

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

Vice Admiral Nancy Hann
Acting Administrator
National Oceanic and Atmospheric Administration
1401 Constitution Avenue NW
Washington, DC 20230

Dear Vice Admiral Hann,

We write to you as the Ranking Members of the Committee on Science, Space, and Technology and the Committee's Environment 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/usaaid-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. Their egregious and seemingly unlawful acts compromise our national security and put Americans at risk. We are alarmed at the reporting that upon arriving at the National Oceanic and Atmospheric Administration (NOAA) on Tuesday, February 4, DOGE representatives “blew through security ... they walked in and they said, basically, take me to your IT... This is basically like doing a major computer hack attack, but doing it inside the agency, because, you know, somebody gave you a badge.”¹⁰ The next day, it was reported that a DOGE employee, Nikhil Rajpal, has been given a NOAA email address and has been granted editor access to NOAA websites.¹¹

DOGE’s infiltration of NOAA presents unacceptable risks to data systems Americans rely on every day. The National Weather Service (NWS) is critical to alert communities of extreme weather threats – including the wildfires that tore through Southern California last month. The National Environmental Satellite, Data, and Information Service (NESDIS) operates the Aviation Weather Initiative, which improves aviation safety by informing operators of weather conditions

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 Paresch 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 Justin Calma, “Elon Musk’s DOGE storms federal weather forecasters’ headquarters,” *The Verge*, February 6, 2025, accessed here: <https://www.theverge.com/news/607224/doge-musk-trump-weather-climate-noaa>

¹¹ Tim Marchman and Matt Giles, “This DOGE Engineer Has Access to the National Oceanic and Atmospheric Administration,” *Wired*, February 5, 2025, accessed here: https://www.wired.com/story/doge-engineer-noaa-data-google-musk-climate-project-2025/?_sp=18b744e5-eab2-4167-8f14-925017e74372.1738955176104

and engine icing.¹² Unvetted, untrained DOGE employees run the risk of breaking these crucial systems. NOAA also houses the Office of Space Commerce (OSC), where meddling in the data systems could not only severely compromise confidential business information (CBI), but also information with serious national security implications. If DOGE employees were able to access OSC's nascent Traffic Coordination System for Space (TraCSS), then their boss, Elon Musk, could ostensibly access space situational awareness data from SpaceX's competitors, potentially compromising the integrity of a competitive commercial space landscape. Furthermore, given Mr. Musk's past difficulty in obtaining high-level security clearance due to his contacts with foreign officials including Vladimir Putin,¹³ it is highly concerning that access to TraCSS could involve sensitive national security information related to space situational awareness.

As Ranking Members, we are extremely concerned that allowing DOGE unfettered access to NOAA systems is an attempt by the Trump administration to sabotage the agency in furtherance of Project 2025's agenda to dismantle it. Project 2025 seeks to privatize NOAA, compromising the essential services it provides.¹⁴ By infiltrating NOAA's systems, DOGE could be improperly exfiltrating data and setting the stage for selling off its capabilities to the highest bidder. This is of particular concern given the potential conflicts of interest between DOGE, SpaceX, and NOAA.

It is critical that the agency adhere to legal requirements, official protocols, and best practices in protecting NOAA 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 NOAA'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 NOAA? 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 NOAA that contain Personally Identifiable Information (PII)? If so, who accessed this information, and for what purpose?

¹² Aviation Weather Initiative, National Environmental Satellite, Data, and Information Service, National Oceanic and Atmospheric Administration, accessed here: <https://www.nesdis.noaa.gov/aviation-weather-initiative>

¹³ Joe Palazzolo, Emily Glazer, and Micah Maidenberg, "Why Musk Doesn't Have Access to SpaceX's Biggest Government Secrets," *The Wall Street Journal*, December 15, 2024, accessed here: <https://www.wsj.com/tech/musk-spacex-security-clearance-secrets-b9774346>

¹⁴ The Heritage Foundation, Roberts, K. D., Dearborn, R., Vought, R., Devine, D., Kirk, D. D., Dans, P., Miller, C., Cuccinelli, K., Skinner, K. K., Carmack, D. J., Namdar, M., Gonzalez, M., Primorac, M., Bakst, D., Burke, L. M., McNamee, B. L., Gunasekara, M. M., Severino, R., . . . Feulner, E. J. (2025). Project 2025. In P. Dans & S. Groves (Eds.), *Mandate for Leadership 2025: The Conservative Promise*.

3. Has any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE), communicated with any NOAA employees or officials in an attempt to secure DOGE access to secure, classified, or proprietary data, information, or systems maintained or overseen by NOAA? 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 NOAA, will you pledge to protect such data, information, or systems from any and all access that would violate any and all NOAA 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 NOAA'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. NOAA cannot risk the integrity of the crucial data it manages. We intend to do our utmost to ensure that NOAA 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 "environmental research and development, marine research ... outer space, including exploration and control thereof," and the National Weather Service.¹⁶ If you have any questions regarding this letter, please contact Kristi Parrott or Sara Palasits with the Committee's Minority staff at (202) 225-6375. Thank you for your attention to this important matter.

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

¹⁶ *Id.*

Sincerely,



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



Gabe Amo
Ranking Member
Subcommittee on Environment



Emilia Sykes
Ranking Member
Subcommittee on Investigations & Oversight

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

Chairman Scott Franklin
Subcommittee on Environment

Chairman Rich McCormick
Subcommittee on Investigations & Oversight