NSF Could Strengthen Key Controls over Electronic Records Management

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

July 6, 2017
OIG 17-2-009

AT A GLANCE

NSF Could Strengthen Key Controls over Electronic Records Management

Report No. OIG 17-2-009
July 6, 2017

WHY WE DID THIS AUDIT

We conducted this audit to determine whether NSF is compliant with applicable standards for preserving electronic messages as Federal records and if NSF has responded to congressional requests for information. This audit responds to a request from Ranking Member McCaskill and Senator Carper of the U.S. Senate Committee on Homeland Security and Government Affairs.

WHAT WE FOUND

NSF has controls in place for managing certain electronic records. For example, it developed a Capstone email policy to permanently preserve select senior officials' email and chat records. It also has issued policies related to the appropriate use of information technology and social media and NSF will adopt NARA's general record schedule for social media once finalized. However, NARA has not yet approved NSF's Capstone email policy, and NSF is exploring solutions to capture text and social media messages.

NSF has also not finalized its guidance related to the use of smartphone applications that support encryption or the automatic deletion of messages for work-related communications, although it has been working to complete the guidance since NARA issued its memo on this topic in March 2017. NSF has the capability to monitor the download of smartphone applications on NSF-owned mobile devices, but it does not actively monitor downloads; instead it provides policies on expected behavior. This allowed some NSF employees to download smartphone applications that support encryption or automatic deletion of messages without consulting required officials.

NSF has taken steps to strengthen its records management, such as by planning on updating its records management training by August 2017 and addressing prior Government Accountability Office records management recommendations. However, without having a NARA-approved Capstone policy, capturing text and social media messages, or monitoring the use of smartphone applications, NSF cannot ensure it is complying with Federal requirements and guidance for electronic records management.

The evidence we examined did not suggest that any NSF or NSB official was asked to delay or withhold responses to congressional requests for information, or any NSF or NSB officials directed or advised any NSF or congressional staff that NSF will only provide information to a committee chair. Therefore, we did not continue our inquiry in this area.

WHAT WE RECOMMEND

We made five recommendations to strengthen NSF's compliance with electronic records management.

AGENCY RESPONSE AND OIG EVALUATION

NSF is reviewing the findings and recommendations. NSF noted that agencies, not NARA, identify Capstone accounts. However, NSF should continue to work with NARA to obtain an approved Capstone policy.

FOR FURTHER INFORMATION, CONTACT US AT (703) 292-7100 OR OIG@NSF.GOV.

MEMORANDUM

DATE: July 6, 2017

TO: Joanne Tornow
Head
Office of Information and Resource Management

Amanda Hallberg Greenwell
Head
Office of Legislative and Public Affairs

FROM: Mark Bell
Assistant Inspector General
Office of Audits

SUBJECT: Final Report No. 17-2-009, *NSF Could Strengthen Key Controls over Electronic Records Management*

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 five recommendations to strengthen NSF's oversight over the retention of electronic records. NSF responded that it will engage us to respond to the final report. In accordance with OMB Circular A-50, *Audit Followup*, please provide our office with a written corrective action plan to address the report's recommendations. In addressing the report's recommendations, the 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, Performance Audits, at (703) 292-7100.

cc:
Christina Sarris
Allison Lerner
Marie Maguire
Elizabeth Goebels
Wendell Reid
Elizabeth Argeris
Brian Gallagher
Vashti Young
Emily Woodruff
John Anderson
Maria Zuber
Dorothy Aronson
Ann Bushmiller
Donna Butler
Dianne Campbell
Aya Collins
Joan Ferrini-Mundy
Fae Korsmo
Wonzie Gardner
Peggy Gartner
Daniel Hofherr
Karen Scott
Peggy Hoyle
Maxine Hynson
Javier Inclan
Kris McFail
Karen Pearce
Erika Rissi
Lawrence Rudolph
Sanya Spencer
John Veysey
Mark Wilson

TABLE OF CONTENTS

ABBREVIATIONS

GAO	Government Accountability Office
IT	information technology
NARA	U.S. National Archives and Records Administration
NSB	National Science Board
OIRM	Office of Information and Resource Management
OLPA	Office of Legislative and Public Affairs

Background

The National Science Foundation 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…." NSF supports basic research and people to create knowledge that transforms the future, and is currently headquartered in Arlington, Virginia.

Records Management of Electronic Messages

The *Federal Records Act* defines Federal records as any material that is recorded, made, or received in the course of Federal business, regardless of its form or characteristics, and is preserved or worthy of preservation because it evidences "the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of [its] informational value."[1] Managing Federal business records is an important responsibility of Federal agencies, which are required to institute records management programs. The U.S. National Archives and Records Administration (NARA) is authorized to promulgate regulations for Federal records.

In 2014, Congress amended the *Presidential Records Act* and the *Federal Records Act* regarding the preservation, storage, and management of Federal records. NARA also provided Federal agencies with specific guidance on July 29, 2015, on how to comply with Federal law regarding the preservation of electronic messages in Bulletin 2015-02, *Guidance on Managing Electronic Records*. There are additional requirements to manage records created or sent in nonofficial and personal electronic message accounts.[2]

On March 15, 2017, NARA issued a memo to senior agency officials for records management that addressed, among other things, electronic messaging and encrypted messages. The memo stated that "agencies are responsible for properly managing electronic messages that are Federal records whether they are SMS texts, encrypted communications, direct messages on social media platforms, email or created on any other type of electronic messaging system or account."[3]

Audit Purpose

The overall objectives of this performance audit were to determine whether NSF is compliant with applicable standards for preserving electronic messages as Federal records and to determine if NSF has responded to congressional requests for information. This audit responds to a request from Ranking Member McCaskill and Senator Carper of the U.S. Senate Committee on Homeland Security and Government Affairs, dated June 8, 2017. The request is included in its entirety in Appendix C.

[1] 44 U.S.C. § 3301(a)
[2] 44 U.S.C. § 2911(a)
[3] *Records Management Priorities for 2017*, March 15, 2017

Results of Audit

NSF has controls in place for managing certain electronic records. For example, it developed its *Capstone Officials Email Records Management Policy* to permanently preserve the email and chat records of 20 of its senior officials, and has issued guidance on the appropriate use of information technology (IT) and social media. However, NARA has not yet approved NSF's Capstone policy due to an issue surrounding Capstone official requirements. As of June 2017, NSF is exploring solutions to capture text messages, but does not have policies, procedures, or tools to retain them. NSF also has issued policies for the use of social media by NSF employees in the course of their employment and personal use and will adopt NARA's general record schedule once finalized by NARA, but it does not have tools to preserve social media messages.

NSF has also not finalized its guidance related to the use of smartphone applications that support encryption or the automatic deletion of messages after they are read or sent for work-related communications, although NSF has informed us it has been working to produce such guidance since NARA issued its memo on this topic in March 2017. NSF has the capability to monitor the use of smartphone applications on NSF-owned mobile devices, but does not actively monitor their use. According to the Head of the Office of Information and Resource Management (OIRM), NSF's general approach is not to monitor staff's use of certain applications, but to set out policies on expected behavior. As a result, some NSF employees downloaded smartphone applications that support encryption or automatic deletion of messages without consulting the appropriate records management and legal officials as required by NARA.

NSF has taken steps to strengthen its records management, such as by planning on updating its records management training by August 2017 and completing all corrective actions to address prior Government Accountability Office (GAO) records management recommendations. However, without having a NARA-approved Capstone policy, capturing text and social media messages, or monitoring the use of smartphone applications, NSF cannot ensure it is complying with Federal requirements for electronic records management.

NSF Could Strengthen Key Controls over Electronic Records Management

NSF has designed controls over managing electronic records, such as its *Capstone Officials Email Records Management Policy*, although NARA has not yet approved that policy due to an issue surrounding Capstone official requirements. In addition, while NSF is exploring solutions, it does not yet have tools to retain text messages or social media messages. However, without having a NARA-approved Capstone policy or capturing text and social media messages, NSF cannot ensure it is complying with Federal requirements for electronic records management.

NSF Has Issued a Capstone Email Policy, But Has Not Yet Received NARA Approval

Issued in August 2013, NARA Bulletin 2013-02 provides agencies with a new records management approach, known as "Capstone," for managing their Federal record emails electronically.[4] The Bulletin discusses the considerations that agencies should review if they choose to implement the Capstone approach to manage their email records. According to the Bulletin, "[t]he Capstone approach allows for the capture of records that should be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent."[5]

NSF developed its *Capstone Officials Email Records Management Policy*, effective December 31, 2016, to permanently preserve the email and chat records of 20 of its senior Foundation officials. NSF defines email records as "email messages with attachments, calendar appointments, tasks, and chat transcripts created and received in the same system as email message." In addition, NSF captures Skype for Business chat and instant messages and Voicemail messages through its permanent email records. Transcripts of the Skype for Business conversations are integrated with NSF's email system.

Agencies submit the Capstone NARA form 1005 (NA-1005), *Verification for Implementing GRS 6.1*, to NARA for approval of their Capstone officials. According to NARA guidance, Capstone officials "*must* include, when applicable: … General Counsel, … and additional roles and positions that predominantly create permanent records related to … policy decisions…."[6] [Emphasis in original.] NSF, however, did not include its General Counsel on its list of Capstone officials. The NARA appraisal archivist who works with NSF on records scheduling notified OIG on June 15, 2017, that, due to "an internal issue surrounding 'Capstone Official Requirements,' NSF's submission has not been approved and is scheduled to be withdrawn."

The Capstone approach supports the *Presidential Memorandum on Managing Government Records* and allows agencies to comply with the requirement in Directive M-12-18 to "manage both permanent and temporary email records in an accessible electronic format." However, without a NARA-approved plan, NSF is at risk for not properly complying with Federal policies for retaining records.

NSF Does Not Have Policies and Procedures for Retaining Text Messages But is Exploring Solutions

According to NARA's *Records Management Priorities for 2017*, issued March 15, 2017, "Agencies are responsible for properly managing electronic messages that are Federal records," including texts. However, NSF does not have policies and procedures related specifically to retaining text messages or a way to capture text messages on NSF-owned mobile devices.

---

[4] NARA Bulletin 2013-02, *Guidance on a New Approach to Managing Email Records*, August 29, 2013
[5] NARA Bulletin 2013-02. This Bulletin also states, "When adopting the Capstone approach, agencies must identify those email accounts most likely to contain records that should be preserved as permanent. Agencies will determine Capstone accounts based on their business needs. They should identify the accounts of individuals who, by virtue of their work, office, or position, are likely to create or receive permanently valuable Federal records."
[6] *General Records Schedule 6.1: Email Managed Under a Capstone Approach*, issued in September 2016

According to NSF's *Senior Agency Official for Records Management FY 2015 Annual Report*, "NSF is still exploring technical solutions to capture … text." NSF's Senior Agency Official for Records Management told us NSF does not have any tools available to capture an individual's text messages or other media not managed by NSF. Without a method to retain text messages, NSF risks not complying with Federal electronic record requirements.

NSF Has Issued Policies for Social Media Use, But Does Not Have Tools for Preservation of Social Media Messages

According to NARA Bulletin 2014-02, "[t]he use of social media [such as Facebook and Twitter] may create Federal records that must be captured and managed in compliance with Federal records management laws, regulations, and policies." The bulletin does not contain platform-specific social media capture guidance.[7] As of May 2017, NARA has not finalized its general records schedule for social media.

NSF plans to adopt NARA's general records schedule for social media once it is finalized. In addition, NSF issued its *Policy for Social Media Use* in December 2015, which describes responsibilities for using social media on behalf of NSF. According to the policy, "[t]he laws, regulations, and policies that govern Federal records management (including the creation, maintenance/use, and disposition of records) also apply when creating social media on behalf of NSF. New content created with social media tools that qualifies as a federal record must be captured and maintained consistent with NSF Records Management policies."[8]

According to NSF's *Senior Agency Official for Records Management FY 2015 Annual Report*, "[a]s with most agencies, NSF is still exploring technical solutions to capture social media…." According to NSF's Senior Agency Official for Records Management, NSF does not have tools to capture social media. On June 20, 2017, the NSF senior official said that NSF's records schedule covers types of information, but not the media or mode of transmission. Without a method to capture social media messages, NSF cannot ensure it is retaining electronic records in compliance with Federal records management laws.

NSF Has IT and Records Management Training and Guidance, But It Does Not Yet Include Preservation of Electronic Records Created on Personal Accounts

According to NARA Bulletin 2017-01, "Agencies must incorporate the following minimum required content areas into annual records management training: Describe how to manage record and nonrecord materials in email, social media, and other electronic messages, including the statutory requirement that all emails and other electronic messages constituting a record that are sent or received using a personal or non-official account must be copied or forwarded into agency recordkeeping systems within 20 days

[7] NARA Bulletin 2014-02, *Guidance on managing social media records*, October 25, 2013
[8] NSF Bulletin No. 15-14, *Policy for Social Media Use*, December 14, 2015

of creation or receipt."[9]

NSF provides its policy to employees regarding the appropriate use of IT, including guidance for personal use and the conduct of NSF business.[10] In addition, NSF's annual IT Security and Privacy Awareness Training covers employee responsibilities for appropriate IT use. The training materials also inform employees that certain types of communications, such as email messages and Skype for Business conversations, are not private and may be retained/releasable as Federal records. Each employee must annually complete the mandatory training, then review and accept the Rules of Behavior indicating he or she is aware of his or her responsibilities with regards to appropriate use of IT.

NSF also provides records management training, called "Records Management Training for Everyone," to provide an overview of NSF's records management processes and procedures including how to properly maintain and dispose of NSF records. However, as of June 2017, the records management training does not meet NARA's minimum requirement content areas. For example, the training does not address NARA's statutory requirement that all emails and other electronic messages constituting a record that are sent or received using a personal or non-official account must be copied or forwarded into agency recordkeeping systems within 20 days of creation or receipt. NSF indicated as part of our last inspection that it is updating the training, which should be ready in August 2017. Such training will help ensure staff are aware of NARA requirements for preserving electronic records created on personal accounts.

NSF Does Not Have Guidance for and Does Not Actively Monitor Download of Smartphone Applications That Support Encryption or the Automatic Deletion of Messages

NSF has not finalized its guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work-related communications. The NARA memo requiring the creation of this guidance was issued in March 2017, only 3 months prior to our fieldwork. In addition, NSF has the capability to monitor download of smartphone applications on NSF-owned mobile devices, but does not actively monitor downloads; instead, according to the Head of OIRM, NSF's general approach is not to monitor staff's use of certain applications, but to set out policies on expected behavior. This allowed some NSF employees to download such smartphone applications without consulting the appropriate records management and legal officials. Without providing guidance or consistent monitoring, NSF cannot be assured that staff are complying with NARA requirements for electronic message retention.

[9] NARA Bulletin 2017-01, *Agency Records Management Training Requirements*, November 29, 2016
[10] NSF Bulletin 13-06, *Personal Use Policy for NSF Technology and Communication Resources,* April 17, 2013; NSF Bulletin 13-05, *Mobile Communications Devices*, April 17, 2013; and NSF Bulletin 15-14, *Policy for Social Media Use*, December 14, 2015.

NSF Did Not Issue Guidance Related to the Use of Smartphone Applications That Support Encryption or the Ability to Automatically Delete Messages

According to NARA's *Records Management Priorities for 2017*, issued March 15, 2017, use of applications that support encryption or the ability to automatically delete messages would require coordination with the agency's legal counsel and records management official to ensure compliance with the *Federal Records Act* and related regulations. Agencies are responsible for setting policies and procedures that govern the use of these applications prior to their deployment and must take steps to manage and preserve records created through their use for as long as required.

NSF has issued no guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work-related communications. NSF also does not provide training on the use of such smartphone applications, and it does not monitor the downloading of such applications.

According to the Head of OIRM, NSF has been working on creating guidance on the use of smartphone applications since the NARA guidance's issuance. Because NARA issued the guidance in March 2017, the Foundation had not finalized the guidance at the time of our fieldwork, which was only 3 months later; in addition, NARA did not specify a mandated implementation date in its guidance.

NSF Has the Capability to Monitor the Download of Smartphone Applications, But Does Not Actively Monitor Downloads

NSF established a Mobile Device Services initiative to enroll approved smartphones and tablets in AirWatch, a mobile device management software. AirWatch provides NSF the capability to centrally control its mobile devices. Administrators can see how many devices are enrolled in the mobile device management software; which type of device (iOS or Android) is enrolled; which operating system version is running; whether the device is in compliance, such as if it has a password; whether the device is NSF-owned; and what applications are installed on the enrolled devices.

We observed an IT administrator using the AirWatch administrative console and saw that he could run more than 100 reports to show additional information, such as the Active Inactive Users By Location report, as well as create custom reports. However, the administrator noted that reports were not run on a regular basis. AirWatch also provides the capability of blocking and approving applications to be installed on NSF mobile devices, but as of June 2017, those features are not enabled at NSF. According to the Head of OIRM, NSF's general approach is not to monitor staff's use of certain applications, but to set out policies on expected behavior

NSF could strengthen information system controls by either blocking applications it deems untrustworthy or allowing the use of only approved applications that it deems trustworthy and in line with its mission. NSF has an application approval process for its laptop and desktop computers, but it could provide a similar guide for mobile devices.

Some NSF Employees Downloaded Smartphone Applications That Support Encryption or the Ability to Automatically Delete Messages

As of June 19, 2017, 21 NSF employees, including one Foundation official,[11] had downloaded WhatsApp, a messaging application which supports encryption, on their NSF-owned mobile devices.[12] In addition, three NSF employees had downloaded Signal, an application that supports the ability to automatically delete messages, on their NSF-owned devices. We found that no NSF employees downloaded Confide, which also supports the ability to automatically delete messages, on their NSF-owned mobile devices.

Staff with whom we spoke who downloaded WhatsApp or Signal[13] told us they had not consulted legal counsel or the records management official prior to doing so because they were not aware that was a requirement, as NSF has not yet issued guidance on such smartphone applications. NSF's Senior Agency Official for Records Management and General Counsel also told us they had not been contacted by staff requesting to download the applications.

Staff told us they downloaded WhatsApp to communicate internationally for both personal and work-related communications because the application does not need cell phone towers to make calls; instead, users can use the Internet to make calls or send messages. Staff who downloaded Signal told us they viewed it as a messaging application alternative to iMessage and were not planning on using it, nor did they ever use it, for work-related communications.

Without providing guidance or consistent monitoring, NSF cannot be assured that staff are complying with NARA requirements for electronic message retention.

OIG and Government Accountability Office Work Related to Electronic Records Management

In the past 10 years, we have not issued any recommendations related to records management, but as of June 2017, we have one ongoing inspection related to records management. Once issued, our inspection report will include several recommendations to NSF. For example, we will recommend NSF update its records management training to meet all minimum content areas required by NARA, such as describing how and where to store agency records; how to manage records and nonrecord materials in email, social media, and other electronic records; and what to do with record and nonrecord materials when an employee leaves the agency. We also will recommend NSF require all staff take records management training, which, at the time of our fieldwork, NSF did not make mandatory for all NSF staff.

[11] We defined "Foundation official" as staff at the Assistant Director level and Office Head level and above.
[12] NSF-owned devices include approved mobile devices, including iPhones and iPads, and are not limited to smartphones.
[13] We met with a judgmental sample of eight employees who downloaded WhatsApp; we met with all three staff members who downloaded Signal.

As part of that inspection, we reviewed NSF's compliance with GAO's May 2015 recommendations related to records management[14] and determined all recommendations had been addressed. In its report, GAO evaluated NSF's implementation of the *Managing Government Records Directive*, issued by NARA and OMB in 2012. The directive sets goals for Federal agencies to meet as an effort to address a 2011 Presidential memorandum on managing government records. Furthermore, the Directive required agencies to establish a records management framework, eliminate paper, and use electronic recordkeeping by December 31, 2019.

Based on its review, GAO reported that NSF required additional work to implement the NARA and OMB directive. GAO recommended that the Director of NSF take the following four actions:

1. Establish a date by which the agency will complete, and then report to NARA, its plans for managing permanent records electronically.
2. Establish a date by which the agency will complete, and then report to NARA on, its progress toward managing permanent and temporary e-mail records in an electronic format.
3. Report to NARA on the identification of its permanent records in existence for 30 years or more, to include when no such records exist.
4. Complete the identification of unscheduled records stored at agency records storage facilities.

We reviewed NSF's actions to address GAO's recommendations and found that NSF had met the requirements. To address GAO's recommendations, NSF took the following steps:

1. Submitted a plan to NARA that identified when NSF would implement an electronic records management system and digitize hard copy records.
2. Established and met the target date for implementation of a new email Capstone policy, allowing the agency to manage permanent and temporary e-mail records in an electronic system.
3. Sent a letter to NARA stating it does not have permanent records in existence for 30 years or more.
4. Conducted a review of records stored at facilities and sent a report to NARA.

In March 2017, GAO determined that NSF has taken corrective action to address the recommendations and now considers the recommendations closed.

Other Matter: NSF's Responses to Congressional Requests

In order to better understand NSF's compliance with Federal laws governing records retention and responsiveness to congressional requests for information, Ranking Member McCaskill and Senator Carper of the U.S. Senate Committee on Homeland Security and Governmental Affairs asked us to conduct a review and provide a written response to its questions.[15] In response to that request, we conducted fieldwork related to NSF's responsiveness to congressional requests during the period from

[14] GAO-15-339, *Additional Actions Are Needed to Meet Requirements of the Managing Government Records Directive*, May 14, 2015
[15] We have included the request in its entirety in Appendix D.

July 1, 2016, to June 13, 2017. As a result of that fieldwork, no information came to our attention to indicate that:

- any Foundation or National Science Board (NSB) official directed or advised any agency employee to delay or withhold a response to a congressional request for information; and
- any Foundation or NSB official directed or advised any agency employee or congressional staff member that NSF will only provide requested documents or information to a Committee chair.

We found that NSF has internal controls for responding to and tracking congressional requests for information. Finally, we have not issued any prior recommendations related to responding to congressional requests for information.

No Evidence Suggests That NSF or NSB Officials Were Asked to Delay or Withhold Responses to Congressional Requests for Information

In their request, Ranking Member McCaskill and Senator Carper expressed concern over newly-implemented policies that "may also run afoul of several laws that prohibit interference with federal employees' ability to communicate with Congress, including, but not limited to the Whistleblower Protection Enhancement Act, Section 713 of the Consolidated Appropriations Act of 2016, as well as 5 U.S.C. § 7211 [Employees' Right to Petition Congress]." Specifically, according to 5 U.S.C. § 7211, "[t]he right of employees, individually or collectively, to petition Congress or a Member of Congress, or to furnish information to either House of Congress, or to a committee or Member thereof, may not be interfered with or denied."

After reviewing Federal and NSF criteria and deciding upon a review period spanning the current and previous presidential administrations (July 1, 2016, through June 13, 2017), we sent questions by email to 14 staff members in OLPA,[16] whose responsibilities include, but are not limited to, congressional affairs and public affairs. None of these employees reported that a Foundation official asked them to delay or withhold a response to a congressional request for information. We also sent questions by email to all senior officials at the Assistant Director level and Office Head level and above, including the Head of OIRM and NSF's General Counsel, as well as to NSB senior officials. All of the Foundation officials responded that they had not requested information be delayed or withheld. In addition, we interviewed the president of NSF's union, who told us he had not heard any complaints from staff that responses to Congress were being delayed. Our Office of Investigations staff also informed us that it had received no complaints about responses to Congress being delayed and had not conducted any investigations of such a complaint. Based on these efforts, we found no evidence to suggest that during the period we examined any Foundation or NSB official directed or advised any agency employee to delay or withhold a response to a congressional request for information.

We also reviewed NSF's congressional log — in which NSF tracks the name of the requestor, date requested, date due, and date completed of congressional requests — for the period of July 1, 2016, to June 13, 2017, and noted delays in responses to congressional requests from both parties during both

[16] One of the 14 OLPA staff members was sent an email but did not respond as he retired on June 21, 2017.

President Trump's and President Obama's administrations. Officials told us that the due dates in the system are sometimes imposed by NSF, and not requested by Congress. In addition, although the log does not reflect the basis for the delays, NSF officials stated that responses to some requests were delayed because of staff turnover, competing priorities, workload issues, or the sensitive nature of the request; for example, some responses required multiple layers of review, which created a delay in response time. Based on the foregoing, we did not find any reason to continue our inquiry in this area.

No Evidence Suggests That NSF and NSB Officials Directed or Advised NSF or Congressional Staff That NSF Will Only Provide Information to a Committee Chair

As part of our review of NSF's congressional log, we found NSF responded both to minority and majority requests for the period of July 1, 2016, to June 13, 2017. In addition, in response to our request, all senior officials at the Assistant Director level and Office Head level and above, including the Head of OIRM and NSF's General Counsel; senior NSB officials; and OLPA staff, including staff in Congressional Affairs, responded that they had not requested information to only go to a Committee chair. The president of NSF's union also told us that he was not aware of anyone being asked to only send information if requested by a Committee chair. In addition, our Office of Investigations informed us it had received no complaints and had not conducted any investigations related to staff being advised to only provide information to a Committee chair. Further, the Head of OLPA stated NSF will continue its practice of responding to both the majority and minority. Based on these efforts, we found no evidence to suggest that between July 1, 2016, and June 13, 2017, any Foundation or NSB official directed or advised any agency employee or congressional staff member that NSF will only provide requested documents or information to a Committee chair. Accordingly, we did not find any reason to continue our inquiry in this area.

NSF Has Internal Controls for Congressional Requests for Information

NSF has internal controls for responding to and tracking congressional requests for information. For example, NSF has developed a *Correspondence Preparation Guide*, dated November 2014. The guide includes OLPA's policies and procedures for responding to committee chairs as well as individual members. The guide does not direct staff to only send documents/information to a committee chair. Further, the guide explains that NSF has a tracking system for congressional requests. If a response is going to be late, OLPA is to contact the congressional office and negotiate a revised date. In addition, OLPA created a correspondence flow document that explains how NSF staff are to handle congressional requests, and according to the Office Head of OLPA, it conducts outreach to NSF Directorates so they know to contact the OLPA office with any congressional requests. However, an official told us that a Directorate may respond directly to congressional staff on an informal email.

As previously discussed, NSF has developed a congressional tracking log to track the status of congressional requests. NSF provided us with the tracking log for the time period we requested, including information on overdue requests. However, an OLPA official stated that not all congressional requests for information, such as quick emails or phone calls, would appear on the log. In addition, OIG and the NSB do not respond to congressional requests through OLPA; therefore, requests sent to these two offices are not included in NSF's congressional log.

According to OLPA, NSF has a performance metric with respect to responding to congressional requests of responding within 10 days, even if Congress has not set a deadline. However, OLPA officials told us that sometimes the 10 days is not realistic; for example, requests related to personnel are sensitive and may take longer than 10 days to process. In addition, OLPA staff are sometimes late in entering completion dates and enter the date they entered the information in the log rather than the date the response to the request was actually completed.

Recommendations

We recommend the Head of OIRM:

1. Update NSF's *Capstone Officials Email Records Management Policy* to ensure it meets NARA requirements.

2. Develop policies, procedures, and controls to capture and retain work-related text messages, social media posts, and electronic records created on government and non-government accounts to meet NARA requirements.

3. Finish updating training to cover all NARA-required elements, including the handling of electronic records created on non-government accounts.

4. Develop policies and procedures related to downloading smartphone applications, including applications that encrypt emails or automatically delete messages or emails, on NSF-issued mobile devices, as required by NARA guidance.

5. Actively monitor application downloads on NSF-issued mobile devices.

OIG Evaluation of Agency Response

NSF responded that it is reviewing OIG's findings and recommendations. NSF provided background on the development of its Capstone policy and noted that NSF's General Counsel determined that agencies, not NARA, have the authority to determine which positions would constitute Capstone accounts based on their business needs. However, as mentioned in our report, NARA has not approved NSF's Capstone policy. Although we do not take a position regarding NSF's interpretation of NARA policy, we believe NSF should continue to work with NARA, the approving agency for this requirement, to obtain an approved Capstone policy.

We have included NSF's response to this report in its entirety as Appendix A.

Appendix A: Agency Response

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

Date: June 29, 2017

From: Joanne Tornow, Ph.D., Head, Office of Information and Resource Management (OIRM), NSF

Amanda Hallberg Greenwell, Head, Office of Legislative and Public Affairs (OLPA), NSF

To: Mark Bell, Assistant Inspector General for Audit, Office of Inspector General (OIG), NSF

Subject: Management's Response to the OIG's Official Draft Report, "NSF Could Strengthen Key Controls over Electronic Records Management"

We appreciate the opportunity to respond to the OIG's Official Draft Report, "NSF Could Strengthen Key Controls over Electronic Records Management," which also addresses another matter, NSF's compliance with Congressional requests. NSF is pleased that the OIG's draft found that there is no evidence of actions by NSF or NSB officials to delay or withhold responses to Congressional inquiries, which was the impetus for this report. In addition, NSF is pleased that the draft report found that NSF has taken corrective actions to address related GAO recommendations, which are now closed.

Because the audit field work spanned only two weeks and NSF received the Official Draft Report only today, NSF is still reviewing the OIG's findings and recommendations. NSF looks forward to engaging the OIG to respond to the final report, when issued.

Meanwhile, NSF provides the following comments to the OIG's discussion of NSF's Capstone policy. By way of background, NSF's Capstone policy was developed following review of all applicable bulletins issued by NARA, as well as the underlying Presidential Memorandum-Managing Government Records, dated November 28, 2011, and subsequent memoranda from OMB and NARA. Based on this information, NSF's General Counsel determined that agencies – not NARA – have the authority to determine which positions will constitute Capstone accounts based on their business needs. To date, NSF is not aware of any statute under which NARA determines for another agency who should be a Capstone Official.

In view of NARA's advice that the goal of identifying Capstone accounts "is to capture the email accounts of high level policy/decision makers", NSF's General Counsel determined that his legal

advice does not constitute a permanent record of persons authorized to make or issue policy decisions, as opposed to legal opinions, rulings, or general legal advice typically issued by agency General Counsels. NSF's position is supported by NARA's language (also quoted in the OIG's Official Draft Report), which states that certain positions "must, when applicable" be included for purposes of the Capstone exercise. NSF recognizes that some agency General Counsels may, in fact, make or issue policy decisions, but NSF's General Counsel does not. For this reason and others, NSF's Capstone policy did not include NSF's General Counsel.

NSF looks forward to reviewing the OIG's final report and working with the OIG to address its recommendations. If you have any questions concerning our response, please contact Dr. Tornow at (703) 292-8100 or Ms. Greenwell at (703) 292-8070.

Appendix B: Objectives, Scope, and Methodology

The overall objectives of this performance audit were to determine whether NSF is compliant with applicable standards for preserving electronic messages as Federal records and to determine if NSF has responded to congressional requests for information. This audit responds to a request from Ranking Member McCaskill and Senator Carper of the U.S. Senate Committee on Homeland Security and Government Affairs, dated June 8, 2017. The request is included in its entirety in Appendix C. Our scope included NSF policies, procedures, and processes in effect from July 1, 2016, through June 13, 2017.

To complete our objectives, we reviewed NARA guidance and NSF policies and procedures related to electronic records; searched NSF employees' NSF-owned mobile devices for the WhatsApp, Signal, and Confide applications, which support the encryption or automatic deletion of messages; interviewed NSF staff with these applications downloaded on their NSF-owned mobile devices; interviewed records management, social media, and IT employees, including senior officials; and discussed NARA requirements with NARA officials.

Through interviews with NSF staff and review of documentation, we obtained an understanding of controls over responding to requests and electronic records management. We identified some internal control deficiencies related to electronic records management, which we discuss in our findings. We did not identify any instances of fraud, illegal acts, or abuse. We identified instances of noncompliance with NARA guidance and requirements, as discussed in our audit findings.

For our review of electronic records, NSF provided us with a list of application downloads on NSF-owned mobile devices. We ran only limited tests to validate the accuracy of the list. For example, we compared the NSF application download list to the list of mobile devices on the April 2017 vendor invoice for NSF devices. By completing this test, we were able to determine that NSF's application download list included staff who had incorrectly coded their own personal phone as an NSF-owed mobile device. However, due to time constraints, we did not conduct any additional testing to validate the NSF-provided list. As a result, we cannot independently confirm that the list provided by NSF includes all staff with WhatsApp, Confide, or Signal on their NSF-owned mobile devices. However, we interviewed the 3 NSF staff with Signal on their NSF phone and a judgmental sample of 8 of the 21 staff with WhatsApp on their NSF-owned mobile devices and confirmed that they did have the application.

Regarding congressional requests for information, we reviewed Federal criteria and NSF policies and procedures to understand the rules governing the cooperation with congressional document requests and electronic messages. We reviewed NSF's records of congressional requests and surveyed OLPA staff on whether they were directed to delay or withhold a response to a congressional request or only respond to a Committee Chair as per the U.S. Senate Committee's June 8, 2017 inquiry. We sent questions by email to Foundation senior officials, including the Head of OIRM and NSF's General Counsel, to determine whether they had directed staff to delay or withhold responses to congressional requests for information or only send responses to a Committee chair. We also met with NSF's union president regarding if he had heard any complaints from staff regarding being asked to delay a response to such requests or only send responses to a Committee chair. Our Office of Investigations staff conducted

research to determine if it had received or investigated any complaints about responses to Congress being delayed or being advised to only respond to a Committee chair. Based on the responses to our requests, we did not find any reason to continue our inquiry in this area.

During the course of this audit, we relied on information received from NSF's congressional log for our review of congressional requests for information. To test the data in NSF's congressional log, we reviewed documentation for any outstanding delays and NSF responses that were overdue by 30 days. Based on our documentation review, we could confirm that delays did occur in responding to both the majority and minority. However, based on our testing, the dates in the congressional log could not be relied upon, and as such, we are not providing statistics on delays in this report.

Except for limited testing of data provided by NSF as discussed above, we conducted this performance audit during June 2017 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.

We held an exit conference with NSF management on June 26, 2017.

Appendix C: Request from U.S. Senate Committee on Homeland Security and Government Affairs

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

June 8, 2017

The Honorable Allison C. Lerner
Inspector General
National Science Foundation
4201 Wilson Boulevard,
Arlington, Virginia 22230

Dear Inspector General Lerner:

We write today to request that the Office of the Inspector General (OIG) conduct a review of the National Science Foundation's processes and compliance with applicable legal standards for preserving certain electronic records as federal records, and cooperation with Congressional document requests.

Preservation of Electronic Records

In 2014, Congress amended the Presidential Records Act and the Federal Records Act (FRA) regarding the preservation, storage, and management of federal records. The National Archives and Records Administration (NARA) also provided federal agencies with specific guidance on how to comply with federal law regarding the preservation of electronic messages in Bulletin 2015-02, "Guidance on Managing Electronic Records".[1] Pursuant to 44 U.S.C. § 2911, agencies have additional requirements to manage records created or received in nonofficial and personal electronic messaging accounts.[2] NARA plays an essential role in preserving our history as the nation's federal record-keeper, and the Archivist of the United States, as head of NARA, has final authority on how agencies must preserve electronic records as federal records.[3] NARA recently surveyed the FRA compliance of federal agencies, and noted that many agencies "reported having difficulty identifying electronic messages that are records."[4]

---

[1] U.S. National Archives and Records Administration, Electronic Messages White Paper (Aug. 2016) (online at https://www.archives.gov/files/records-mgmt/resources/emessageswp.pdf).

[2] 44 U.S.C. § 2911.

[3] Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187, 128 Stat. 2203.

[4] U.S. National Archives and Records Administration, Electronic Messages White Paper (Aug. 2016) (online at https://www.archives.gov/files/records-mgmt/resources/emessageswp.pdf).

Although NARA has confirmed that the capture of electronic messages creates unique challenges throughout government, various public reports raise questions about whether Trump Administration officials are intentionally skirting compliance with federal record keeping requirements. For example, *The Independent* recently reported that White House staffers are using a "confidential messenger" app called "Confide" that deletes messages once they have been opened, leaving no record of them or their content thereafter.[5] Confide messages cannot be printed or archived and the company indicates that "Even we at Confide cannot decrypt or see any messages."[6] The app allows users to transmit text messages, photos, documents, and voice messages, and provides two forms of screenshot protection, which prevents recipients of an image from taking a screenshot of it. Use by federal employees of private messenger applications, such as Confide, to conduct official business flies in the face of federal recordkeeping laws and the principles of government transparency.

In response to these reports, on March 7, 2017, we wrote to the Archivist of the United States seeking information regarding any guidance NARA has provided to Trump Administration officials, as well as the Trump Administration's compliance with records preservation laws.[7] Archivist David Ferriero provided a detailed response to our letter and included copies of Presidential Records Act (PRA) guidance provided by NARA to the Office of the White House Counsel in a February 2, 2017 briefing on PRA compliance.[8] According to the Archivist's response letter, NARA was not in a position to answer our questions regarding whether officials at federal agencies used any smartphone apps, such as Confide, for work-related communications, or whether any government official at federal agencies have been instructed to avoid using email as a method of work-related communication.

Following the transmittal of our letter to Archivist Ferriero, NARA issued a memo on March 15, 2017, "to all Senior Agency Officials for Records Management that addresses, among other things, 'Electronic Messaging and Encrypted Messages.'"[9] Archivist Ferriero's memo reiterates that "agencies are responsible for properly managing electronic messages that are Federal records whether they are SMS texts, encrypted communications, direct messages on social media platforms, email or created on any other type of electronic messaging system or

---

[5] *Donald Trump's White House Staff 'Communicate Through App Which Automatically Deletes Messages'*, The Independent (Feb. 15, 2017) (online at http://www.independent.co.uk/news/world/americas/us-politics/donald-trump-white-house-staff-confide-communicate-app-auto-delete-messages-leaks-russia-us-a7581046.html).

[6] Frequently Asked Questions, Confide (online https://getconfide.com/faq) (accessed on Feb. 17, 2017).

[7] Letter from Sen. Claire McCaskill, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs and Sen. Tom Carper to David Ferriero, Archivist of the United States (Mar. 7, 2017).

[8] Letter from David Ferriero, Archivist of the United States to Sen. Claire McCaskill, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs and Sen. Tom Carper (Mar. 30, 2017).

[9] *Id.*

account."[10] The Archivist's memo also addressed the recent "news stories referring to the possible use by government employees of non-official, commercial communication applications such as WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically delete messages after they are read or sent."[11] Archivist Ferriero advised federal agencies that:

> Any use of such communication applications requires coordination with your legal counsel and records management officials to ensure compliance with the Federal Records Act and related regulations. Agencies are responsible for setting policies that govern the use of these applications prior to their deployment and must take steps to manage and preserve records created through their use for as long as required.[12]

Cooperation with Congressional Requests

Reports that Trump Administration officials have used practices that undermine transparency of public records are also unfortunately consistent with this Administration's problematic pattern of delaying or ignoring requests from minority Members of Congress. For example, on March 15, 2017, Senate Democrats released a list of more than 100 oversight request letters that Trump Administration officials had not answered.[13] Among those unanswered requests was a letter we sent to Donald McGahn, Counsel to the President, regarding White House officials' use of private email accounts.[14] The list also included outstanding requests to a range of Trump Administration officials at various federal agencies, including Attorney General Sessions, Secretary of State Tillerson, Environmental Protection Agency Administrator Pruitt, Secretary of Defense Mattis, and Secretary of Commerce Ross, among others.

While it might be reasonable to attribute some delay in responding to Congressional requests to the presidential transition process, recent reports suggest that the Trump Administration's lack of transparency and responsiveness may be by design. For example, a January 20, 2017, memo from the Acting Secretary of Health and Human Services (HHS) to agency staff prohibit the dissemination of any "correspondence to public officials (e.g., Members of Congress, Governors) or containing interpretation or statements of Department regulations or

---

[10] Memorandum from David Ferriero, Archivist of the United States to Senior Agency Officials for Records Management re: Records Management Priorities for 2017 (March 15, 2017).

[11] *Id.*

[12] *Id.*

[13] Sen. Sheldon Whitehouse, *Senate Democrats Release List of Over 100 Oversight Letters President Trump Refuses to Answer* (Mar. 15, 2017) (online at https://www.whitehouse.senate.gov/news/release/senate-democrats-release-list-of-over-100-oversight-letters-president-trump-refuses-to-answer).

[14] *Id.*

policy, unless specifically authorized by me [the Acting Secretary]" or a designee.[15] Most recently, Senator Carper noted, regarding GSA's lack of responsiveness to congressional requests for information on the Trump Organization's lease with the General Services Administration (GSA) to redevelop and manage the Old Post Office building, that, effective January 20, 2017, the Trump Administration appeared to have changed GSA's "long-standing practice of providing certain documents requested by minority members of congress, including the ranking member of the committee of jurisdiction with direct oversight."[16] During a recent bipartisan briefing with GSA, "agency personnel stated that its new practice only assures that [requested] documents will be provided to the committee's chairman."[17] Additionally, *Politico* recently reported that during meetings this spring with senior officials for various federal agencies, a Deputy Counsel and Special Assistant to the President, "told agencies not to cooperate" with congressional oversight requests from Democrats.[18] These newly-implemented policies are deeply troubling and may also run afoul of several laws that prohibit interference with federal employees' ability to communicate with Congress, including, but not limited to the Whistleblower Protection Enhancement Act, Section 713 of the Consolidated Appropriations Act of 2016, as well as 5 U.S.C.§ 7211.

In order to better understand the Foundation's compliance with federal laws governing records retention and compliance with Congressional requests and federal recordkeeping requirements for electronic messages, we ask that you conduct a review and provide a written response not later than July 6, 2017, which addresses the following questions:

1. Since January 20, 2017, has any Foundation official directed or advised any agency employee to delay or withhold a response to a Congressional request for information? If any such directive is in writing, please provide a copy.

2. Since January 20, 2017, has any Foundation official directed or advised any agency employee or Congressional staff member that the agency will only provide requested documents or information to a Committee chair? If any such directive is in writing, please provide a copy.

3. Since January 20, 2017, has the Foundation issued any guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work related communications?

---

[15] Memorandum from Acting Secretary, U.S. Department of Health and Human Services to HHS OPDIVHeads and StaffDiv Heads (Jan. 20, 2017).

[16] Senator Tom Carper, *Carper Statement on Trump Hotel Lease* (Mar. 31, 2017) (online at https://www.carper.senate.gov/public/index.cfm/pressreleases?ID=77B68657-FD23-4902-9A64-AE1314F64EAF).

[17] *Id.*

[18] *White House Orders Agencies to Ignore Democrats' Oversight Requests*, Politico (June 2, 2017) (online http://www.politico.com/story/2017/06/02/federal-agencies-oversight-requests-democrats-white-house-239034).

4. Since January 20, 2017, has any Foundation official used, for work-related communications, a smartphone app, including, but not limited to, WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically delete messages after they are read or sent?

5. Since January 20, 2017, has any Foundation official failed to abide by federal law and/or NARA or Departmental guidance regarding preservation of electronic records related to official business, including, but not limited to, text messages, chats, instant messages, social media messages, or emails created on non-government accounts?

6. Has the OIG previously provided recommendations to the Foundation regarding its management of the preservation of electronic records and compliance with Congressional document requests? If so, please provide a list of any OIG recommendations that remain outstanding.

If you or members of your staff have any questions about this request, please feel free to ask your staff to contact Donald Sherman with Ranking Member McCaskill's office at 202-224-2627 or Roberto Berrios with Senator Carper's office at 202-224-2441. Please send any official correspondence relating to this request to Amanda_Trosen@hsgac.senate.gov. Thank you very much for your attention to this matter.

Sincerely,

Claire McCaskill
Ranking Member

Tom Carper
United States Senator

cc: The Honorable Ron Johnson
Chairman

Appendix D: OIG Staff Acknowledgments

Wendell Reid, Audit Manager; Elizabeth Goebels, Director, Performance Audits; Marie Maguire, Deputy Assistant Inspector General for Audit; Vashti Young, Senior Management Analyst; Brian Gallagher, IT Specialist; Elizabeth Argeris, Communications Analyst; and Brittany Moon, Laura Rainey, and Jeanette Hyatt, Independent Report Referencers, made key contributions to this report.

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL