BRIAN BABIN, D.D.S., Texas
CHAIRMAN

ZOE LOFGREN, California
RANKING MEMBER

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 10th, 2025

Craig Burkhardt
Acting Under Secretary of Commerce for Standards and Technology
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Acting Under Secretary Burkhardt,

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/usaid-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 Department[5], the General Services Administration (GSA)[6], the Office of Personnel Management (OPM)[7], the Small Business Administration[8], 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. While the National Institute of Standards and Technology (NIST) does not conduct classified research, its cutting edge work in topics such as artificial intelligence (AI), [10] quantum sensors and clocks, [11] and semiconductors[12] are world-class, and improper exfiltration to non-secure servers would be a boon for our adversaries. NIST also partners with private industry to assess their technologies, meaning that a DOGE infiltration could jeopardize the confidential business information of companies doing state-of-the-art work that, in some cases, has military and intelligence applications.[13] This includes recent agreements with AI companies to evaluate their products before they are released, including companies that directly compete with Elon Musk's AI company xAI.[14]

---

[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] Paresh 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] "U.S. Artificial Intelligence Safety Institute," National Institute of Standards and Technology, accessed here: https://www.nist.gov/aisi

[11] "World's Most Accurate and Precise Atomic Clock Pushes New Frontiers in Physics," accessed here: https://www.nist.gov/news-events/news/2024/07/worlds-most-accurate-and-precise-atomic-clock-pushes-new-frontiers-physics.

[12] "Semiconductors," National Institute of Standards and Technology, accessed here: https://www.nist.gov/semiconductors

[13] "Research Test Beds," National Institute of Standards and Technology, accessed here: https://www.nist.gov/labs-major-programs/research-test-beds

[14] "U.S. AI Safety Institute Signs Agreements Regarding AI Safety Research, Testing and Evaluation With Anthropic and OpenAI," accessed here: https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research.

The Committee has heard unconfirmed reports that DOGE employees have arrived at NIST. It is critical that the agency adhere to legal requirements, official protocols, and best practices in protecting NIST 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 NIST's data systems remain secure and security protocols have not, and will not, be violated by DOGE's ongoing presence. Please respond to the following questions no later than one week from today, 5:00 PM on February 18th, 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 NIST? 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 NIST 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 NIST employees or officials in an attempt to secure DOGE access to secure, classified, or proprietary data, information, or systems maintained or overseen by NIST? 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 NIST, will you pledge to protect such data, information, or systems from any and all access that would violate any and all NIST policies and procedures, federal laws and regulations, and official protocols? 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 NIST'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 have been 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. NIST cannot risk the integrity of the crucial data it manages. We intend to do our utmost to ensure that NIST 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 Institute of Standards and Technology.[16] If you have any questions regarding this letter, please contact Alan McQuinn 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

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

Chairman Jay Obernolte
Subcommittee on Research & Technology

Chairman Rich McCormick
Subcommittee on Investigations & Oversight

[15] 119 First Session House Rules.
[16] *Id*.