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 6th, 2025

Janet Petro
Acting Administrator
National Aeronautics and Space Administration
300 Hidden Figures Way, SW
Washington, D.C., 20546

Dear Acting Administrator Petro,

We write to you as the Ranking Members of the Committee on Science, Space, and Technology and the Committee's Space and Aeronautics Subcommittee 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] Press reports have additionally detailed the successful efforts of DOGE personnel to gain access to highly sensitive systems at the Treasury

[1] https://www.whitehouse.gov/presidential-actions/2025/01/establishing-and-implementing-the-presidents-department-of-government-efficiency/. Italics added.
[2] https://www.nbcnews.com/politics/national-security/usaid-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357.
[3] *Id*.
[4] *Id*.

Department[5], the General Services Administration[6], the Office of Personnel Management,[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 delicate 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 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. But the risk to NASA is unique in certain respects, largely due to the vast conflicts-of-interest that the leader of DOGE, Elon Musk, has with NASA. Mr. Musk, apparently serving as a "special government employee," is personally directing DOGE's activities.[9] He is also the CEO of SpaceX, the privately-held rocket manufacturer and commercial spaceflight company that is currently NASA's second-largest contractor, holding more than $2 billion worth of agency contracts.[10] An executive from SpaceX, Michael Altenhofen, recently joined NASA as a "senior advisor to the NASA Administrator."[11]

As Ranking Members, we intend to closely monitor the broad potential for conflicts-of-interest between DOGE, SpaceX and NASA. This issue will be the subject of ongoing oversight. But our immediate concern is to ensure that the integrity of NASA's secure systems, including any classified data managed or accessed by the agency, is being preserved. Under certain circumstances, NASA may use classified information in support of certain agency functions. Any breach of protocol surrounding the preservation or safeguarding of secure systems could have grave consequences for the agency and the country. Furthermore, NASA possesses highly sensitive proprietary data related to the capabilities and contractual obligations of its contractors – some of whom are or could become direct competitors to SpaceX and may compete with SpaceX for forthcoming agency contracts. The possibility that such proprietary data could be obtained by the CEO of SpaceX without regard to NASA procurement rules and regulations risks compromising the integrity of NASA procurement decisions in the future. Mr. Musk's personal communications with Russian President Vladimir Putin,[12] as well as his significant business ties to China,[13] further underscore the gravity of this matter.

There is enormous potential for damage and abuse if DOGE personnel improperly access secure systems and classified information at NASA. The agency is mandated by law to protect classified

---

[5] https://www.washingtonpost.com/business/2025/02/01/elon-musk-treasury-payments-system/.
[6] https://www.nytimes.com/2025/01/30/us/politics/elon-musk-general-services-administration.html.
[7] https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/.
[8] https://www.npr.org/2025/02/03/nx-s1-5285539/doge-musk-usaid-trump.
[9] https://www.nbcnews.com/politics/donald-trump/white-house-says-elon-musk-serving-special-government-employee-rcna190520.
[10] https://spaceproject.govexec.com/civil/2024/07/top-100-nasa-contractors-2023/398145/.
[11] https://arstechnica.com/space/2025/02/as-nasa-flies-into-turbulence-the-agency-could-use-a-steady-hand/.
[12] https://www.wsj.com/world/russia/musk-putin-secret-conversations-37e1c187.
[13] https://www.wsj.com/world/china/china-looks-to-musk-as-conduit-to-trump-seeking-to-ward-off-harsh-policies-bdbb5a4a.

and confidential information,[14] implement data security safeguards,[15] and prevent conflicts-of-interest among its major contractors.[16] It is critical that the agency adhere to legal requirements, official protocols, and best practices in protecting sensitive 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 classified information remains secure and security protocols have not, and will not, be violated. Please respond to the following questions no later than one week from today, 5:00 PM on February 13th, 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 NASA?

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 that contain Personally Identifiable Information (PII)?

3. Has any individual employed by, affiliated with, or acting on behalf of the Department of Government Efficiency (DOGE), communicated with any NASA employees or officials in an attempt to secure DOGE access to any data, information, or systems maintained or overseen by NASA?

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 NASA, will you pledge to protect such data, information, or systems from any and all access that would violate any and all NASA 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 NASA'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. NASA cannot risk the leak or exposure of sensitive information to malicious or conflicted external actors. We intend to do our utmost to ensure that it does not, and that if a security violation does occur, it results in severe consequences for all involved.

---

[14] https://www.law.cornell.edu/uscode/text/51/20131.
[15] https://www.law.cornell.edu/uscode/text/51/20132.
[16] https://uscode.house.gov/view.xhtml?path=/prelim@title51/subtitle3/chapter303&edition=prelim.

If you have any questions regarding this letter, please contact Pamela Whitney or Josh Schneider 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

Valerie P. Foushee
Ranking Member
Subcommittee on Space and Aeronautics

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

Chairman Mike Haridopolos
Subcommittee on Space and Aeronautics