

Congress of the United States

Washington, DC 20515

July 9, 2025

The Honorable Doug Burgum
Secretary
Department of the Interior
1849 C Street, NW
Washington, DC 20240

Dear Secretary Burgum:

We write regarding public reports that you granted unfettered access to critical Department of the Interior (DOI) systems and sensitive data to individuals affiliated with the so-called Department of Government Efficiency (DOGE)—over the objections of senior DOI career officials whom you later terminated. The circumstances described in these reports raise profound risks to national security, the operations of multiple federal agencies and tribal nations, and the privacy of hundreds of thousands of Americans. We urge you to immediately rescind their access.

DOI is responsible for the administration of roughly 420 million acres of federal lands, nearly 55 million acres of tribal lands, more than 700 million acres of subsurface minerals, and about 2.5 billion acres of the outer continental shelf.¹ The Department also fulfills the United States' trust responsibilities to tribal nations and oversees a workforce of more than 60,000 civil servants. Through its Interior Business Center (IBC), DOI also plays a critical role in supporting over 150 different federal organizations with shared services, including acquisition, financial management, and human resources.² IBC systems such as the Federal Personnel and Payroll System (FPPS) support personnel and payroll operations for nearly 300,000 employees across more than 50 agencies.³

As DOI's operational scope has expanded, so too has its importance to U.S. national security. In January, President Trump designated the Secretary of the Interior as a member of the National Security Council (NSC) for the first time in the Department's history, joining the Secretaries of State and Defense and the National Security Advisor in shaping national security policy. With DOI's leading role in assisting in the operations of numerous federal agencies,⁴ safeguarding its information systems and data is among your most critical responsibilities.

Against this backdrop, we are deeply concerned by recent reports that you provided at least three DOGE-affiliated individuals—Tyler Hassen, Stephanie Holmes, and Katrine Trampe—with unfettered access to the IBC's FPPS system. These reports indicate that you granted this access despite significant concerns expressed by senior career DOI officials, including the Chief Information Officer and Chief Information Security Officer, who raised alarms in a risk assessment memorandum. According to the memorandum, DOGE's access requests were unprecedented and posed significant cybersecurity, operational, and legal risks—including potential

¹ "U.S. Department of the Interior: An Overview", Congressional Research Service (CRS), June 23, 2021, https://www.congress.gov/crs_external_products/R/PDF/R45480/R45480.3.pdf.

² "About the Interior Business Center," U.S. Department of the Interior, <https://www.doi.gov/ibc/about-us>.

³ "IBC Fact Sheets: Federal Personnel Payroll System," U.S. Department of the Interior, August 2024, <https://www.doi.gov/sites/default/files/documents/2024-08/ibc-fact-sheets-federal-personnel-payroll-system.pdf>.

⁴ "Organization of the National Security Council and Subcommittees," The White House, January 20, 2025, <https://www.whitehouse.gov/presidential-actions/2025/01/organization-of-the-national-security-council-and-subcommittees/>.

violations of the Privacy Act of 1974, which may carry criminal penalties. Rather than addressing these concerns, you reportedly placed these officials on administrative leave and later terminated them.

Since granting FPPS access to Mr. Hassen, Ms. Holmes, and Ms. Trampe, it is likely they have received—or will receive—similar access to additional DOI systems and data, including those relied upon by DOI’s federal partners.⁵ That level of access, reportedly exceeding even that of DOI’s Chief Information Officer (CIO), is deeply troubling. It creates exactly the kind of cybersecurity, operational, and privacy vulnerabilities that the experienced civil servants warned about in their risk assessment memo and sought to prevent. These individuals now have access that could allow, among other things, the exfiltration of data to unknown and unprotected destinations, the deletion of records and logs, the modification of system code or data, and the ability to grant the same capabilities to others. This is unacceptable for a multitude of reasons.

First, their access creates significant cybersecurity risks. A single compromised credential—whether through hacking, phishing, or coercion—could provide a direct pathway into DOI systems and, by extension, systems across the federal government. In 2015, the Chinese government obtained and exploited log-in credentials through a federal contractor to breach the Office of Personnel Management’s (OPM) network, allowing it to exfiltrate personnel data and security clearance files for tens of millions of individuals.⁶ Granting DOGE-affiliated employees unfettered access to any one system, let alone multiple systems, ignores the explicit information security controls put in place following the massive OPM breach and represents a major regression in federal cybersecurity posture. These individuals are now high-value targets for foreign intelligence services and criminal networks.

Second, such access puts core government operations at work. Mr. Hassen, Ms. Holmes, and Ms. Trampe likely possess the ability to modify the computer code that underlies critical DOI systems. In standard software development environments, code changes undergo rigorous testing and peer review before being deployed. Unvetted modifications, intentional or not, could introduce bugs that crash systems supporting personnel actions, facility access, and procurement.⁷ A single disruption could halt services relied upon by the Supreme Court, other federal agencies, and tribal governments, affecting millions of Americans.

Finally, your actions reflect a broader pattern under the Trump Administration of weakening privacy safeguards and centralizing access to personal data under the pretense of “efficiency.” Since taking office, President Trump and his designees have exploited the Privacy Act’s “need to know” exception to grant unvetted individuals unfettered access to sensitive data across dozens of agencies. A federal judge issued a temporary restraining order (TRO) blocking DOGE from accessing systems and the Social Security Administration (SSA), writing that “the DOGE Team is essentially engaged in a fishing expedition at SSA, in search of a fraud epidemic, based on little more than suspicion”.⁸ Yet the Trump Administration and DOGE continue their data aggregation

⁵ Coral Davenport, “DOGE Accesses Federal Payroll System Over Objections of Career Staff,” *The New York Times*, March 31, 2025, <https://www.nytimes.com/2025/03/31/us/politics/doge-musk-federal-payroll.html>; Tim Marchman, “Top Officials Places on Leave After Denying DOGE Access to Federal Payroll Systems,” *WIRED*, March 31, 2025, <https://www.wired.com/story/doge-access-federal-payroll-systems-officials-leave-interior/>; Natalie Alms, “Interior fires senior leaders after fight over DOGE access to key payroll system,” *Nextgov*, April 9, 2025, <https://www.nextgov.com/people/2025/04/interior-fires-senior-leadership-after-fight-over-doge-access-key-payroll-system/404421/>.

⁶ Majority Staff Report, “The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,” House Committee on Oversight and Government Reform, September 7, 2016, <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>.

⁷ “IBC Systems and Services,” U.S. Department of the Interior, <https://www.doi.gov/ibc/services>.

⁸ *American Federation of State, County, and Municipal Employees, AFL-CIO, et al. v. Social Security Administration, et al.*, No. ELH-25-0596 (D. Md. Mar. 20, 2025) <https://storage.courtlistener.com/recap/gov.uscourts.mdd.577321/gov.uscourts.mdd.577321.49.0.pdf>

and centralization efforts. Just days after the TRO was issued, President Trump signed an Executive Order (EO) that directs agency heads to “ensure Federal officials designated by the President or Agency Heads (or their designees) have full and prompt access to all unclassified agency records, data, software systems, and information technology systems.”⁹

The EO further instructs agency heads to “rescind or modify all agency guidance that serves as a barrier to the inter- or intra-agency sharing of unclassified information” and to facilitate “consolidation of unclassified agency records.”¹⁰ As the Administration paves the way for data centralization, DOGE staffers have likely been illegally exfiltrating personal information from other agencies.¹¹ We hope that you share our resolve to secure Americans’ privacy from abuse and that you recognize the glaring security risk of granting unfettered access to DOI’s information systems to Mr. Hassen, Ms. Holmes, and Ms. Trampe.

We therefore demand that you immediately reinstate the officials you terminated for raising concerns about DOGE’s access to DOI systems and data. Additionally, we urge you to issue a formal decision in response to the concerns raised in their risk assessment memorandum and to implement sufficient security controls if you continue to permit Mr. Hassen, Ms. Holmes, Ms. Trampe, or any other DOGE affiliates to retain their current level of access to FPPS or other DOI systems.

Moreover, we request a briefing on your decision to grant these individuals access to DOI’s information systems. At that briefing, please be prepared to answer the following questions:

1. For each of Mr. Hassen, Ms. Holmes, Ms. Trampe, and any other official who holds, or has held since January 20th, 2025, access to DOI information systems:
 - a. What is the nature of that individual’s relationship with DOI?
 - i. If the employee is full-time, to what other agencies are they detailed?
 - ii. If the individual is detailed to DOI, from which agency are they detailed?
 - iii. If the individual is a contractor, what firm do they work for?
 - b. For each DOI system to which the individual has had, currently has, or will have access:
 - i. What level of access to do they possess?
 - ii. What was the justification for providing such access?
 - iii. When was access provided?
 - iv. What training, including on security and privacy, was provided and did it occur before or after access was provided?

⁹ “Stopping Waste, Fraud, and Abuse by Eliminating Information Silos,” March 20, 2025, <https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/>

¹⁰ *Id.*

¹¹ “Elon Musk and DOGE team sit down with Bret Baier in ‘Special Report’ Exclusive,” FOX News, March 28, 2025, <https://www.foxnews.com/video/6370654580112>; Representatives Trahan, Brown, DelBene, “Letter to Treasury on DOGE,” https://trahan.house.gov/uploadedfiles/trahan_treasury_gsa_oig_letter_doge_spreadsheet_v2.0.pdf

- v. To the extent that access to the system was provided under a Privacy Act exception, what exception was invoked?
 - vi. What security controls were implemented, if any, for individuals granted access to the system?
 - vii. Has the individual modified, copied, shared, or removed any records from the system?
 - viii. Has the individual modified the system's code in any way?
 - ix. Has the individual granted, revoked, or otherwise modified access to the system for any other users?
 - x. Has the individual deleted logs or other evidence of their actions?
- c. Have all system logs related to the individual's access been preserved in accordance with the Federal Records Act?

Thank you for your attention to this important matter. Should you have any questions, please do not hesitate to contact us or our staff.

Sincerely,



Lori Trahan
Member of Congress



Jared Huffman
Member of Congress