Inspection of NSF’s Compliance with International Telework Requirements

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

September 14, 2022
OIG 22-3-001

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

AT A GLANCE

Inspection of NSF's Compliance with International Telework Requirements

Report No. OIG 22-3-001
September 14, 2022

WHY WE DID THIS INSPECTION

We performed this inspection in response to a question during an April 1, 2021 NSF-wide virtual townhall. The objectives of this inspection were to determine whether NSF employees were connecting to the NSF network from international locations and whether NSF had implemented adequate controls to ensure compliance with government-wide and NSF requirements for international telework.

WHAT WE FOUND

We identified 22 NSF employees, guests, and contractors who intentionally connected to the NSF network from international locations without authorization between June and September 2021. In addition, although NSF required staff to complete telework training, the training did not address NSF's prohibition on international telework or reference the Department of State requirements for federal employees teleworking overseas. Further, NSF did not periodically communicate the prohibition on international telework and did not have a process in place to monitor international connections to the NSF network. Finally, NSF has not established guidance to address the use of mobile devices to access NSF applications while traveling internationally on personal leave. Without adequate controls to mitigate physical and cybersecurity threats associated with international telework and travel, NSF faces increased risks to the integrity, availability, and confidentiality of its data and systems. NSF has taken steps to strengthen its controls by issuing NSF Bulletin No. 22-07, *International Telework*, on June 30, 2022, which provides NSF personnel with guidance on the NSF international telework policy.

WHAT WE RECOMMEND

We made six recommendations related to communicating policies, conducting a risk assessment, monitoring and retaining connection data, and developing additional guidance for contractors, which are aimed at improving NSF's compliance with international telework requirements.

AGENCY RESPONSE

NSF agreed with all six recommendations. NSF's response is included in its entirety in Appendix A.

FOR FURTHER INFORMATION, CONTACT US AT OIGPUBLICAFFAIRS@NSF.GOV.

National Science Foundation • Office of Inspector General
2415 Eisenhower Avenue, Alexandria, Virginia 22314

MEMORANDUM

DATE: September 14, 2022

TO: Wonzie L. Gardner
Office Head
Office of Information and Resource Management

Patrick Breen
Division Director
Division of Acquisition and Cooperative Support
Office of Budget, Finance and Award Management

FROM: Mark Bell [redacted]
Assistant Inspector General
Office of Audits

SUBJECT: Report No. OIG 22-3-001, *Inspection of NSF's Compliance with International Telework Requirements*

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 six recommendations aimed at improving NSF's compliance with international telework requirements. NSF concurred with all six 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.

We appreciate the courtesies and assistance NSF staff provided during the inspection. If you have any questions, please contact Laura Rainey, at 703.292.7100, or lrainey@nsf.gov.

cc:
Christina Sarris
Karen Marrongelle
Steve Willard
Ann Bushmiller
Ona Hahs
Jennifer Kendrick
Mary Lou Tillotson
Daniel Hofherr
Nancy Kaplan
John McCarthy
William Malyszka
Sarita Marshall
Lisa Vonder Haar
Karen Scott
Allison Lerner
Ken Chason
Dan Buchtel
Laura Rainey
Melissa Prunchak
Kathleen Covino
Matias Rosner Ortiz

TABLE OF CONTENTS

ABBREVIATIONS

DACS	Division of Acquisition and Cooperative Support
DETO	Domestic Employee Teleworking Overseas
DIS	Division of Information Systems
HRM	Division of Human Resources Management
IPA	Intergovernmental Personnel Act
M365	Microsoft 365
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network

Background

The National Science Foundation is an independent federal agency created by Congress in 1950 “[t]o promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes” (Pub. L. No. 81-507). With an annual budget of $8.8 billion (fiscal year 2022), NSF is the funding source for approximately 25% of all federally supported basic research conducted by America's colleges and universities. NSF, including the staffs of the National Science Board office and the Office of the Inspector General, has a total workforce of approximately 2,100 at its Alexandria, VA, headquarters, including approximately 1,400 career employees, 200 scientists on temporary duty from research institutions, and 450 contract workers.

Due to the coronavirus disease 2019 pandemic, NSF adopted a maximum telework posture in March 2020. According to NSF, the health and safety of the NSF workforce and visitors has been its top priority over the past two years. NSF announced its return to site plans on February 10, 2022, with some staff returning to the office (onsite in Alexandria, VA) on April 4, 2022, while also implementing a hybrid workplace and assessing positions eligible for remote work and increased telework.

NSF Telework Requirements

Telework is a flexible work arrangement under which an employee performs the duties and responsibilities of their position, and other authorized activities, from an approved alternate worksite, other than the agency worksite.

In 2016, the Department of State distributed a memorandum with policy and guidance on requirements regarding international telework for federal Executive Branch employees. Specifically, all federal employees in the Executive Branch who are assigned to domestic positions are prohibited from teleworking in an overseas location without official approval from the employee’s agency and the Department of State through a Domestic Employee Teleworking Overseas (DETO) arrangement.[1] The DETO arrangement must be established prior to the individual teleworking outside of the United States.[2]

According to the NSF telework policy[3], NSF employees are not permitted to telework in a foreign country due to increased security concerns and costs. NSF contractors are also prohibited from teleworking from an international location unless such an arrangement is directly specified by the contracting officer or required by the terms of the contract.[4] NSF’s telework policy applies to all NSF employees and to individuals assigned to NSF under Title IV of the *Intergovernmental Personnel*

[1] A DETO agreement is a State Department-approved arrangement allowing for a Federal Executive Branch employee assigned to a domestic position to perform official U.S. Government from an approved overseas location.

[2] Office of Personnel Management, *2021 Guide to Telework and Remote Work in the Federal Government*, November 2021.

[3] NSF, *Personnel Manual, Chapter 8 – Work/Life Programs, Subchapter 500 – Telework Program*, May 1, 2020.

[4] NSF, *Contracting Officer Representatives Handbook,* 08 2021.

Act (IPA), 5 U.S.C. §§ 3371 – 3376. The NSF telework policy states that prior to engaging in any type of telework, NSF employees must receive agency approval through a telework agreement. The telework agreement identifies the employee's alternate worksite, which is a worksite, other than the agency worksite, that is approved for teleworking, including an employee's residence or other work location that supports productive work and provides an appropriate environment, connectivity, and security for the work effort.

NSF Network and Application Connections

NSF's Division of Information Systems (DIS) provided data identifying international connections from several sources for our inspection. Specifically, NSF network and application connections include the following 3 types:

1. Virtual Private Network (VPN) connections are encrypted connections over the internet to a network that helps ensure that sensitive data is safely transmitted. VPN connections to the NSF network can be made from an NSF-issued laptop or contractor furnished computer with the NSF VPN profile. VPN connections from international locations indicate the user traveled out of the country with their NSF or contractor-issued laptop.

2. Virtual Desktop Infrastructure (VDI) is a Web-based remote access system that lets the user work remotely from any Windows or Mac computer. VDI includes a virtual desktop environment that can be set up to match how individuals use their NSF computer. Individuals use VDI when they want to connect to NSF systems with a non-NSF or personal computer.

3. Microsoft 365 (M365) connections include any connection to NSF's M365 applications (Outlook, Word, Teams, SharePoint, Excel, etc.) from personal devices or NSF-issued and/or contractor devices, including mobile devices such as cell phones, watches, and tablets. Data received through M365 may result from "passive" connections (i.e., cell phone receives an email notification without any intentional steps taken by the employee or contractor).

Inspection Objectives

The objectives of this inspection were to determine whether NSF staff were connecting to the NSF network from international locations and whether NSF implemented adequate controls to ensure compliance with government-wide and NSF requirements for international telework. We initiated this inspection in response to a question[5] that arose during an April 1, 2021, NSF-wide virtual

[5] During the townhall, a participant anonymously asked the following question: "During the pandemics [*sic*] colleagues have been working remotely from other countries, while maintaining a DMV [District, Maryland, Virginia] home. If this happened in the future, during or after the pandemic, then would the employee a) continue to receive DMV locality pay, b) need remote work approval post-pandemic?" An HRM staff member responded that "[u]nder no circumstance should any employee be teleworking from a foreign country. This is in our current telework policy. Department of State

townhall. To accomplish our objectives, we reviewed VPN, VDI, and M365 data provided by NSF and identified 77 users with international connections from 37 countries between June and September 2021.[6] See Appendix C for details on the countries and number of connected users. We further reviewed 32 of the 77 NSF staff who used VPN and/or VDI from international locations because VPN and VDI data represent intentional connections (the user took proactive steps to connect to the NSF network). Please see Appendix B for more information about our objectives, scope, and methodology and Appendix D for more information on the M365 data.

Results of Inspection

We identified 22 NSF employees, guests, and contractors who intentionally connected without authorization to the NSF network via VPN and/or VDI from international locations between June and September 2021. In addition, although NSF required employees to complete telework training, the training did not address NSF's prohibition on international telework or reference the Department of State requirements for federal employees teleworking overseas. Further, NSF did not periodically communicate the prohibition on international telework and did not have a process in place to monitor international connections to the NSF network. Finally, NSF has not established guidance to address the use of mobile devices to access NSF applications while traveling internationally on personal leave. For example, the *NSF Rules of Behavior for Access to IT Resources,* which detail the responsibilities and expectations for all NSF staff (employees, IPAs, contractors, and all other personnel), does not mention the use of devices outside the US (whether on official travel or on personal leave).

Mobile devices are susceptible to compromise, theft, physical damage, and loss, regardless of user location because of their portability and traveling internationally intensifies this risk. Additionally, governments in some countries have direct or proxy control of the commercial cellular infrastructure, which gives them a remote conduit to attack connected mobile devices, steal the information processed by or stored on the device, or used a compromised device to attack connected enterprise networks. Without adequate controls to mitigate physical and cybersecurity threats associated with international telework and travel, NSF faces increased risks to the integrity, availability, and confidentiality of its data and systems.

provides the regulation for working outside of the U.S. Employees may only work outside of the U.S. if it's for NSF official business or IR/D [Independent Research and Development] that have been vetted through OISE [Office of International Science and Engineering]."

[6] The time frames for the three datasets were June 12, 2021, through September 10, 2021, for VPN; August 3, 2021, through September 3, 2021, for VDI; and July 25, 2021, through September 2, 2021, for M365.

NSF Staff Connected from International Locations without Authorization

Distribution of International VPN/VDI Connections

We identified 32 NSF staff members, including 12 employees, 6 IPAs, 2 guests, and 12 NSF contractors who connected to the NSF network through VPN and/or VDI from international locations.[7] These 32 users connected from 19 countries using VPN and/or VDI. There were three users who connected from more than one country.

Table 1. International Countries where NSF Staff Used VPN and/or VDI

Country	Unique NSF Users	Country	Unique NSF Users	Country	Unique NSF Users
Australia	1	Germany	4	Mexico	1
Austria	1	Greece	1	New Zealand	2
Canada	3	Hungary	1	Spain	1
Colombia	1	India	3	Turkey	1
Dominican Republic	1	Israel	1	United Kingdom	8
France	2	Italy	1		
French Polynesia	1	Jamaica	1		

Source: OIG analysis of NSF data on users who connected to the NSF network from international locations via VPN between June 12, 2021, and September 10, 2021, and/or VDI between August 3, 2021, through September 3, 2021.

Of the 32 NSF staff, we judgmentally reviewed 26 users (12 employees, 2 guests, and 12 contractors) because employee timecards and contract information were readily available. We did not request information for the 6 IPAs because IPA timecards are maintained by the IPA’s respective home institution. We confirmed with Human Resources Management (HRM) for the employees and guests, and with the Division of Acquisition and Support (DACS) for the contractors, whether these individuals were conducting official U.S. business from a foreign location on international travel orders, teleworking (and therefore conducting domestic duties) from an international location under a DETO agreement or contract, or intentionally connecting to NSF networks from a foreign location absent official travel orders, DETO agreement, or contract approval.

We identified 22 NSF employees, guests, and contractors who intentionally connected without NSF approval or authorization to connect to the NSF network via VPN and/or VDI from international locations between June and September 2021.

[7] The two guests included one intern and one fellow.

Table 2. Results of Connection Testing

Type of NSF User	Authorized International Connection (While on Official Travel Orders or Contract Approval)	Unauthorized International Connection (Without Official Travel Orders, DETO Agreement, or Contract Approval)	Total
Employees (including two experts)	3	9	12
Guests (one intern and one fellow)	0	2	2
Contractors	1	11*	12
Total	**4**	**22**	**26**

* Two contractors had permission from the contracting officer's representative to log in while outside the U.S., but did not have approval from the contracting officer, as required.

Source: OIG analysis of NSF employees, guests, and contractors who connected to the NSF network from international locations via VPN between June 12, 2021, and September 10, 2021, and/or VDI between August 3, 2021, through September 3, 2021, and whether these connections were authorized or unauthorized.

NSF Employees and Guests Made Unauthorized Connections from International Locations

HRM records for the 12 employees we reviewed confirmed that 3 employees had received authorization for international travel to conduct NSF official business[8] and therefore did not need DETO agreements, according to HRM. The remaining 9 employees connected to the NSF network via VDI from international locations without authorization to work internationally. Additionally, the two guests were not on authorized NSF travel when they connected via VDI from international locations.

HRM provided timecards for eight of the nine employees who were not on authorized NSF travel. The timecards documented that on the dates when these individuals accessed the NSF network from international locations, five employees claimed annual leave for the full day. However, three employees claimed work time on the dates in question. Specifically:

- One individual claimed work time with no telework indicator selected;
- One individual claimed work time with the "pandemic" telework indicator selected; and
- One individual claimed work time with a combination of "regular employee home" and "pandemic" telework indicators selected.

HRM explained that the remaining one of the nine employees was an expert[9] who did not claim work time during the pay period in question and therefore NSF did not require them to submit a timecard.

[8] Official business conducted on behalf of the agency off-site.

[9] NSF hires highly qualified consultants and experts to supplement the skills of its staff. NSF appointed consultants and experts normally have intermittent work schedules and are compensated for authorized activities.

Additionally, HRM explained that there were no timecards for the two guests — one summer scholar intern and one fellow — because they were not federal employees and did not use the NSF timekeeping system.

NSF Contractors Made Unauthorized Connections from International Locations

DACS records for the 12 contractors we reviewed confirmed that 1 contractor had authorization from the contracting officer to work remotely from an international location. Two additional contractors had permission from the contracting officer's representative to check email while outside the U.S., but did not have approval from the contracting officer, as required by NSF's August 2021 *Contracting Officer Representative Handbook*.[10] The remaining 9 contractors connected to the NSF network via VPN and/or VDI from international locations without any NSF authorization to work internationally.

NSF Did Not Implement Effective Controls Related to International Telework

NSF did not periodically communicate its international telework policy to staff and NSF's telework training did not address NSF's prohibition on international telework or reference the Department of State requirements applicable to all federal employees working overseas. Additionally, NSF did not provide guidance to address permitted activities and connections to the NSF network or applications to inform staff how to comply with NSF requirements while outside the United States. Without additional training and communication, NSF staff (*i.e.*, employees, IPAs, and contractors) may remain unaware of the prohibition on international telework, increasing the risk that NSF data and devices could be compromised. Finally, NSF did not have a process in place to monitor and maintain data on international connections to the NSF network.

NSF Did Not Communicate its International Telework Policy

NSF's telework policy includes a prohibition on international telework; however, NSF has not widely publicized this prohibition through training or NSF-wide communications, other than responding to the April 1, 2021 question. NSF requires employees to complete telework training provided by the Office of Personnel Management's Telework.gov website, which does not include NSF's telework policy regarding international telework. Further, the Telework.gov training does not include a reference to the DETO requirements for federal employees who wish to request approval for international telework. Although NSF has continuously communicated to employees throughout the pandemic, the written operating posture communications did not include reminders that international telework is prohibited federal employees; IPA assignees; Visiting

[10] Some of these contractors made VPN/VDI connections prior to this handbook revision. The prior April 2020 version stated "the decision to allow a contractor to telework would be made by the contractor's supervisor. The COR should work with the contracting office to identify if the work required in the contract can be performed onsite or offsite."

Scientists, Engineers, and Educators; external detailees; American Association for the Advancement of Science and Einstein Fellows; and NSF Pathways Students.

NSF Did Not Establish Guidance for Permitted Activities on Personal Leave in International Locations

Our review of the VPN and/or VDI connections and timecards showed NSF employees connected from international locations during personal leave. NSF's telework policy prohibits international telework, but NSF did not address whether NSF resources may be used for limited personal use while traveling internationally for personal travel. Specifically, NSF's telework and mobile device[11] policies do not state whether staff and contractors are allowed to connect to NSF platforms (e.g., check email or connect to Microsoft Teams) for limited personal use while on personal travel outside the U.S. Similarly, the *Contracting Officer's Representative Handbook* does not provide further guidance regarding this activity for NSF contractors. NSF also has an International Travel with Laptops and Mobile Devices flyer that provides guidance for staff traveling internationally with NSF-issued laptops and mobile devices. However, this guidance does not state whether it applies to staff on personal leave connecting to the NSF network or applications using their government, corporate, or personal devices.

The Federal Mobility Group[12] recently published government-wide security guidance[13] to address the use of government furnished equipment, such as mobile devices, in a public network for federal employees and contractors who are traveling to, from, and within foreign countries. The purpose of this guidance is to minimize an adversary's ability to exploit government furnished mobile devices to obtain sensitive data, as well as to limit damage should a device be compromised. Additionally, the guidance outlines threats which are also applicable to personal devices used for official government duties through a bring-your-own-device program or similar agency arrangements. NSF could leverage the procedures and best practices described in this document to further develop its agency-specific policy and guidance based on its risk tolerance.

NSF Did Not Monitor NSF Staff Connecting from International Locations

NSF did not have a process in place to monitor international connections to the NSF network. Because NSF did not have a monitoring process in place for these types of connections, it did not identify a business need to retain connection data and stored the data on a temporary basis. Specifically, DIS explained that it considered these records to be "system access records," which

[11] NSF Bulletin No. 19-14, *Mobile Communications Devices*, states "[i]ndividuals who are traveling with their NSF-issued mobile device must follow agency guidance for international travel with mobile devices." However, that guidance does not address the use of devices when traveling internationally for personal travel.

[12] The Federal Mobility Group is chartered under the Federal Chief Information Security Council and works across the federal government to identify common mobility challenges, develop workable solutions and create opportunities to share best practices. The group's purpose is to share information and identify cross-agency needs for mobile policy, guidance and best practices, acquisition of mobile devices and services, and operational requirements for federal mobility programs.

[13] Federal Mobility Group, *International Travel Guidance for Government Mobile Devices*, January 2022.

are temporary records created when authorized users gain access to NSF systems and are subject to destruction after the end of the record's business use lifecycle.[14] NSF's monitoring software captured data on VPN connections going back 90 days and data on VDI and M365 connections going back 32 and 40 days, respectively.

In the event that NSF begins monitoring international connections, the connection records may not be considered temporary system access records and may therefore be subject to longer retention periods. For example, if NSF establishes a monitoring process for detecting unauthorized international telework, it will have to define a business use for the VPN, VDI, and M365 connection data which may require a longer retention period for these records. Retaining and reviewing these records would allow NSF to confirm whether international connections reflect staff conducting authorized NSF official business outside the U.S. or unauthorized international telework. Any future NSF monitoring process would need to consider the accuracy of the country assignment based on internet protocol address. As noted in Appendix B: Objective, Scope, and Methodology, we found the DIS monitoring software did not always accurately reflect the user's country.

Conclusion

Over a 4-month period in 2021, 77 NSF employees, IPAs, guests, and contractors connected to the NSF network from multiple international locations, without authorization in at least 22 cases. The data showed that these connections were made via a variety of pathways (VPN, VDI, and M365) on a variety of devices (NSF and contractor-issued laptops and mobile devices as well as personally owned devices). These connections increase the risk that the NSF network and its data could be compromised through exploitation and/or theft, damage, or loss of the devices. In addition, NSF has not effectively communicated its prohibition on international telework or its policies regarding connection to the NSF network from outside the U.S. while on leave. Finally, NSF did not monitor connections to the NSF network to identify and follow-up on any unauthorized access from international locations.

These findings support the need for a risk assessment to consider threats, vulnerabilities, likelihood, and impact to NSF operations, assets, and individuals resulting from compromised connections and devices. Such a risk assessment would also help NSF identify and implement any necessary mitigating security and privacy controls and could help inform future NSF monitoring efforts and data retention policies. Additionally, developing agency-specific policies and guidance based on its risk tolerance and incorporating applicable best practices from the Federal Mobility Group's *International Travel Guidance for Government Mobile Devices* could help strengthen NSF's oversight of its hybrid workforce.

[14] National Archives and Records Administration *General Records Schedule 3.2: Information Systems Security Records, 030 System Access Records,* September 2016.

As a result of our inspection, NSF has taken steps to strengthen its controls by issuing NSF Bulletin No. 22-07, *International Telework*, on June 30, 2022. This NSF Bulletin provides guidance for NSF personnel[15] to comply with the Department of State requirements and states that individuals traveling internationally for reasons other than official business are not permitted to engage in such international travel with the intent to telework. The guidance clarifies what NSF considers travel for official business and the permitted use of NSF-issued devices and/or personal devices to access NSF systems when travelling internationally for official business.

Additionally, the NSF guidance defines what work activities are considered telework. Specifically, NSF considers telework to include "checking NSF email from a personal or NSF-issued device; virtually attending, or calling into NSF meetings for any purpose, including to stay informed; and contacting NSF coworkers by phone, email, or other means for business reasons" regardless of whether the time is recorded as telework on the individual's timesheet. The guidance instructs individuals traveling internationally for reasons other than official business [to] leave their NSF-issued laptops and mobile devices at home[, and] to disable NSF email on their [personal] devices before departing the United States. Finally, the guidance states that NSF's Chief Operating Officer may approve exceptions to this policy when a critical NSF mission need outweighs the concerns and costs to the agency, and states that any such approval will be limited to only the amount of telework needed to accomplish the critical mission need.

The new guidance will help ensure NSF personnel understand what activities are permitted while traveling outside of the United States. Additional communications and monitoring will further reduce the risk to NSF systems, devices, and data resulting from international connections to the NSF network.

Recommendations

We recommend that NSF's Chief Human Capital Officer:

1. Communicate at least annually to NSF personnel NSF's international telework policy and guidance for acceptable use of mobile devices, if any, to connect to the NSF network while on leave.

2. Conduct a risk assessment to determine the vulnerabilities created by NSF staff who connect to the NSF network from international locations via personal and/or government-furnished devices and identify compensating security controls.

3. Implement a process to monitor connections to the NSF network from outside the U.S., ensuring the system accurately captures the user's country location, and take any

[15] This policy applies to all NSF personnel, which includes federal employees; IPA assignees; Visiting Scientists, Engineers, and Educators; external detailees; American Association for the Advancement of Science and Einstein Fellows; and NSF Pathways Students.

necessary measures to protect NSF's network and data when unauthorized connections are identified.

4. Identify the appropriate data retention timeframe for records detailing Virtual Private Network, Virtual Desktop Infrastructure, and Microsoft 365 connections from international locations.

We recommend that NSF's Division Director, Division of Acquisition and Cooperative Support:

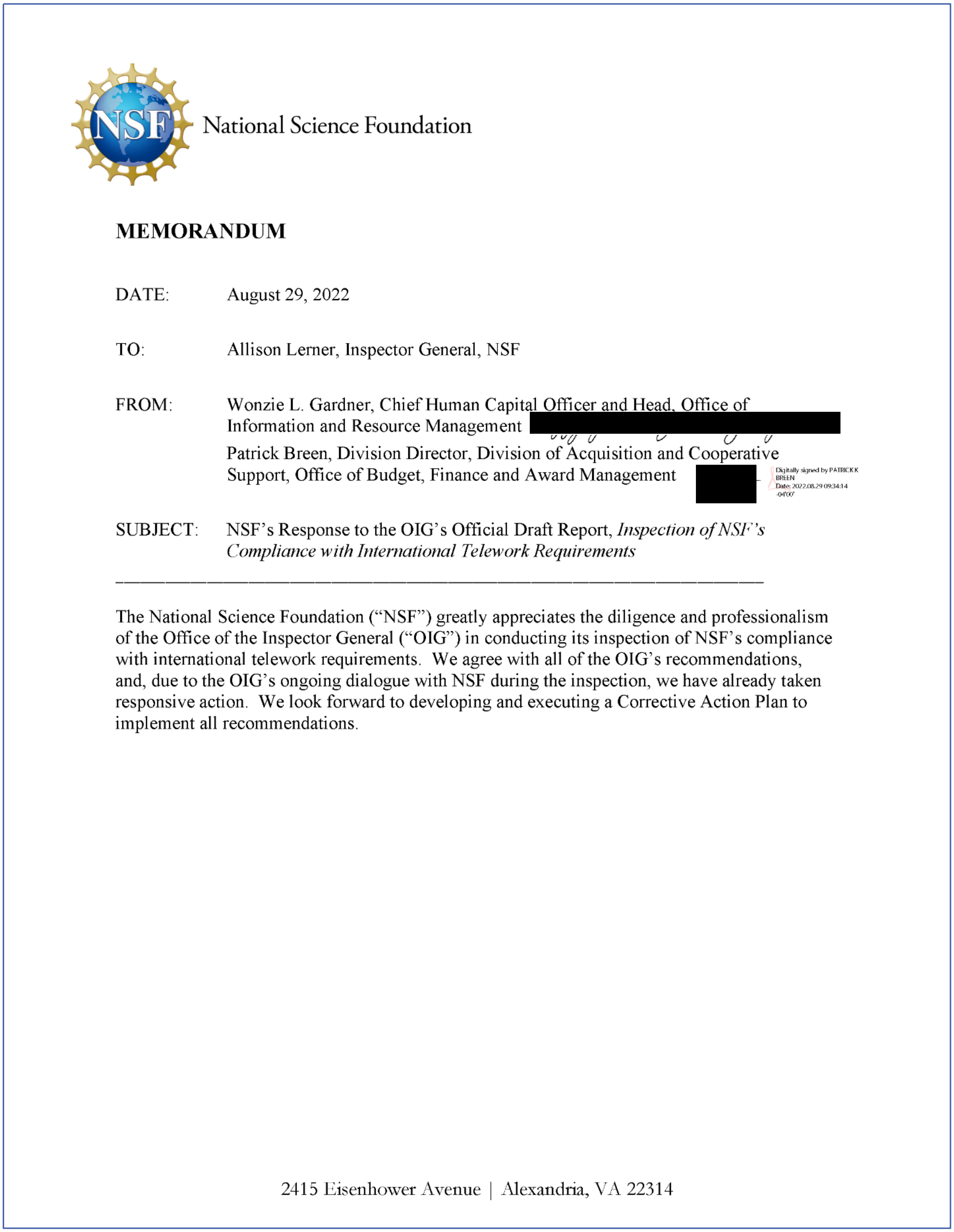
5. Develop and implement additional guidance for contractors to address permitted activities (official business) and connections to the NSF network or applications via personal and/or government or corporate-issued devices while on international travel during personal leave. The guidance should address whether NSF contractors are permitted to monitor emails while on leave outside the U.S. If such access is permitted, the guidance should describe the authorization process to be followed to obtain that access. The guidance should also incorporate applicable best practices from the Federal Mobility Group's *International Travel Guidance for Government Mobile Devices*.

6. Communicate at least annually to NSF contracting officers and contracting officer's technical representatives NSF's contractor international telework policy and guidance for acceptable use, if any, of mobile devices to connect to the NSF network while on leave.

OIG Evaluation of Agency Response

NSF agreed with all six of our recommendations. We have included NSF's response to this report in its entirety in Appendix A

Appendix A: Agency Response



National Science Foundation

MEMORANDUM

DATE: August 29, 2022

TO: Allison Lerner, Inspector General, NSF

FROM: Wonzie L. Gardner, Chief Human Capital Officer and Head, Office of Information and Resource Management [redacted]

Patrick Breen, Division Director, Division of Acquisition and Cooperative Support, Office of Budget, Finance and Award Management [redacted]

Digitally signed by PATRICK K BREEN
Date: 2022.08.29 09:34:14 -04'00'

SUBJECT: NSF's Response to the OIG's Official Draft Report, *Inspection of NSF's Compliance with International Telework Requirements*

The National Science Foundation ("NSF") greatly appreciates the diligence and professionalism of the Office of the Inspector General ("OIG") in conducting its inspection of NSF's compliance with international telework requirements. We agree with all of the OIG's recommendations, and, due to the OIG's ongoing dialogue with NSF during the inspection, we have already taken responsive action. We look forward to developing and executing a Corrective Action Plan to implement all recommendations.

2415 Eisenhower Avenue | Alexandria, VA 22314

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

Appendix B: Objective, Scope, and Methodology

The objectives of this inspection were to determine whether NSF staff were connecting to the NSF network from international locations and whether NSF had implemented adequate controls to ensure compliance with government-wide and NSF requirements for international telework. To accomplish these objectives, we first gained an understanding of the international telework requirements by reviewing NSF policies and procedures as well as government-wide laws, regulations, and guidance.

We conducted interviews regarding NSF's oversight of international telework with NSF staff in the Division of Information Systems (DIS), HRM, and DACS. We requested available data to determine the extent to which NSF staff were connecting to the NSF network from international locations. DIS used monitoring software to capture and provide datasets for international connections via VPN (June 12, 2021, through September 10, 2021), VDI (August 3, 2021, through September 3, 2021), and M365 (July 25, 2021, through September 2, 2021). DIS also provided the Account Role Manager daily report dated September 13, 2021, which listed NSF usernames and other details such as the individual's account type (employee, IPA, guest, or contractor), and the status of the individual's access (active or inactive). We used this data to determine which NSF users had accessed the NSF network from international locations and whether the NSF users were employees, contractors, IPAs, or guests.

We obtained computer-processed data from NSF (the VPN, VDI, and M365 datasets) and we assessed the reliability of this data. The NSF monitoring software assigned country information based on the user's internet protocol information captured in each dataset. During our data reliability assessment, we identified discrepancies for some of the countries assigned. We validated the country assigned for each internet protocol address against three publicly available websites[16] and adjusted as needed to decrease the probability of errors in the dataset. We determined that the verified and/or adjusted data was reliable for the purposes of this inspection.

The datasets initially identified 99 NSF users who connected to the NSF network from outside the U.S. between June and September 2021. The DIS monitoring software incorrectly assigned foreign countries to internet protocol addresses for 24 users that should have been assigned as the United States, making the total 75 users. We then added 2 users that the DIS monitoring software incorrectly assigned the United States to internet protocol addresses that should have been assigned as other countries. There could be more users who were incorrectly assigned the United States and inadvertently left out of the data provided by NSF. After the data reliability assessment and validation of country information, we confirmed that at least 77 NSF users had connected from international locations during this timeframe.

[16] The websites we used were https://ipgeolocation.io/, https://www.whatismyip.com/ and https://ipwhois.io/.

We focused further inspection testing on the 32 users who used VPN and/or VDI as these connections represent intentional connections, in contrast to M365 data which had the potential to show non-intentional (passive) connections. Of the 32 NSF staff and contractors, we judgmentally reviewed 26 users (12 employees, 2 guests, and 12 contractors) because employee timecards and contract information were readily available. We requested timecards from HRM for the 12 employees and 2 guests (one intern and one fellow) as well as confirmation whether the individuals were conducting NSF official business abroad. Additionally, we obtained confirmation from DACS whether the 12 contractors were permitted to telework from an international location or were on travel for NSF official business. We did not request additional information for the 6 IPAs because IPA timecards are maintained by the IPA's respective home institution. Furthermore, we did not review whether NSF complied with the Department of State's country clearance requirements for those on official travel in foreign location or the contractor permitted to work from another country.

We conducted this review from August 2021 through April 2022 under the authority of the *Inspector General Act* of 1978, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we plan and perform the inspection consistent with our inspection objectives and sufficient, to provide a reasonable basis for our conclusions. We believe that the evidence obtained provided a reasonable basis for our conclusions and observations based on our inspection objective.

Key contributors to this report include Laura Rainey, Director, Financial & IT Audits; Melissa Woolson Prunchak, Audit Manager; Kathleen Covino, IT Specialist; Matias Rosner-Ortiz, IT Specialist; Elizabeth Argeris Lewis, Executive Officer and Communications Analyst; Darrell Drake, Independent Report Referencer; and Keith Nackerud, Independent Report Referencer.

Appendix C: International Countries with NSF Connections via VPN, VDI, and M365

We identified 77 NSF staff members who connected to the NSF network through VPN, VDI, and/or M365 from 37 countries between June and September 2021, including 17 users who connected from more than one country.

Table 3. International Countries where NSF Staff Used VPN, VDI and/or M365

Country	Unique NSF Users per Country	Country	Unique NSF Users per Country
Antigua and Barbuda	1	Hungary	2
Aruba	1	Iceland	1
Australia	1	India	7
Austria	2	Ireland	1
Bahamas	1	Israel	1
Belgium	1	Italy	4
Brazil	1	Jamaica	2
Bulgaria	2	Luxembourg	1
Canada	12	Mexico	7
China	1	Netherlands	1
Colombia	2	New Zealand	2
Costa Rica	1	Pakistan	1
Dominican Republic	2	Portugal	2
Ecuador	1	Russia	1
France	5	Spain	3
French Polynesia	1	Turkey	1
Germany	8	United Arab Emirates	1
Greece	3	United Kingdom	13
Honduras	1		

Source: OIG analysis of NSF data on users who connected to the NSF network via VPN, VDI and/or M365. The time frames for the three datasets were June 12, 2021 through September 10, 2021 for VPN; August 3, 2021 through September 3, 2021 for VDI; July 25, 2021 through September 2, 2021 for M365.

Appendix D: International Countries with NSF Connections via M365

We identified 63 NSF users on the M365 dataset that connected from international locations between July 25, 2021, and September 2, 2021. Of the 63 users, 45 were exclusively identified in the M365 data and 18 were also identified on the VPN and/or VDI datasets. As previously noted, M365 data may represent unintentional connections (e.g., a user's mobile device is set to automatically download NSF email on a periodic basis), and we were unable to distinguish whether the user intentionally connected to the M365 applications. The M365 data showed NSF staff members connected from 36 countries via M365 applications such as Outlook Mobile, Microsoft Teams, and Office 365 Sharepoint. Table 4 lists the 36 countries identified for the 63 users in the M365 data, including 16 users who connected from more than one country.

Table 4. International Countries where NSF Staff Used M365

Country	Unique NSF Users per country	Country	Unique NSF Users per country
Antigua and Barbuda	1	Hungary	2
Aruba	1	Iceland	1
Austria	2	India	7
Bahamas	1	Ireland	1
Belgium	1	Israel	1
Brazil	1	Italy	3
Bulgaria	2	Jamaica	1
Canada	11	Luxembourg	1
China	1	Mexico	6
Colombia	1	Netherlands	1
Costa Rica	1	New Zealand	1
Dominican Republic	1	Pakistan	1
Ecuador	1	Portugal	2
France	4	Russia	1
French Polynesia	1	Spain	3
Germany	7	Turkey	1
Greece	3	United Arab Emirates	1
Honduras	1	United Kingdom	8

Source: OIG analysis of NSF data on users who connected to the NSF network via M365 from international locations between July 25, 2021, and September 2, 2021.

NATIONAL SCIENCE FOUNDATION
OFFICE OF INSPECTOR GENERAL

About NSF OIG

We promote effectiveness, efficiency, and economy in administering the Foundation's programs; detect and prevent fraud, waste, and abuse within NSF or by individuals who receive NSF funding; and identify and help to resolve cases of research misconduct. NSF OIG was established in 1989, in compliance with the *Inspector General Act of 1978*, as amended. Because the Inspector General reports directly to the National Science Board and Congress, the Office is organizationally independent from the Foundation.

Obtain Copies of Our Reports

To view this and any of our other reports, please visit our website at oig.nsf.gov.

Connect with Us

For further information or questions, please contact us at OIGpublicaffairs@nsf.gov or 703.292.7100. Follow us on Twitter at @nsfoig. Visit our website at oig.nsf.gov.

Report Fraud, Waste, Abuse, or Whistleblower Reprisal

- File online report: oig.nsf.gov/hotline
- Anonymous Hotline: 1.800.428.2189
- Mail: 2415 Eisenhower Avenue, Alexandria, VA 22314 ATTN: OIG HOTLINE