

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
<http://science.house.gov>

February 14th, 2025

Sethuraman Panchanathan
Director
National Science Foundation
2415 Eisenhower Avenue
Alexandria, VA 22314

Dear Director Panchanathan,

We write to you as the Ranking Members of the Committee on Science, Space, and Technology and the Committee's Research and Technology and Investigations and Oversight Subcommittees regarding a matter of grave concern. This inquiry requires a prompt and transparent response.

We have observed, with great alarm, the shocking disregard for data privacy and security protocols exhibited by personnel associated with the so-called "Department of Government Efficiency," or DOGE. The executive order that created DOGE explicitly limited its access to "all *unclassified* agency records," and only "to the maximum extent consistent with law."¹ Recent press reports, however, described a confrontation between DOGE personnel and security officials at the U.S. Agency for International Development (USAID), during which DOGE employees without proper security clearances sought to gain access to secure systems containing classified information.² When the Director of Security at USAID and his deputy did their duty and denied access in order to protect the integrity of the agency's classified data, DOGE employees threatened to call U.S. Marshals against the USAID officials.³ The USAID security officials were subsequently placed on administrative leave and the DOGE personnel gained access to the agency's classified systems.⁴

¹ "Establishing and Implementing the President's 'Department of Government Efficiency,'" Executive Order, White House, January 20, 2025, accessed here: <https://www.whitehouse.gov/presidential-actions/2025/01/establishing-and-implementing-the-presidents-department-of-government-efficiency/>. Italics added.

² Abigail Williams, Vaughn Hillyard, Yamiche Alcindor, Dan De Luce, "USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems," *NBC News*, February 2, 2025, accessed here: <https://www.nbcnews.com/politics/national-security/usaids-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357>.

³ *Id.*

⁴ *Id.*

Since these events, press reports have additionally detailed the successful efforts of DOGE personnel to gain access to highly sensitive systems at the Treasury Department⁵, the General Services Administration (GSA)⁶, the Office of Personnel Management (OPM)⁷, the Small Business Administration⁸, and an unknown number of other federal agencies. These data systems touch every aspect of American life and contain some of the most personal and sensitive information imaginable for individual Americans. There is simply no legitimate purpose that can be conceived to explain why DOGE personnel should gain access to this information. This system access is particularly alarming given recent reporting that DOGE is attempting to develop an AI chatbot, “GSAi,” to comb through GSA data.⁹ This raises serious questions about whether government data is being improperly exfiltrated and manipulated on servers that lack the security measures required of government systems.

This is an appalling situation. The recklessness and contempt with which DOGE personnel are rampaging through the federal government threatens a wide range of security interests, privacy controls, and government services. There is enormous potential for damage and abuse if DOGE personnel improperly access secure systems at NSF. The agency houses Personally Identifiable Information (PII) of grant recipients – some of whom have been villainized by the right-wing misinformation ecosystem, including Senator Ted Cruz, for conducting research that includes diversity-, equity-, inclusion-, and accessibility-related language. Opening up these researchers’ PII to Elon Musk’s DOGE henchmen, many of whom have public records of racism and white supremacy,¹⁰ would be incredibly dangerous – members of Trump’s last Administration have already tried suing for information on these researchers.¹¹ The NSF’s gold-standard merit review process also depends on confidentiality and respect for the privacy of individual reviewers, which is at risk if DOGE purposefully, or through sloppy and non-secure data practices, compromises NSF’s systems. NSF’s National Center for Science and Engineering Statistics (NCSES) conducts 17 surveys of various cross-sections of the scientific population, sampling

⁵ Jeff Stein, “Musk aides gain access to sensitive Treasury Department payment system,” *The Washington Post*, February 1, 2025, accessed here: <https://www.washingtonpost.com/business/2025/02/01/elon-musk-treasury-payments-system/>.

⁶ Theodore Schleifer, Kate Conger, Madeleine Ngo, “Elon Musk’s Next Target: Government Buildings,” *The New York Times*, January 30, 2025, accessed here: <https://www.nytimes.com/2025/01/30/us/politics/elon-musk-general-services-administration.html>.

⁷ Isaac Stanley-Becker, Greg Miller, Hannah Natanson, Joseph Menn, “Musk’s DOGE agents access sensitive personnel data, alarming security officials,” *The Washington Post*, February 6, 2025, accessed here: <https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/>.

⁸ Bobby Allyn, Shannon Bond, “Elon Musk is barreling into government with DOGE, raising unusual legal questions,” *NPR*, February 3, 2025, accessed here: <https://www.npr.org/2025/02/03/nx-s1-5285539/doge-musk-usaid-trump>.

⁹ Pares Dave, Zoe Schiffer, Makena Kelly, “Elon Musk’s DOGE Is Working on a Custom Chatbot Called GSAi,” *Wired*, February 6, 2025, accessed here: <https://www.wired.com/story/doge-chatbot-ai-first-agenda/>

¹⁰ Katherine Long, “Trump Calls for Rehiring of DOGE Staffer Who Resigned Over Racist Posts,” *The Wall Street Journal*, February 7, 2025, accessed here: <https://www.wsj.com/politics/policy/trump-calls-for-rehiring-of-doge-staffer-who-resigned-over-racist-posts-7ff131aa>

¹¹ Kathryn Palmer, “Legal Team With Ties to Trump Investigating NSF’s ‘Leftist Ideology,’” *Inside Higher Ed*, November 7, 2024, accessed here: <https://www.insidehighered.com/news/quick-takes/2024/11/07/america-first-legal-investigating-nsfs-leftist-ideology>

hundreds of thousands of individuals at various stages of their career.¹² If the data security of survey results were to be compromised, sensitive and potentially career-damaging information could be released – information about mistreatment experienced by a graduate student who is vulnerable to retaliation, or the outing of LGBTQ+ researchers at institutions that they fear will discriminate against them. Confidential business information and trade secrets are also at risk, as such information may be included in project proposals.¹³ NSF also houses Controlled Unclassified Information pertaining to international agreements, procurement, and law enforcement-sensitive information.¹⁴

It is critical that the agency adhere to legal requirements, official protocols, and best practices in protecting NSF data from DOGE intrusions. Given the manner in which DOGE has been operating – with no notification, no transparency, and no public explanation for many of its activities – we are compelled to seek clarification directly from the agency to establish conclusively that NSF’s data systems remain secure and security protocols have not, and will not, be violated by DOGE. Please respond to the following questions no later than one week from today, 5:00 PM on February 21st, 2025:

1. Has any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE), accessed or attempted to access secure, classified, or proprietary data, information, or systems within NSF? If so, who accessed this information, and for what purpose?
2. Has any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE), accessed or attempted to access data or systems within NSF that contain Personally Identifiable Information (PII)? If so, who accessed this information, and for what purpose?
3. Has any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE), communicated with any NSF employees or officials in an attempt to secure DOGE access to secure, classified, or proprietary data, information, or systems maintained or overseen by NSF? If so, who accessed this information, and for what purpose?
4. If any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE) attempts to access secure, classified, or proprietary data, information, or systems within NSF, will you pledge to protect such data, information, or systems from any and all access that would violate any and all NSF policies and procedures, federal laws and regulations, and official protocols?

¹² Surveys, National Center for Science and Engineering Statistics, National Science Foundation, accessed here: <https://nces.nsf.gov/surveys>

¹³ “Chapter I – Pre-Submission Information,” National Science – Foundation Office of Budget Finance and Award Management, accessed here: https://www.nsf.gov/pubs/policydocs/pappguide/nsf09_29/gpg_1.jsp#:~:text=Patentable%20ideas%2C%20trade%20secrets%2C%20privileged,understanding%20of%20the%20proposed%20project.

¹⁴ “Controlled Unclassified Information at NSF,” National Science foundation, accessed here: <https://new.nsf.gov/policies/cui>

Furthermore, will you pledge to immediately notify the Committee if any such incidents occur?

It is imperative that you fully disclose, now and in the future, the extent of NSF's interactions with DOGE so the Committee can assess the potential consequences of any breaches in security protocols. If any secure systems or classified data are accessed, and thus compromised, by individuals lacking proper security clearance, we request that Committee staff who do possess appropriate security clearance be given the opportunity to review any such data to inform the Committee's response and any remedial steps that may be required.

This is a matter of the utmost significance. Any delay or lack of transparency on the part of the agency is unacceptable. NSF cannot risk the integrity of the crucial data it manages. We intend to do our utmost to ensure that NSF data remains secure and operable, and if they do not, that any breach or destruction of data results in severe consequences for all involved.

Pursuant to Rule X of the House of Representatives, the Committee on Science, Space, and Technology "shall review and study on a continuing basis laws, programs, and Government activities relating to nonmilitary research and development."¹⁵ The Committee possesses jurisdiction over the National Science Foundation.¹⁶ If you have any questions regarding this letter, please contact Albert Hinman or Sara Palasits with the Committee's Minority staff at (202) 225-6375. Thank you for your attention to this important matter.

Sincerely,



Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology



Haley Stevens
Ranking Member
Subcommittee on Research & Technology



Emilia Sykes
Ranking Member
Subcommittee on Investigations & Oversight

¹⁵ [119 First Session House Rules](#).

¹⁶ *Id.*

CC: Brian Babin
Chairman
Committee on Science, Space, and Technology

Chairman Jay Obernolte
Subcommittee on Research & Technology

Chairman Rich McCormick
Subcommittee on Investigations & Oversight