



One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

February 5, 2025

Mr. Matthew J. Vaeth
Acting Director
Office of Management and Budget
725 17th St. NW
Washington, DC 20503

Dear Acting Director Vaeth:

We write to express our serious concerns about the unprecedented access to sensitive government data granted to Elon Musk and his US DOGE Service (DOGE) associates and inquire about what policies and procedures are in place to protect the security and integrity of sensitive government information.

Under the Federal Information Security Modernization Act (FISMA) of 2014, the Director of the Office of Management and Budget (OMB) is responsible for “developing and overseeing the implementation of policies, principles, standards, and guidelines on information security” and “requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (A) information collected or maintained by or on behalf of an agency; or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.”¹

Executive Order (EO) 14158, *Establishing and Implementing the President's “Department of Government Efficiency,”* gave DOGE unprecedented access to information systems across government.² It directs Agency Heads “to take all necessary steps” to ensure DOGE “has full and prompt access to all unclassified agency records, software systems, and IT systems.”³ The EO also directs DOGE to adhere to “rigorous data protection standards.”⁴ Although the EO fails to

¹ 44 U.S.C. 3553(a).

² Exec. Order No. 14158, *Establishing and Implementing the President's “Department of Government Efficiency,”* 90 Fed. Reg. 8441 (Jan 20, 2025), <https://www.federalregister.gov/documents/2025/01/29/2025-02005/establishing-and-implementing-the-presidents-department-of-government-efficiency>.

³ *Id.*

⁴ *Id.*

articulate those standards, they presumably include Federal laws including, but not limited to, FISMA, the E-Government Act of 2002,⁵ and the Federal Acquisition Regulation, as well as OMB policies intended to protect Federal networks, including OMB 22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.⁶ Instead, by all accounts, DOGE is running roughshod across Federal networks, accessing untold amounts of information about Americans in complete disregard for security and privacy standards.

According to media reports, in recent days, Elon Musk and his DOGE associates have accessed a broad range of government databases at multiple Federal agencies. These agencies include the Treasury Department, the U.S. Office of Personnel Management, the U.S. Agency for International Development, the Small Business Administration, and possibly others.⁷ The systems include the payment systems that the Treasury Department uses to honor U.S. financial obligations, those that store sensitive personnel data on Federal employees, and reportedly classified information systems, which DOGE has absolutely no authority to access. This reporting also indicates that DOGE officials have transferred data to commercial servers that may not have been vetted for compliance with security and privacy requirements, another potential violation of Federal law.⁸ These databases include personally identifiable information on Federal employees and millions of other American, and any risk of exposure to foreign adversaries could have grave national security consequences. Due to the complete lack of transparency about DOGE's activities, it is possible that DOGE has gained access to other information that the public is not yet aware of.

We know that China and other foreign adversaries are regularly seeking to breach Federal agency networks to gather exploitable information about government officials, American citizens, and U.S. businesses. That is why the U.S. government has implemented numerous policies and programs to secure sensitive data. Elon Musk and his DOGE associates are not exempt from those policies. Under your statutory obligations, you are responsible for ensuring that Elon Musk complies with data privacy and security requirements, and we urge you to take action to ensure compliance.

The American public deserves to know who is accessing their personal information and why. The government also has an obligation to keep their information secure. To help us better

⁵ 44 U.S.C. § 101.

⁶ OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (Jan. 26, 2022), <https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf>.

⁷ Fatima Hussein, *Elon Musk's DOGE commission gains access to sensitive Treasury payment systems: AP sources*, Associated Press, Feb. 1, 2025, <https://apnews.com/article/donald-trump-elon-musk-doge-treasury-5e26cc80fcb766981cea56afd57ae759>; Abigail Williams, Vaughn Hillyard, Yamiche Alcindor and Dan De Luce, *USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems*, NBC News, Feb. 3, 2023, <https://www.nbcnews.com/politics/national-security/usaids-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357>; Tim Reid, *Exclusive: Musk aides lock workers out of OPM computer systems*, Reuters, Feb. 2, 2023, <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/>.

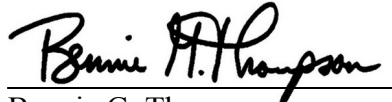
⁸ Caleb Ecarma and Judd Legum, *Musk associates given unfettered access to private data of government employees*, Musk Watch, Feb. 3, 2025, <https://www.muskwatch.com/p/musk-associates-given-unfettered>.


understand what policies and procedures are currently in place to secure data obtained by DOGE and what steps are being taken to secure Americans' data, we request that you respond to the following questions by February 19, 2025:

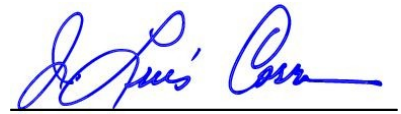
1. Which departments and agencies have granted DOGE access to their information systems and data? Please specify the types of information DOGE has accessed and the purpose of the access.
2. DOGE has no authority to access classified systems, but media reports indicate DOGE employees have, in fact, accessed such systems.
 - a. Have DOGE employees accessed classified systems? Please specify the authority under which DOGE employees accessed classified systems, which classified systems DOGE employees have accessed, and the purpose of DOGE access.
 - b. Do the DOGE employees who have accessed classified systems have security clearances? If so, did they complete the SF-86 form and undergo the background investigations required for Federal employees to obtain access to classified information. Please provide the dates upon which each DOGE employee who accessed classified information received their clearance, the type of security clearance each DOGE employee has, the date of their clearance security education meeting, and who provided the clearance security education meeting
3. What procedures are in place to ensure that DOGE complies with the E-Government Act of 2002's requirement of Privacy Impact Assessments for the use of new information technology?
4. How is OMB ensuring DOGE is in compliance with the Federal government's mandatory information security policies under FISMA and other relevant laws?
5. What guidance, if any, has OMB provided to Federal agencies how to mitigate security risks posed by DOGE access to their networks?
6. In the past, the US Digital Service accessed Federal department and agency information systems after being invited to do so. Do Federal agencies have the authority to refuse DOGE access to their information systems and data?


OMB has an obligation to ensure Federal information systems and data security laws are being followed, and we urge to move expeditiously to investigate what Federal laws and policies DOGE may have violated and take appropriate action. We look forward to your timely response.

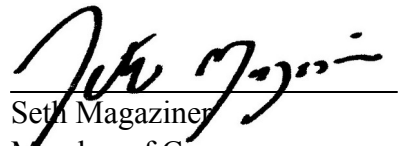
Sincerely,

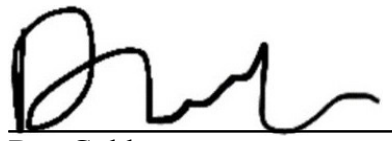

Bennie G. Thompson
Member of Congress
Ranking Member, Committee
on Homeland Security



Eric Swalwell
Member of Congress



J. Luis Correa
Member of Congress



Shri Thanedar
Member of Congress



Seth Magaziner
Member of Congress



Dan Goldman
Member of Congress


Delia C. Ramirez
Member of Congress


Timothy M. Kennedy
Member of Congress

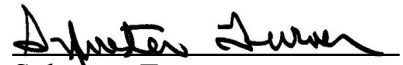

LaMonica McIver
Member of Congress


Julie Johnson
Member of Congress


Pablo José Hernández
Member of Congress

A handwritten signature in black ink that reads "Nellie Pou". The signature is written in a cursive style with a large, looping initial "N".

Nellie Pou
Member of Congress

A handwritten signature in black ink that reads "Sylvester Turner". The signature is written in a cursive style with a large, looping initial "S".

Sylvester Turner
Member of Congress