National Science Foundation • Office of Inspector General
4201 Wilson Boulevard, Arlington, Virginia 22230

MEMORANDUM

DATE: July 21, 2016

TO: Amy Northcutt
Chief Information Officer
Office of Information and Resource Management

FROM: Marie A. Maguire
Assistant Inspector General for Audit (Acting)

SUBJECT: NSF OIG Report No. 16-3-006, *Report on the National Science Foundation's Covered Systems under the 2015 Cybersecurity Act*

Attached is the final report on NSF's access control policies, procedures, and practices as required by Section 406 of the Cybersecurity Act of 2015.

Based on the information NSF provided, we conclude that NSF's policies and practices for access controls appeared to generally reflect appropriate standards. However, we did not verify or test the effectiveness of the access controls that NSF reported that it uses to protect its systems and applications from unauthorized users. The report contains no findings or recommendations.

We appreciate the courtesies and assistance provided by your staff during the review. If you have any questions, please contact Elizabeth Goebels, Acting Director of Performance Audits, at (703) 292-8483 or Kelly Stefanko, Audit Manager, at (757) 962-6922.

Attachment

cc: Dorothy Aronson
Daniel Hofherr
Mary Lou Tillotson
Maria Zuber
Allison Lerner
Elizabeth Goebels
Kelly Stefanko
Christina Sarris
John Anderson
Michael Van Woert

Report on the National Science Foundation's Covered Systems under the 2015 Cybersecurity Act

National Science Foundation

Office of Inspector General

July 21, 2016

OIG 16-3-006

Results in Brief

Preventing access to an agency's systems by unauthorized users is the primary purpose of logical access controls. Section 406 of the Cybersecurity Act of 2015[1] requires Inspectors General for agencies with covered systems[2] to: 1) describe the logical access[3] policies and practices used to access a covered system; 2) describe and list the agency's access controls; 3) explain the reasons for not using access controls, if applicable 4) describe the agency's information security management practices; and 5) describe agency policies designed to ensure that entities, including contractors that provide services to the agency, implement information security practices.

The statute also requested Inspectors General to determine whether the agency's access policies and procedures reflected appropriate standards. Therefore, we reviewed NSF's Fiscal Year (FY) 2015 Federal Information Security Management Act (FISMA), assessment report, which found no material weaknesses in NSF's compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

Based on the information NSF provided, we conclude that NSF's policies and practices for access controls appeared to generally reflect appropriate standards. However, we did not verify or test the effectiveness of the access controls that NSF reported that it uses to protect its systems and applications from unauthorized users, because verification or testing was not required by the Cybersecurity Act of 2015.

Information Requested by the Cybersecurity Act of 2015

The following report generally describes the agency's policies, procedures and practices for the five items required in Section 406 of the Cybersecurity Act of 2015. A complete list of the access control policies and procedures NSF provided in response to our request is attached.

1. Access Policies and Procedures

In response to our request, NSF provided its access policies, many of which are contained in its *Information Security Handbook.* The *Handbook* states that the agency reviews and updates its access control policy every five years[4] and reviews and updates access control procedures every two years, unless the Chief Information Security Officer requires an earlier update.

In addition, the Handbook describes the roles and responsibilities of personnel responsible for ensuring that access control requirements are followed. NSF's access policies include requirements for creating network access for new employees and deleting access for departing personnel (including those under the Intergovernmental Personnel Act (IPAs)), determining the

[1] Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113 (2015).
[2] Covered systems include systems that provide access to personally identifiable information (PII), such as name, social security number, or biometric records.
[3] Logical access controls are system or application based. This report addresses logical access controls as required by the statute and will refer to these controls as access controls throughout this report. Physical access controls refer to such things as locking rooms where servers are located.
[4] The most recent update was dated April 2016.

appropriate role and access for users of NSF's systems, establishing usage restrictions for mobile devices and wireless access, and authorizing individuals to post information on NSF's publicly accessible systems.

With respect to access practices, NSF stated that it follows the principle of least privilege; that is, it limits users to the access that is necessary for them to accomplish their assigned tasks. Other practices NSF reported included requiring administrative managers to review and recertify that users' levels of access to systems reflect current job responsibilities, using automated mechanisms to investigate and respond to suspicious activity, and reviewing information system audit records weekly for indications of misuse or unapproved access.

2. Access controls

NSF's policy includes two major access controls: multi-factor authentication and timed lock out. First, NSF uses multi-factor authentication to allow users to access its network and many of NSF's covered systems are only accessible within the network. [redacted] Multi-factor authentication is the use of two or more types of identification, such as a personal identification number, Personal Identity Verification (PIV) Card[5], and/or a fingerprint, to authenticate users. Second, NSF's lock out policy blocks a user's access to NSF's systems after an incorrect password or other information is entered [redacted]

To provide insight on the quality of NSF's access controls, we note that NSF's FY 15 FISMA assessment contained management letter findings related to password controls for certain administrative accounts for NSF's financial system, timely removal of information technology accounts for separated employees, and documentation of approval to access NSF's system used to process award proposals.

3. Reasons for not using such logical access controls or multi-factor authentication

As noted above, NSF uses multi-factor authentication to access its network and many of NSF's covered systems are only accessible within the network. [redacted] NSF also stated that it is implementing software to require PIV card validation of unprivileged network accounts before an individual can access the local privileged account.

[5] A PIV card is a physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials.

4. Information security management practices

Policies and Procedures to Conduct Inventories of the Software and Associated Licenses on its Systems

NSF reported that its procedures include: automated mechanisms to detect the presence of both authorized and unauthorized hardware, software, and firmware components within the information system; scanning tools to identify software that poses a security risk; and reviewing and updating a list of unauthorized software programs when a new request for software is submitted or when a request for software is denied. NSF has an application that keeps track of the software licenses that it owns, such as Microsoft Office Suite, that are installed on the machines of end users. Additionally as described below, NSF reported that it has several capabilities to monitor and detect exfiltration (unauthorized transfer of data from a computer) and unauthorized access to its systems.

Data Loss Prevention (DLP)

According to NSF, one of its information security practices is the use of automated tools that monitor its entire network, such as all data being sent from NSF to an external source, to detect potential exfiltration of large amounts of data and to protect unintentional loss of sensitive data. NSF also stated that it uses automated tools that can analyze events, such as discovery of a virus, in real time so that the information technology (IT) security team can respond quickly to security threats.

Another practice NSF informed us about was its use of a Trusted Internet Connections (TIC) to alert IT Security personnel if a potential compromise or a system or application is detected or occurs. NSF also reported that it uses a network-based intrusion detection system to identify unauthorized use of its information system through real time malware detection, and through the use of other tools. NSF stated that both inbound and outbound external NSF traffic that passes through a NSF system is filtered and continuously monitored.

Forensics and Visibility Capabilities

Another information security practice NSF stated that it uses is incident response procedures to investigate and review data and to identify malicious activity. In addition, NSF stated that it uses automated mechanisms to support the incident handling process and that it preserves important data for investigative purposes.

NSF also said that agency computer security personnel regularly coordinate with security officials at the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT) to receive and stay abreast of current security related information including threats, vulnerabilities, and incidents.

Digital Rights Management (DRM)

Office of Management and Budget Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, states that "a digital rights

management shared service capability could enable a systematic approach to data-level protection across the Federal Government and help prevent unauthorized review, redistribution, and modification of sensitive Government information. While protections at the network level remain essential, adding protection at the data level is critical to achieving defense in depth."

DRM refers to access control technologies that are used to restrict use of proprietary hardware and copyrighted works. NSF officials stated that NSF does not have the type of data that would require DRM for protection against unauthorized distribution. Further, they also stated that there is no federal requirement for NSF to have a DRM capability. However, to address issues related to copyrighted material, NSF said that it has a Peer-to-Peer (P2P) file sharing policy that prohibits P2P software on NSF computers because such software can be used to download copyrighted material such as movies and music. NSF reported that it controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Finally, NSF requires all NSF staff, and contractors to complete annual security awareness training which reinforces that P2P software use is prohibited.

Other security management practices include the following threat monitoring capabilities:

According to NSF, it is on target to be the first agency in the federal government to implement the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation Program (CDM) in FY16.

Additionally, NSF's threat monitoring capabilities include:

- **Anti-Malware** – virus protection software to protect NSF computers and network. NSF utilizes real-time malware detection to detect downloaded malware, and to identify traffic that would indicate a compromised system.

- **Vulnerability Scans** – NSF conducts daily, weekly, and ad-hoc scans for vulnerabilities in the information system to identify unauthorized devices and to scan workstations, servers, and other network devices.

5. Policies and procedures to ensure that agency information security practices are followed by entities, including contractors, that provide services to NSF

NSF contracts contain a clause requiring contractor personnel to comply with all FISMA requirements, Office of Management and Budget policy, National Institute of Standards and Technology guidelines, and NSF IT security policy. This contract clause and NSF policy state that contractors must follow the same rules as NSF personnel to protect PII.

NSF said that contractors who maintain certain NSF systems, such as iTRAK (NSF's financial system), provide monthly monitoring and compliance statistics on the health of the system. Finally, NSF employees, and contractors are required to certify that they have completed annual IT security training.

With respect to other Federal agencies that provide services to NSF, [redacted] NSF has Memoranda of Understanding and Interconnection Security Agreements between NSF and servicing agencies that state how data will be protected by the servicing agency.

Conclusion: Based on the information NSF provided, we conclude that NSF's policies and practices for access controls appear to generally reflect appropriate standards. However, we did not verify or test the effectiveness of the access controls that NSF reported that it uses to protect its systems and applications from unauthorized users.

Agency Response and OIG Comments: NSF responded that it concurred with the OIG's conclusion. We have included NSF's full response as an attachment to this report.

Office of Chief Information Officer

Date: Jul 15 2016

To: Ms. Allison C. Lerner
Inspector General

From: Amy Northcutt /s/
Chief Information Officer, National Science Foundation

Subject: OIG Report on NSF Covered Systems Under Section 406 of the 2015 Cybersecurity Act

---

National Science Foundation (NSF) appreciates the opportunity to review and comment on the subject report, which presents the results of the Office of the Inspector General's (OIG) assessment of NSF's systems covered under Section 406 of the Cybersecurity Act of 2015. The report succinctly summarized the OIG's review and correctly concluded NSF's policies and practices for access controls generally reflect appropriate standards.

If you need more information, you may contact me at (703) 292-8150 or anorthcu@nsf.gov.

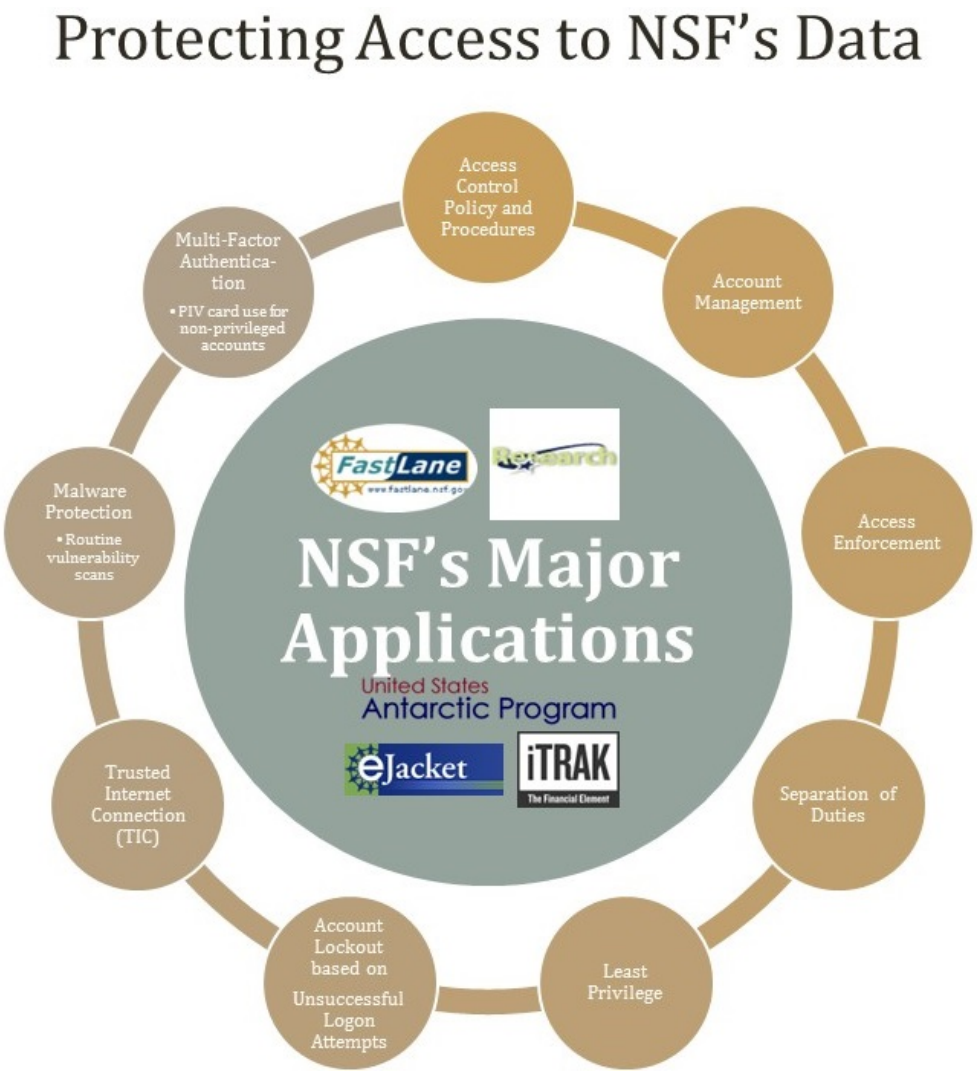
cc:
Joanne Tornow, OIRM
Dorothy Aronson, OIRM/DIS
Dan Hofherr, OIRM/DIS
Mary Lou Tillotson, OIRM/DIS

Attachment II: NSF's Policies and Practices Governing Logical Access

- *Account Management Procedure* (April 11, 2014), which defines the process and responsibilities for creating, managing, monitoring and deleting NSF IT accounts for network access;
- *Unified Profile Maintenance (UPM) Control Procedure (March 16, 2016),* which documents the process for managing the users and application authorizations in UPM;
- *Administrative Manager and Operations Specialist User Access Guide , (January 29, 2016),* which provides guidance to administrative managers on assigning proper roles to research directorate staff through UPM;
- *United States Antarctic Program (USAP) Information Security Program (May 11, 2013),* establishes the security policy for information systems supporting the USAP;
- *iTRAK User Provisioning Policy and Overview (November 2015),* establishes that Administrative Officers, based on their knowledge of the user's job duties, will determine what roles their staff will perform in the agency's financial system; and
- System Security Plans [redacted] document system security requirements and describe the controls in place or planned to provide a level of security appropriate for the information to be transmitted, processed or stored by the system.

Attachment III: Depiction of NSF Logical Access Controls

The following graphic depicts how NSF's access controls help protect NSF data by restricting and monitoring system usage.



Source: OIG developed based on information provided by NSF

Attachment IV: Objectives, Scope, and Methodology

Section 406 of the Cybersecurity Act of 2015 (Division N of the Consolidated Appropriations Act, 2016) requires Inspectors General for agencies with covered systems to report to Congress specific information regarding the agencies logical access policies and security management practices systems. The Act's definition of a covered system includes federal computer systems that provide access to PII. Since NSF has such systems, we conducted this inspection to identify and provide the requested information.

In keeping with the statutory requirement, the objectives of our inspection were to:

- Identify and document NSF logical access policies and practices
- Identify and document NSF logical access controls and multi-factor authentication
- Identify and document NSF information security management practices
- Identify and document NSF policies and procedures to ensure that entities, including contractors, that provide services to NSF are implementing information security management practices

The scope of our inspection included NSF logical access policies, practices and controls for NSF computer systems that provide access to PII at the time of the inspection. NSF reported to us that it had 21 applications (e.g., systems or databases) with PII. NSF listed five as major applications: eJacket, iTRAK, FastLane, Research.gov, and United States Antarctic Program Enterprise Business System. NSF defines major applications as those which require special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information. NSF major applications are required to undergo a security assessment and authorization every three years or when a significant change occurs. NSF labeled the remaining 16 applications as minor applications.[6]

To accomplish our objectives, we reviewed the results of NSF's most recent FISMA report as well as industry and NSF standards for access control and information security. We identified the universe of NSF computer systems that provide access to personally identifiable information. We interviewed individuals from NSF's Division of Information Systems to obtain an understanding of system identification and information security processes and issued a data call to NSF requesting the information required by the Cybersecurity Act. We reviewed and verified the information provided by NSF with other sources as available. We did not verify or test the effectiveness of the access controls that NSF reported that it uses to protect its systems and applications from unauthorized users.

We conducted this inspection from May to June 2016 in accordance with Quality Standards for Inspection and Evaluation, dated January 2012, issued by the Council of Inspectors General on Integrity and Efficiency.

[6] The National Institute of Standards and Technology states that certain applications, because of the information in them, require special management oversight and should be treated as major. Minor applications are typically included as part of a general support system. According to NIST, adequate security for minor applications should be provided by security of the systems in which they operate.