facilities as intermediate targets.

3. Well-established best practices exist for cybersecurity. Technical approaches include system segmentation, immediate application of patches, adherence to the principle of least privilege, multi-factor authentication, and intrusion monitoring. Also needed are continuous monitoring of threats; training for users; governance and communications that support the balancing of cyber risks, mission, and cost; and planning for cybersecurity incident response.

4. Cybersecurity needs at major facilities are not unique compared to industry or other federal agencies in terms of the threats and the technical approaches needed to counter these threats. Similarly, as in most enterprises, facility users and personnel are highly variable in their understanding of cybersecurity issues.

5. The primary unique aspect of cybersecurity for NSF's major facilities, compared to science centers run by other federal agencies, is NSF's management approach, characterized by:

    - operations distributed across many organizations;
    - funding primarily via cooperative agreement, as opposed to contract;
    - wide spectrum of major facility size, age, budget, infrastructure type, staffing level; and
    - a lean financial model that minimizes overhead spending.

6. Major facilities differ substantially as to the state of cyberinfrastructure, which in turn impacts the ability to implement cybersecurity controls. Newer facilities have largely been able to take cybersecurity into account as they developed their cyberinfrastructure. Some older facili-

ties will require cyberinfrastructure modernization in support of cybersecurity goals.

7. To adequately respond to the rapidly changing threat landscape, all major facilities must sustain and continually evolve their cybersecurity practices.

8. NSF's current approach of offering independent external advice on cybersecurity is valuable. This mechanism can provide facility operators with needed expertise and allows for frank conversations about cybersecurity challenges outside of the NSF review processes. However, this approach does not ensure that cybersecurity best practices are consistently implemented and evolved in response to the changing threat landscape, nor does it support NSF Program Officers in their decision making.

9. The present approach to cybersecurity oversight offers valuable flexibility and reduced effort for review and reporting, but may leave major facilities unprepared to prevent and respond to cyber attacks. NSF has reputation risk due to the potential for physical harm and for loss of confidence of users and decision makers.

10. Overly prescriptive cybersecurity requirements could add administrative burdens and costs, and may slow scientific progress.

11. As major facilities shift to using cloud computing and storage, cybersecurity responsibility and control will be increasingly shared with cloud providers.

12. With future facilities expected to include more corporate, government and non-profit partners, cybersecurity policy and management will become more complex.

13. Some facilities have technologies or collect some data with potential national security concerns, and these must be properly managed. Avoiding collection and/or storage of potentially sensitive data may be the best approach.

Recommendations

1. NSF should maintain its current approach of supporting major facilities to enhance cybersecurity through assessments of risk, and development and implementation of mitigation plans. A prescriptive approach to cybersecurity should be avoided because it would be a poor fit to the diversity of facilities, would inefficiently use resources, and would not evolve quickly enough to keep up with changing threats.

2. An executive position for cybersecurity strategy and coordination for major facilities should be created at NSF. This executive should have authorities that allow them to continually support the balancing of cybersecurity, scientific progress, and cost in the distinct ways that will be appropriate for each facility.

3. Using annual reporting and review processes, NSF should ensure major facilities implement robust cybersecurity programs that remain consistent with current best practice.

4. NSF should develop a procedure for response to major cybersecurity incidents at its major research facilities, encompassing public relations, coordination mechanisms, and a pre-ordained chain of authority for emergency decisions. Each major facility should also have their own response plan that is both specific to its needs and consistent with NSF's plan.

5. NSF and the major facilities must be adequately resourced for their cyberinfrastructure and cybersecurity needs. What is appropriate will depend on each facility's unique characteristics and specific needs. The cybersecurity budget should be commensurate with perceived risk of an event, which may be unrelated to the cost of constructing or operating the facility.

6. NSF should refine facility proposal and design review processes to ensure that new major facilities plan cybersecurity as an integral part of the information technology infrastructure. NSF should regularly review the cybersecurity plans and efforts of both new and existing major facilities. Shifts to cloud-based cyberinfrastructure and to a wider range of partners will impact cybersecurity planning and need to be considered at proposal time.

7. NSF should remain aware of national security concerns regarding its facilities and continue to facilitate coordination with appropriate agencies.