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

MEMORANDUM

DATE: September 16, 2020

TO: Wonzie L. Gardner
Office Head and Chief Human Capital Officer
Office of Information and Resource Management

Daniel A. Hofherr
Division Director
Division of Information Systems

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

SUBJECT: OIG Project No. 20-6-003, Management Notification Regarding Access to Social Security Numbers in the NSF Report Database

In February 2020, we initiated an audit of the National Science Foundation's Graduate Research Fellowship Program (GRFP), OIG Project No. 20-P-1-004. The objective of this audit is to determine whether NSF properly distributes, monitors, and accounts for GRFP funding. We are issuing this memorandum to alert you to a matter regarding access to social security numbers (SSNs). We found some NSF staff and contractors without a current or continuing business need could view SSNs in the Report Database.

This memorandum contains three recommendations aimed at strengthening controls over access to sensitive information, including SSNs. We have included NSF's response to the draft memorandum in its entirety as an attachment. NSF concurred with all 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 recommendations. In addressing the recommendations, this corrective action plan should detail specific actions and associated milestone dates. Please provide the action plan within 60 calendar days.

Background

NSF has several transaction databases that may be populated with information or modified throughout the proposal life cycle by NSF staff, panelists, reviewers, and the research community. These databases are copied regularly into the read-only Report Database, which contains personally identifiable information and is used for a variety of functions, such as querying award and financial data. NSF's Division of Information Systems (DIS) provides individuals different levels of access to information, including SSNs, depending on their business needs. During our ongoing GRFP audit, we found that our data analyst could view SSN fields in the Report Database.[1] Accordingly, we reviewed NSF's internal controls to determine whether NSF staff and contractors who did not have a business need could view SSNs in the Report Database.[2]

NSF Needs Better Controls over Access to SSNs

Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, requires agencies to develop and implement agency-wide information security and privacy programs to "…[p]rotect information and information systems from unauthorized access…." According to DIS, 115 NSF staff and contractors had SSN access in the Report Database at the time of our review.[3] After we initiated our review, DIS began determining how many of these individuals needed continued access. We interviewed 11 people with access to SSNs to learn whether they were aware they had this level of access, why they needed to view this information, and how they obtained access. Of the 11 staff and contractors we interviewed, 5 said they were unaware of their access to SSNs in the Report Database, and 8 said they did not need access to this information to accomplish their duties. Some staff did not know who provided them access to this information.

NSF's *IT Security Handbook* establishes controls for handling sensitive information, including SSNs. However, the Handbook does not specify controls for how staff or contractors receive access to SSNs in NSF databases, whether they must justify a business need for access, or whether their supervisors must review or approve these requests. Additionally, NSF's *IT Security Handbook* did not detail whether or how DIS recertifies if users require use of sensitive information, including SSNs, after access is provided. DIS said it is currently verifying who still requires access to SSNs in the Report Database.

We also found that several individuals DIS included on the list of users with SSN access were no longer working at NSF. DIS stated it blocks former users who are no longer affiliated with NSF from accessing NSF systems. We did not test this assertion as part of this review. However, the assertion is currently being tested as part of the audit of NSF's compliance with the *Federal Information Security Management Act* for FY 2020.

Recommendations

We recommend the Division Director, Division of Information Systems, Office of Information and Resource Management:

1. Strengthen controls to ensure staff and contractors have a business need to view sensitive information, including SSNs, before providing this level of access in the Report Database.

2. Verify whether individuals with current SSN access in the Report Database have a

[1] As this level of access was unexpected, we reported this observation to DIS.

[2] We did not evaluate whether NSF meets applicable requirements for the collection and use of SSNs.

[3] DIS showed us how it identified these individuals; we did not independently verify this information because we concluded it was sufficient for our limited review.

business need for this level of access.

3. Take steps to regularly remove or recertify access to sensitive information, including SSNs, in the Report Database to ensure only individuals with continuing business need may view this sensitive information.

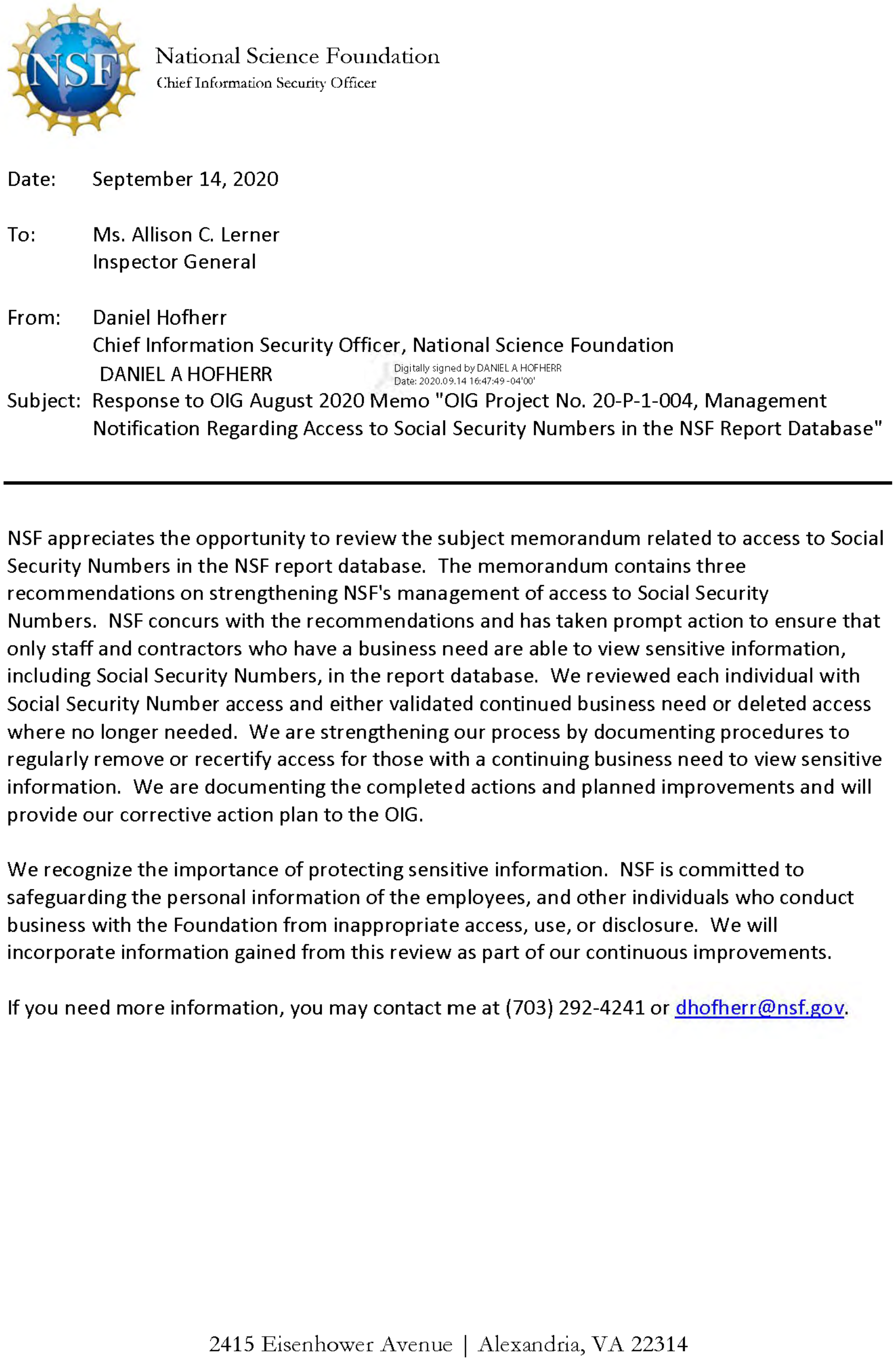
We appreciate the courtesies and assistance NSF staff provided during the review. Should you have questions, please contact Elizabeth Kearns, Director of Audit Execution, at 703.292.7100 or oigpublicaffairs@nsf.gov.

cc:

Christina Sarris
Nancy Kaplan
Mary Lou Tillotson
John McCarthy
Allison Lerner
Lisa Vonder Haar
Dan Buchtel
Elizabeth Kearns
Vashti Young
Ashley Lippolis Aviles
Laura Rainey
Melissa Prunchak

Attachment

Attachment: Agency Response



National Science Foundation
Chief Information Security Officer

Date: September 14, 2020

To: Ms. Allison C. Lerner
Inspector General

From: Daniel Hofherr
Chief Information Security Officer, National Science Foundation
DANIEL A HOFHERR
Digitally signed by DANIEL A HOFHERR
Date: 2020.09.14 16:47:49 -04'00'

Subject: Response to OIG August 2020 Memo "OIG Project No. 20-P-1-004, Management Notification Regarding Access to Social Security Numbers in the NSF Report Database"

NSF appreciates the opportunity to review the subject memorandum related to access to Social Security Numbers in the NSF report database. The memorandum contains three recommendations on strengthening NSF's management of access to Social Security Numbers. NSF concurs with the recommendations and has taken prompt action to ensure that only staff and contractors who have a business need are able to view sensitive information, including Social Security Numbers, in the report database. We reviewed each individual with Social Security Number access and either validated continued business need or deleted access where no longer needed. We are strengthening our process by documenting procedures to regularly remove or recertify access for those with a continuing business need to view sensitive information. We are documenting the completed actions and planned improvements and will provide our corrective action plan to the OIG.

We recognize the importance of protecting sensitive information. NSF is committed to safeguarding the personal information of the employees, and other individuals who conduct business with the Foundation from inappropriate access, use, or disclosure. We will incorporate information gained from this review as part of our continuous improvements.

If you need more information, you may contact me at (703) 292-4241 or dhofherr@nsf.gov.

2415 Eisenhower Avenue | Alexandria, VA 22314