

Congress of the United States
Washington, DC 20515

April 16, 2025

The Honorable Russell Vought
Director
Office of Management and Budget
725 17th St, NW
Washington, DC 20503

Dear Director Vought:

We write to express concern about the use of artificial intelligence (AI) systems within this Administration’s “Department of Government Efficiency” (DOGE), without standards or regard for sensitive data. We understand AI’s potential for modernization and efficiency improvements within the federal government, and support implementation of AI technologies in a manner that complies with existing data security and software development, acquisition, and usage laws, and that provides proper transparency, vetting, and oversight over the use of such AI technologies. We are specifically concerned about reports of Elon Musk and DOGE’s monitoring and sharing of federal employee and non-public federal data using AI tools, and reports of intentions to use sensitive data to train private AI models. These present serious security risks, self-dealing, and potential criminal liability if not handled correctly, and have the potential to undermine successful and appropriate AI adoption.

A DOGE staffer who is also currently employed at SpaceX reportedly created an “AI assistant” for DOGE staff, powered by Musk’s xAI Grok-2 model—this model was hosted on a subdomain of the staffer’s external website, raising both security concerns and conflict of interest issues.¹ In addition to privacy and security concerns, Musk stands to profit from access to government data or contracting opportunities that are not available to competitors or the public.² Increased access to sensitive government data would set his AI models at an unfair competitive advantage over other AI service providers—the conflicts of interest become exponentially worse if Musk pursues further contracts to become a major provider of government AI services.

Further, DOGE reportedly used a chatbot named “GSAi” based on Anthropic and Meta models with the stated intent of analyzing contract and procurement data via a centralized system consolidated under GSA, which would pose similar security and conflict of interest problems.³ Giving Musk’s teams access to sensitive government data on other contracts across the federal government is especially problematic when considering Musk’s business interests with SpaceX

¹ Rollet, Charles and Zack Whittaker, “[Elon Musk staffer created a DOGE AI assistant for making government ‘less dumb’](#),” *TechCrunch*, February 18, 2025.

² Stone, Peter, “[Elon Musk’s Conflicts of Interest ‘Should Scare Every American.’](#)” *The Guardian*, February 27, 2025.

³ Kelly, Makena and Zoë Schiffer, “[DOGE Has Deployed Its GSAi Custom Chatbot for 1,500 Federal Workers.](#)” *Wired*, March 7, 2025.

—already a major government contractor—as well as with SpaceX subsidiary Starlink, Tesla, and elsewhere.^{4,5}

In addition, DOGE’s reported use of AI technologies on sensitive information raises significant concerns about data security. Musk’s DOGE team at the Office of Personnel Management reportedly used AI systems to analyze emails from a large portion of the two million person federal workforce describing their previous week’s accomplishments—without model transparency and without addressing major concerns about security or conflicts of interest.⁶ Alarming, sensitive data from across the Department of Education was also reportedly fed into an AI system, including data with personally identifiable information for people who manage grants, as well as sensitive internal financial data.⁷ Without proper protections, feeding sensitive data into an AI system puts it into the possession of a system’s operator—a massive breach of public and employee trust and an increase in cybersecurity risks surrounding that data. Generative AI models also frequently make errors and show significant biases—the technology simply is not ready for use in high-risk decision-making without proper vetting, transparency, oversight, and guardrails in place.

Sharing of such data would constitute a major data privacy and data security risk. Specifically, we are concerned that sharing such data outside of federal systems or lawfully vetted contracts may run in violation of laws such as the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Information Security Modernization Act of 2014.⁸ These laws set requirements for the federal government’s collection and use of personal information and sensitive data—including through establishing limits on agency information sharing, and requirements for data minimization, disclosure limitations, cybersecurity, transparency, and privacy impact assessments for developing or procuring information technology. In addition, the federal government is legally obligated to comply with codified requirements for vetting software and cloud products and services across the federal government, through programs such as the Federal Risk and Authorization Management Program (FedRAMP).⁹

In 2023, OMB established memoranda to help implement requirements to vet and approve AI technologies for federal use, such as OMB memoranda M-24-10 and M-24-18, which directed federal agencies to use AI only after developing tests and guidelines to ensure that its use would not compromise privacy and cybersecurity.^{10,11,12} These memoranda recognized the sensitive nature of the information the federal government handles every day and the significant privacy

⁴ Swan, Jonathan, Theodore Schleifer, Maggie Haberman, Kate Conger, Ryan Mac, & Madeleine Ngo, “[Inside Musk’s Aggressive Incursion Into the Federal Government](#),” *New York Times*, February 3, 2025.

⁵ Koebler, Jason, Joseph Cox, & Emanuel Maiberg, “[‘Things Are Going to Get Intense:’ How a Musk Ally Plans to Push AI on the Government](#),” *404 Media*, February 4, 2025.

⁶ Smith, Alan, “[‘HHS warns employees that responses to Elon Musk’s request may ‘be read by malign foreign actors!’](#)” *NBC News*, 24 February 2025.

⁷ Natanson, Hannah, Gerrit De Vynck, Elizabeth Dwoskin & Danielle Douglas-Gabriel, “[Elon Musk’s DOGE is feeding sensitive federal data into AI to target cuts](#),” *Washington Post*, February 6, 2025.

⁸ Pub. L. No. 93-579; Pub. L. No. 107-347; Pub. L. No. 107-347.

⁹ Pub. L. No. 117-263.

¹⁰ Executive Office of the President, Joseph R. Biden Jr., “[Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#),” November 11, 2023.

¹¹ Office of Management and Budget, Shalanda Young, “[M-24-10](#),” March 28, 2024.

¹² Office of Management and Budget, Shalanda Young, “[M-24-18](#),” October 3, 2024.

risks of using unvetted AI technologies on such information—including the risk of sharing personally identifiable or otherwise sensitive information with the AI model deployers. While these memoranda were recently revised through OMB’s M-25-21 and M-25-22, the new memoranda retain some provisions on data security and data privacy, including calls against using non-public data for training commercial AI models.¹³ These memoranda also define employment decisions for federal employees as a high-impact AI use application.

It is clear that DOGE’s use of AI clearly does not meet the standards the previous memoranda set. Worse, existing AI systems like CamoGPT have been used in the misguided purging of federal materials from references to achievements of Americans of color and women, including the Navajo Code Talkers and the Tuskegee Airmen.^{14,15,16} It is not clear how the use of CamoGPT meets the Congressional authorization for AI usage provided in the 2021 National Defense Authorization Act, but it is alarming that the result of such usage by this Administration was referred to as an error—raising questions about the appropriateness of and lack of sufficient oversight of its use.

While we support the federal government integrating new, approved AI technologies that can improve efficiency or efficacy, we cannot sacrifice security, privacy, and appropriate use standards when interacting with federal data. We also cannot condone use of AI systems, often known for hallucinations and bias, in decisions regarding termination of federal employment or federal funding without sufficient transparency and oversight of those models—the risk of losing talent and critical research because of flawed technology or flawed uses of such technology is simply too high. We ask that you immediately terminate any use of AI systems that have not been approved by FedRAMP or equivalent formal approval procedures or that do not comply with existing laws. In addition, we ask that you do not use any AI system to make employment termination decisions relating to civil servants.

It is important to understand the extent to which this administration’s reckless disregard for legal authorities and necessary security protocols has extended into use of AI systems. Thoughtful adoption of AI is of strategic national importance. Please provide responses to the following questions by no later than April 25, 2025:

1. Has DOGE or the Trump Administration used AI technologies powered by xAI’s models?
2. What new AI software has been deployed and used by this Administration that was not used by a previous administration? Provide a list.
 - a. Include whether each is on the CISA or DISA authorized technologies list or FedRAMP approved services list, and the date such technology or service was added.

¹³ Office of Management and Budget, Russell T. Vought, “[M-25-21](#),” April 3, 2025; Office of Management and Budget, Russell T. Vought, “[M-25-22](#),” April 3, 2025.

¹⁴ Tang, Terry, “[Pentagon restores histories of Navajo Code Talkers, other Native veterans after public outcry](#),” *Associated Press*, March 19, 2025.

¹⁵ Keller, Jared, “[The US Army Is Using ‘CamoGPT’ to Purge DEI From Training Materials](#),” *Wired*, March 6, 2025.

¹⁶ Baldor, Lolita C. and Tara Cropp, “[Military Ordered to Purge Social Media Sites of Diversity Mentions by March 5](#),” *Military.com*, February 27, 2025.

- b. Include how this Administration’s use of each of such technologies is in compliance with laws such as the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Information Security Modernization Act of 2014.
3. Of the models used in the past two months, who has access to the information submitted to such models and how is oversight being conducted?
 - a. Please provide the level of clearance, authorization, and training they have received.
 - b. Please provide whether they are a special government employee or what category of employee they are.
4. Have the “Grok” models used or the AI technologies used in “GSAi” gone through a federal procurement process prior to use?
 - a. Describe the process such technologies were subject to, and provide documentation.
5. As many AI deployers collect information on the prompts input into their AI models, and use those prompts and their inferences to train their models, how are you ensuring that no deployers of any AI technologies that DOGE or the Trump Administration may use engage in this practice?
6. Has DOGE or the Trump Administration to date used any AI technology to make or recommend an employment decision about a federal employee?
 - a. If so, which technologies has the Department or Administration used?
 - b. If so, how many federal employees did the Department or Administration use AI technology to make or recommend an employment decision about?
7. Has DOGE or the Trump Administration to date used any AI technology to make or recommend a decision regarding a contract or federal funding?
 - a. If so, which contracts and/or which funding? Please provide the search query and rationale for the decision.
8. Have Musk or DOGE employees used government datasets that are not publicly accessible in the training of any non-Federal AI technologies, including for any “Grok” models?
9. Has DOGE or the Trump Administration to date shared any government datasets that are not publicly accessible with any services, sites, or actors that are not approved by FedRAMP or in a way that is not in compliance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Modernization Act of 2014, or any other relevant laws governing data security?
 - a. If so, which data or datasets? Provide a list containing the following:
 - i. The name, agency or department of origin, and a timespan of the information covered in the dataset;
 - ii. A description of the static or dynamic data sources and scope of the data accessed for the analyses performed; and

iii. A description of the content of the data accessed, including data types and known features. This should include identification of any metadata collected (such as associated users, IP addresses, locations, or timestamps).

10. Do any DOGE servers or websites incorporate AI technologies not previously approved under the requirements set by M-24-10 or M-24-18, or agency guidance in compliance with those memoranda, or not on the CISA or DISA authorized technologies list or FedRAMP approved services list? If so, provide a list.

11. What steps has the Trump Administration taken to ensure that Musk and all DOGE employees are not using their federal government role to enrich themselves personally or the companies in which they hold ownership or maintain affiliation, including through sharing of data?

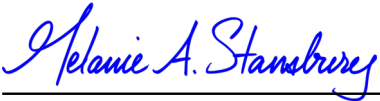
Sincerely,



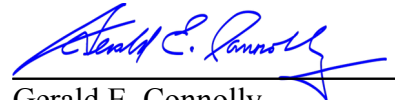
Donald S. Beyer Jr.
Member of Congress



Mike Levin
Member of Congress



Melanie Stansbury
Member of Congress



Gerald E. Connolly
Member of Congress



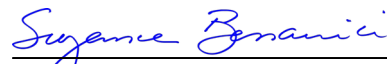
Zoe Lofgren
Member of Congress



Pramila Jayapal
Member of Congress



Doris Matsui
Member of Congress



Suzanne Bonamici
Member of Congress

Yvette W. Clarke

Yvette D. Clarke
Member of Congress

Valerie P. Foushee

Valerie P. Foushee
Member of Congress

Brittany Pettersen

Brittany Pettersen
Member of Congress

Rick Larsen

Rick Larsen
Member of Congress

Gwen S. Moore

Gwen S. Moore
Member of Congress

Hank Johnson

Henry C. "Hank" Johnson, Jr.
Member of Congress

Bill Foster

Bill Foster
Member of Congress

Sara Jacobs

Sara Jacobs
Member of Congress

Haley Stevens

Haley M. Stevens
Member of Congress

Adam Smith

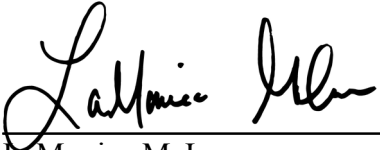
Adam Smith
Member of Congress

Dave Min

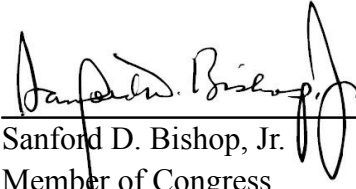
Dave Min
Member of Congress

Nanette Diaz Barragán

Nanette Diaz Barragán
Member of Congress



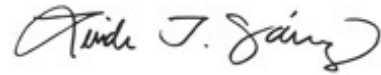
LaMonica McIver
Member of Congress



Sanford D. Bishop, Jr.
Member of Congress



Paul D. Tonko
Member of Congress



Linda T. Sánchez
Member of Congress



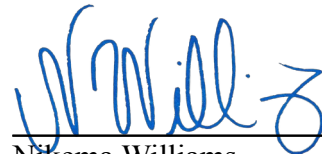
Danny K. Davis
Member of Congress



Kim Schrier, M.D.
Member of Congress



Bonnie Watson Coleman
Member of Congress



Nikema Williams
Member of Congress



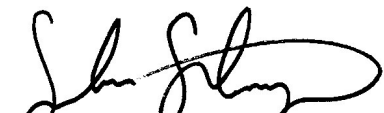
Shontel M. Brown
Member of Congress



James P. McGovern
Member of Congress



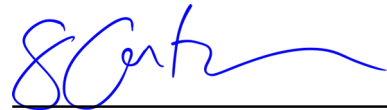
Stephen F. Lynch
Member of Congress



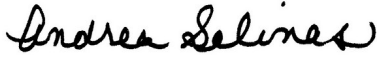
Suhas Subramanyam
Member of Congress



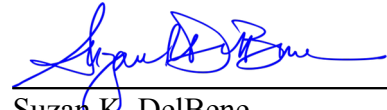
Brad Sherman
Member of Congress



Sean Casten
Member of Congress



Andrea Salinas
Member of Congress



Suzan K. DelBene
Member of Congress



Chrissy Houlahan
Member of Congress



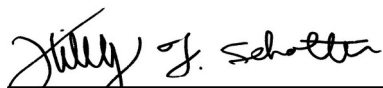
Betty McCollum
Member of Congress



Sylvia R. Garcia
Member of Congress



Robert J. Menendez
Member of Congress



Hillary J. Scholten
Member of Congress



Greg Casar
Member of Congress



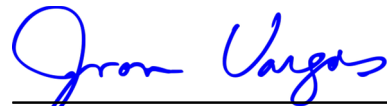
Jared Huffman
Member of Congress



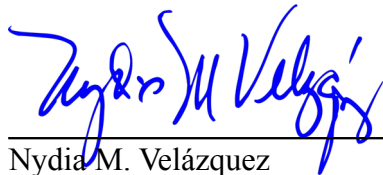
Gabe Amo
Member of Congress



Mark DeSaulnier
Member of Congress



Juan Vargas
Member of Congress



Nydia M. Velázquez
Member of Congress



Bradley Scott Schneider
Member of Congress

CC:

Ms. Amy Gleason
Acting Administrator
“Department of Government Efficiency”
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20502

The Honorable Michael Kratsios
Director
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, DC 20502

The Honorable Stephen Ehikian
Deputy Administrator and Acting Administrator
General Services Administration
1800 F Street, NW
Washington, DC 20405