NSF Could Improve its Controls to Prevent Inappropriate Use of Electronic Devices

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

December 21, 2018
OIG 19-2-003

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

AT A GLANCE

NSF Could Improve its Controls to Prevent Inappropriate Use of Electronic Devices

Report No. OIG 19-2-003
December 21, 2018

WHY WE DID THIS AUDIT

We conducted this audit to determine whether NSF detects, deters, and remedies inappropriate usage of electronic devices.

WHAT WE FOUND

NSF could improve its controls to detect, deter, and remedy inappropriate use of its electronic devices. Specifically, NSF does not always 1) ensure its mobile phones and tablet computers are properly enrolled in mobile device management software, 2) prevent users from installing inappropriate applications on its mobile devices, 3) ensure an ongoing business need exists for mobile devices, or 4) review reports identifying excessive attempts to access inappropriate websites. As a result, NSF may be missing opportunities to prevent and remedy inappropriate use of its IT resources. Additionally, NSF may be paying for mobile communication devices that are no longer needed or services beyond the business needs of its users.

WHAT WE RECOMMEND

We recommended NSF provide additional guidance on applications necessary to conduct agency business; develop a policy for the quarterly application review process; implement a mechanism to ensure all NSF-owned mobile devices are enrolled in a mobile device management service; develop an enforcement mechanism to ensure the annual mobile device recertification process is completed; require mobile device managers to review and discuss the user’s data plan, data usage, and acceptable mobile device use during the recertification process; and develop and implement a procedure to periodically obtain web filter reports and identify individuals who are repeatedly triggering the filter.

AGENCY RESPONSE

NSF agreed with our recommendations. NSF’s response is included in its entirety in Appendix A.

CONTACT US

For further information, contact us at (703) 292-7100 or oig@nsf.gov.

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: December 21, 2018

TO: Fleming Crim
Chief Operating Officer

Wonzie Gardner
Acting Office Head
Office of Information & Resource Management

FROM: Mark Bell Mark Bell
Assistant Inspector General
Office of Audits

SUBJECT: Final Report No. 19-2-003, *NSF Could Improve its Controls to Prevent Inappropriate Use of Electronic Devices*

Attached is the final report on the subject audit. We have included NSF's response to the draft report as an appendix.

This report contains seven recommendations aimed at improving NSF's controls to detect, deter, and remedy inappropriate use of its electronic devices. NSF concurred with all of our recommendations. In accordance with Office of Management and Budget Circular A-50, *Audit Followup*, please provide a written corrective action plan to address the report recommendations. In addressing the report's recommendations, this corrective action plan should detail specific actions and associated milestone dates. Please provide the action plan within 60 calendar days of the date of this report.

We appreciate the courtesies and assistance NSF staff provided during the audit. If you have questions, please contact Elizabeth Goebels, Director of Performance Audits, at (703) 292-7100.

cc:
Christina Sarris
Marie Maguire
Allison Lerner
Brian Gallagher
Ann Bushmiller
Nancy Kaplan
Elizabeth Goebels
Louise Nelson
Kelly Stefanko
Anneila Sargent
Dan Hofherr
Peg Hoyle
Dorothy Aronson
Karen Scott
Philip Emswiler
John Veysey
Mary Lou Tillotson
Karen Santoro

TABLE OF CONTENTS

ABBREVIATIONS

Apps	Applications
GB	Gigabytes
IP	Internet Protocol
IT	Information Technology
MDAS	Mobile Device Application System

Background

The National Science Foundation (NSF) is an independent Federal agency created by Congress in 1950 to “promote the progress of science; to advance the national health, prosperity, and welfare; and to secure the national defense.” To help accomplish this mission, NSF provides its staff with electronic devices, such as laptop, desktop, or tablet computers, and mobile phones. NSF staff may also use their personal electronic devices to access some NSF information technology (IT) resources.

NSF has various methods to deter inappropriate use of electronic devices connected to its network. For example, NSF disables network access for users who do not complete annual security and privacy awareness training. NSF also uses a web filtering service on its network, which blocks access to categories of websites NSF deems inappropriate, such as pornography, hacking, and gambling. Neither personal nor NSF-owned mobile communication devices (mobile phones and tablets) can connect to NSF’s internal network.

According to records NSF provided, NSF owned 321 iPhones and 337 iPads as of July 2018. Between May 2017 and April 2018, NSF spent $30,000 on the purchase of mobile devices and $340,000 for related device service plans and contract management fees.

NSF uses mobile device management software (AirWatch[1]) to meet Federal security requirements, including password protection, encryption, and the capability to remotely delete data from mobile devices. AirWatch enrollment is required for any mobile device used to access NSF email, whether NSF-owned or personal. AirWatch has the capacity to detect applications (apps) that NSF designates as prohibited, as well as provide reports of all apps downloaded on NSF-issued mobile devices.

To be eligible for an NSF mobile device, an individual’s supervisor must determine that the individual has a business need for it, and the individual’s office head or assistant director must authorize the device assignment. Additionally, division directors and assistant directors must annually recertify the need for each mobile device, and device users must annually recertify that they have read and understand NSF’s mobile device rules of behavior.

NSF has two policies governing personal use of IT resources. The first, Bulletin No 13-06, *Personal Use Policy for NSF Technology and Communication Resources*, dated April 17, 2013:

- prohibits, among other things, the use of IT resources for personal gain, pornography, illegal activities, gambling, material that could be offensive to coworkers, and online auctions;
- prohibits unauthorized persons, such as family members, from using NSF technology and communication resources; and
- permits occasional personal use of NSF-supplied technology and communication resources when the cost to the Government is negligible and the personal use does not interfere with official business (and provided that the use is not prohibited, and users comply with other listed requirements, such as agreeing to NSF Rules of Behaviors).

[1] Since our fieldwork was completed, AirWatch Agent has been renamed “Intelligent Hub.”

According to the second policy, NSF Bulletin No. 18-07, *Mobile Communication Devices*, dated April 30, 2018:

- individuals with NSF-issued mobile devices should use them only for work-related purposes, except for limited personal use; and
- only applications necessary to conduct agency business may be installed on NSF-issued devices.[2]

In our July 2008 management implication report, *Employee Use of Communication Resources*, we reported six cases of inappropriate computer use and recommended NSF take steps to prevent employee access to inappropriate websites and review internet filtering software reports of attempts to access inappropriate websites. As a follow-up to the 2008 report, we performed this audit to determine whether NSF detects, deters, and remedies inappropriate usage of electronic devices.

Results of Audit

NSF could improve its controls to detect, deter, and remedy inappropriate use of its electronic devices. Specifically, NSF does not always 1) ensure its mobile phones and tablet computers are properly enrolled in mobile device management software, 2) prevent users from installing inappropriate applications on its mobile devices, 3) ensure an ongoing business need exists for mobile devices, or 4) review reports identifying excessive attempts to access inappropriate websites. As a result, NSF may be missing opportunities to prevent and remedy inappropriate use of its IT resources. Additionally, NSF may be paying for mobile communication devices that are no longer needed or services beyond the business needs of its users.

Not All NSF-Owned iPhones and iPads Were Properly Enrolled in Mobile Device Management Software

We identified 102 NSF-owned iPhones and iPads that were either not enrolled or enrolled incorrectly in mobile device management software (AirWatch). Some NSF-owned devices were incorrectly enrolled as personal, and some personal devices were incorrectly enrolled as NSF-owned. When a device is enrolled as NSF-owned, NSF can view all downloaded apps and remotely delete data from the entire device. For devices enrolled as personally owned, NSF only has access to the “container” added to the device for NSF information and cannot view other apps or remove any data outside of the NSF container.

NSF allows mobile device users to enroll in AirWatch themselves, as opposed to requiring enrollment by a central point of service, such as IT Help Central. As part of the enrollment process, users must

[2] NSF’s previous Mobile Communication Devices policy, dated April 17, 2013, included the first bullet but did not include the second bullet.

specify whether the device is personal or NSF-owned. However, NSF does not have a mechanism to ensure NSF staff complete the enrollment process or enroll in AirWatch correctly.

AirWatch has the capacity to detect apps that NSF designates as prohibited, as well as provide reports of all apps downloaded on NSF-owned mobile devices. If NSF-owned mobile devices are not correctly enrolled in AirWatch, NSF cannot ensure the security of NSF information that may be accessible through NSF email accounts or ensure compliance with NSF policies on prohibited and personal use. Additionally, if users incorrectly enroll their personal devices as NSF-owned, they may inadvertently grant NSF access to their personal content.

We also found that NSF email could be accessed from mobile devices (an iPhone and an iPad) that were not enrolled in AirWatch, which may circumvent security requirements. We informed NSF of this issue, and it responded that it is taking technical steps to enforce the use of AirWatch and develop monitoring to ensure those technical controls work as designed.

Some NSF-Owned Mobile Devices Contain Inappropriate Apps

After excluding personal devices that were incorrectly enrolled as NSF-owned, we identified 7,652 total apps[3] (including 1,875 different apps) installed on 456 devices enrolled in AirWatch as NSF-owned devices. Because of the large volume of apps, we used key word searches to identify potentially prohibited uses. We found apps on some devices that may violate NSF's personal use policies. For example, some users had auction apps, games that could constitute gambling, or apps that could be used for personal gain. We also searched for apps that could indicate use of the device by unauthorized persons and found children's entertainment apps. However, we do not know the context in which these apps were used or if they were used.[4]

In April 2018, NSF emailed staff that it had updated its policy on mobile communication devices. The policy included a new provision that "only applications necessary to conduct agency business may be installed on NSF-provided devices." However, the policy did not define "applications necessary to conduct agency business" or specifically instruct users to remove apps that did not meet this criteria. We found apps that do not appear necessary to conduct agency business, including media streaming apps, music streaming apps, and popular games played on mobile devices. We did not identify whether these apps were installed before or after April 2018.

NSF's use of AirWatch's capability to continuously monitor for and detect prohibited apps has been limited. At the time of our audit, NSF had designated only two apps as prohibited, both related to records destruction. Also, NSF had not been reviewing AirWatch reports of apps installed on NSF-owned mobile devices for apps that may violate its personal use policy. By limiting its use of AirWatch,

[3] AirWatch reports do not include pre-installed apps that are part of the device's operating systems and cannot be removed.
[4] After we brought this to NSF's attention, NSF said it was working with the Office of General Counsel and Division of Human Resource Management to determine which apps should be prohibited on NSF devices.

NSF may have missed opportunities to detect and deter inappropriate use of NSF-owned mobile devices, which could discredit NSF or damage its public reputation.

In May 2018, NSF established a quarterly monitoring process to review mobile devices for prohibited apps that automatically delete emails. In response to our audit, NSF expanded the scope of its September 2018 quarterly review to search for apps in 10 categories, such as piracy, auction, and gambling, that could contain content prohibited by NSF Bulletin No. 18-07. NSF found apps in these 10 categories and plans to determine whether it should expand its list of prohibited apps.

NSF's Mobile Device Recertification Processes Could Be More Robust

NSF does not have an enforcement mechanism to ensure its mobile device recertification process is completed annually. For calendar year 2017, the mobile device recertification process was not completed for 98 NSF-owned mobile devices (14 percent). Both NSF's 2013 and 2018 policies on mobile communication devices require each office and directorate to "ensure continued eligibility for assigned mobile communications devices by conducting an annual review of organizational devices by October 31st of each year," but provide no further detail on the recertification process.

NSF uses the Mobile Device Application System (MDAS) to initially approve and recertify a business need for each mobile device issued to NSF employees. MDAS automatically generates a notification to the employee's division director or equivalent to document the determination of the business need for the device. Once this is completed, MDAS generates a notification to the applicable assistant director or office head to provide authorization for assignment of the device. Next, MDAS sends notification to the employee to electronically sign the "Certification of Awareness" of the rules of behavior and other NSF policies applicable to mobile device use. However, if the recertification process stalls at any point, MDAS does not move to the next step, and users may never receive a request to sign the rules of behavior. There is no recourse if a director or manager does not respond to one of the system-generated requests.

An administrative manager or IT Specialist (mobile device manager) within the employee's division typically selects the data and voice plan for the issued device but is not required to discuss individual mobile device needs, such as limited or unlimited data plans, with the user or the user's supervisor. No one is assigned the responsibility to communicate to users the limits of the voice and data plans selected for them, inform users if their usage has incurred additional costs, or educate users on how their personal use may increase costs. Users we interviewed did not know what type of plan they were on.

Once a user has a mobile device, NSF's mobile device contractor optimizes the individual's plan based on usage. A user who exceeds the plan's data limits will be moved to a new plan with more data without the mobile device manager determining if the increased data usage is driven by a business need. Because of the lack of communication, users may not be aware when NSF has accommodated their personal use by purchasing a larger data plan.

According to Verizon Wireless, customers with data devices average between 1 and 2 gigabytes (GB) per month per device. However, we found a dozen users at NSF exceeded 10 GB of data a month in

March 2018, including one user consuming more than 87 GB of data. Some of these high data users told us their primary business use of their NSF-owned mobile devices was to connect to their calendar and email, and review documents. Because they believed they were on unlimited data plans, these users thought their personal use of the devices was acceptable. Although there is not a significant price difference between limited and unlimited data plans under NSF's contract, high data usage may indicate personal use beyond NSF's limited personal use policy.

NSF's mobile device recertification processes would be more effective if mobile device managers reviewed and discussed with users their mobile device billing data and plan, particularly any high data usage or additional charges incurred. This discussion could inform mobile device managers of how NSF staff are using NSF devices and data and provide a basis for discussing the ongoing need for unlimited data. It would also ensure that individuals assigned a mobile device understand the impact of their use of data for non-business purposes.

NSF Does Not Use Internet Filter Reports to Identify Potential Misuse

NSF performs web filtering to block access to inappropriate websites (e.g. gambling, hacking, and pornography) when users are connected to NSF's network. The filter automatically blocks access to a website when it determines that the website or a portion of it, such as a pop-up advertisement, contains restricted content. The filter cannot distinguish between accidental triggers and deliberate attempts to access restricted content. We tested the filter by attempting to access pornographic content from mobile devices connected to the NSF network, and all our attempts were denied.

The web filter service provider can provide reports that include the number of times the filter was triggered, the location (IP address) that triggered it, and the websites that triggered it. However, NSF does not obtain web filter reports or have a policy or procedure requiring the regular review of these reports. According to logs that NSF provided, the web filter blocked access to restricted websites numerous times in May and June 2018. We also identified one user who triggered the filter 459 times for two categories of inappropriate websites in June 2018.[5] By not obtaining and reviewing the web filter reports, NSF may be missing the opportunity to detect and remedy inappropriate use of electronic devices connected to its network.

Recommendations

We recommend the NSF Chief Operating Officer:

1. Provide additional guidance in NSF Bulletin No. 18-07 that clarifies the definition of "applications necessary to conduct agency business" and instruct mobile device users to remove applications that do not comply.

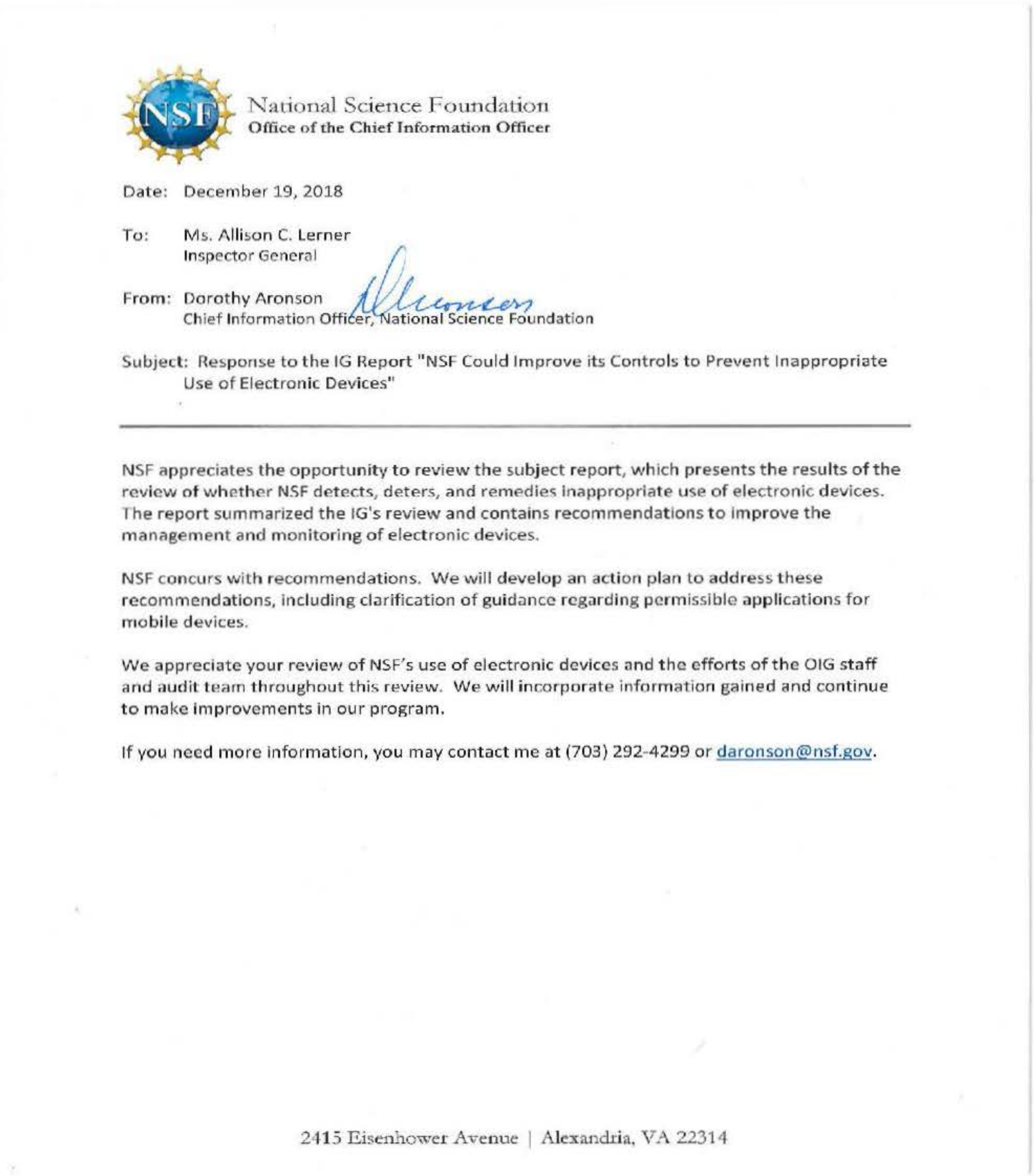
[5] After we brought this to NSF's attention, NSF said it referred information about the individual assigned to this IP address to its Division of Human Resource Management for follow up.

2. Develop a policy for the quarterly app review process and ensure that it includes a search for apps that may violate NSF Bulletin No. 18-07, as well as notification of users and their supervisors when such apps are discovered.
3. Implement the Apple Device Enrollment Program, which may automatically enroll NSF-purchased devices in AirWatch upon shipment or develop an alternative mechanism to centralize and enforce enrollment of NSF-owned devices in a mobile device management service.
4. Ensure that all existing NSF-owned mobile devices (iPhones and iPads) are enrolled in AirWatch.
5. Develop an enforcement mechanism for offices and directorates to complete the annual recertification process for mobile devices and have all users sign the certificate of awareness.
6. Annually educate users on acceptable mobile device use and the consequences of personal and inappropriate use.
7. Develop and implement a procedure to periodically review web filter reports and identify individuals who are repeatedly triggering the filter.

OIG Evaluation of Agency Response

NSF agreed with our recommendations. NSF’s response is included in its entirety in Appendix A.

Appendix A: Agency Response



National Science Foundation
Office of the Chief Information Officer

Date: December 19, 2018

To: Ms. Allison C. Lerner
Inspector General

From: Dorothy Aronson
Chief Information Officer, National Science Foundation

Subject: Response to the IG Report "NSF Could Improve its Controls to Prevent Inappropriate Use of Electronic Devices"

NSF appreciates the opportunity to review the subject report, which presents the results of the review of whether NSF detects, deters, and remedies inappropriate use of electronic devices. The report summarized the IG's review and contains recommendations to improve the management and monitoring of electronic devices.

NSF concurs with recommendations. We will develop an action plan to address these recommendations, including clarification of guidance regarding permissible applications for mobile devices.

We appreciate your review of NSF's use of electronic devices and the efforts of the OIG staff and audit team throughout this review. We will incorporate information gained and continue to make improvements in our program.

If you need more information, you may contact me at (703) 292-4299 or daronson@nsf.gov.

2415 Eisenhower Avenue | Alexandria, VA 22314

Appendix B: Objectives, Scope, and Methodology

Our audit objective was to determine whether NSF detects, deters, and remedies inappropriate usage of electronic devices. To achieve our objective, we reviewed NSF policies and procedures related to the management of NSF's IT programs and systems. We interviewed staff from NSF's Division of Information Systems, contractors responsible for overseeing NSF's mobile device services application, and the vendor responsible for the Fortinet web filter. We also interviewed NSF-owned mobile device users to assess their awareness and understanding of NSF IT requirements.

Apps on NSF-Owned Mobile Devices: To identify any NSF-owned mobile devices that were not enrolled in AirWatch, we compared a list of all NSF-owned mobile devices enrolled in AirWatch against mobile devices listed on NSF's invoices. We interviewed users assigned to five judgmentally selected devices identified as NSF-owned without AirWatch installed to physically examine the device and confirm whether AirWatch was installed.

We reviewed an NSF-provided list from AirWatch of apps installed on NSF-owned mobile devices. To exclude personally owned devices incorrectly enrolled as NSF-owned, we compared the mobile devices on the list from AirWatch to NSF invoices. We excluded any mobile devices and the apps installed on them that did not appear on the invoices. Because of the large volume of apps, we ran judgmentally selected key word searches related to prohibited uses, such as pornography, gambling, personal gain, auctions, and illegal activities.

To test NSF's controls to remove prohibited apps, we installed two prohibited apps on an NSF-owned mobile phone. AirWatch detected the apps and generated an email with directions to remove them. When we ignored these instructions, an NSF IT contractor deleted NSF email from the phone approximately 48 hours later.

Mobile Device Recertification Process: We obtained and analyzed a spreadsheet from NSF's MDAS database showing the approval status of all NSF-owned mobile devices to determine the number that were incomplete.

Network Web Filter: We tested the effectiveness of the NSF network web filter by attempting to access 1) 10 judgmentally selected pornographic sites using an NSF laptop connected to the NSF internal network, 2) 5 judgmentally selected pornographic sites using a mobile phone configured as NSF-owned connected to the NSF guest wireless network, and 3) 5 judgmentally selected pornographic sites using a mobile phone configured as personally owned connected to the NSF guest wireless network. All of our attempts were blocked by the filter.

We reviewed the web filter logs for May and June 2018. These reports capture the total number of times the filter was activated on all NSF networks during the month, the internet protocol (IP) address responsible for each individual filter activation, and the website that the filter blocked in each case. Because NSF uses dynamic IP addresses, we requested NSF provide us with a copy of NSF's Dynamic Host Configuration Protocol log for June 2018. This showed the IP address assignments for NSF users that month. We matched the Dynamic Host Configuration Protocol logs to the web filter reports and identified users who repeatedly triggered the filter for the categories “pornography” and “nudity and risqué” in June 2018, including the websites they were attempting to visit and the total number of times they triggered the filter in those categories.

We confirmed that NSF disabled network access for IT users who had not completed IT security training as of September 30, 2017.

We reviewed the accuracy and completeness of computer-processed data that we used as audit evidence by interviewing agency officials, returning our analysis of the data and exceptions to NSF officials to confirm, tracing our results to other documents, and testing a judgmental sample. In some cases, our finding was that the data was not reliable. In the cases where the data was central to supporting our condition, we deemed it sufficiently reliable for that purpose.

We conducted this performance audit between May 2018 and September 2018 in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix C: OIG Staff Acknowledgments

Elizabeth Goebels, Director, Performance Audits; Kelly Stefanko, Audit Manager; Philip Emswiler, Senior Management Analyst; Brian Gallagher, Information Assurance Specialist; Emma Bright, Management Analyst; and Billy McCain, Independent Report Referencer, made key contributions to this report.

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL