

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<https://oversight.house.gov>

February 25, 2025

The Honorable Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear President Trump,

We write with increasing alarm about how individuals associated with Elon Musk and the Department of Government Efficiency (DOGE) appear to have introduced negligent cybersecurity practices into information technology systems at multiple government agencies. This reckless disregard of critical cybersecurity practices creates opportunities for hostile actors to access sensitive information. We urge your Administration to cease all DOGE activities that create serious cybersecurity vulnerabilities, expose government networks to cyberattacks, and risk disclosures of sensitive and personal information.

On February 4, 2025, we sent a letter to the Office of Personnel Management (OPM) highlighting reports of a server added to the OPM network “without regard for crucial security and privacy protections.” That letter requested information and records related to the installation of this server and its role in sending a potentially illegal resignation offer to federal employees across government agencies.¹ Although the deadlines in that letter have passed, we have received no response.

Since then, further evidence indicates that DOGE activities have exposed sensitive data at additional agencies. For example, public reporting indicates that DOGE has access to the Department of Treasury’s Secure Payment System, which distributes more than \$5 trillion in federal funding each year.² Internet histories show that under the current Trump Administration, any outside actor could reach Treasury’s Secure Payment System from the public internet, making this system accessible to malicious actors.³ Similar records show that systems at the

¹ Letter from Ranking Member Gerald E. Connolly, Committee on Oversight and Government Reform and Ranking Member Shontel Brown, Subcommittee on Cybersecurity, Information Technology, and Government Innovation to Acting Director Charles Ezell, Office of Personnel Management (Feb 4, 2025) (online at <https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.02.04.%20GEC%20and%20Brown%20to%20OPM-Ezell-%20DOGE%20Emails.pdf>).

² “DOGE” Access to Treasury Payment Systems Raises Serious Risks, Center on Budget and Policy Priorities (Feb. 11, 2025) (online at www.cbpp.org/research/federal-budget/doge-access-to-treasury-payment-systems-raises-serious-risks).

³ Shodan.io, “title:“Secure Payment System” country:“US”” (online at

Office of the Comptroller of the Currency, the Treasury Inspector General for Tax Administration, and the Office of the Inspector General were publicly exposed.⁴

Public internet records also show that servers at the Lawrence Livermore National Laboratory, Los Alamos National Laboratory, Thomas Jefferson National Accelerator Facility, and Fermi Accelerator National Laboratory all exposed entry points through which a malicious actor could remotely access their computer systems.⁵ Some of these labs study and manage the critical systems that support the U.S. nuclear weapons stockpile.⁶ It is deeply alarming that an adversary could exploit these vulnerabilities to gain full access to these systems.

Decades of efforts by both Republican and Democratic administrations, along with bipartisan collaboration in Congress, have strengthened the federal government's cybersecurity practices, making them more transparent, enforceable, and resilient.⁷ In a matter of weeks, reckless behavior by the unelected and unaccountable DOGE team has undermined this progress and left multiple government agencies vulnerable to cyberattacks by foreign agents and malicious actors.

To determine the severity of reported cybersecurity and privacy violations, we request that you provide the following information, as well as a briefing from the leadership of DOGE, on how DOGE is ensuring malicious actors do not have access to sensitive government systems, by March 11, 2025:

1. A list of all federal agencies to which individuals connected to DOGE have introduced new technology, including, but not limited to, virtual and physical servers, network appliances, databases, workstations, external application programming interfaces, or outside data endpoints;
2. A full inventory of virtual and physical machines introduced by individuals associated with DOGE into federal government networks since the first actions of the Trump Transition Team;
3. Any external entities to which the DOGE team has exfiltrated data;

www.shodan.io/search?query=title%3A%22Secure+Payment+System%22+country%3A%22US%22 (accessed Feb. 11, 2025).

⁴ Shodan.io, 199.83.35.87 (online at www.shodan.io/host/199.83.35.87) (accessed Feb. 11, 2025); Shodan.io, 164.95.159.34 (online at www.shodan.io/host/164.95.159.34) (accessed Feb. 11, 2025); Shodan.io, 164.95140.12 (online at www.shodan.io/host/164.95.140.12) (accessed Feb. 11, 2025).

⁵ Shodan.io, 'department of energy country:"US"' (online at www.shodan.io/search?query=department+of+energy+country%3A%22US%22) (accessed Feb. 11, 2025)

⁶ Department of Energy, National Nuclear Security Administration, *Locations* (online at www.energy.gov/nnsa/locations) (accessed Feb. 11, 2025).

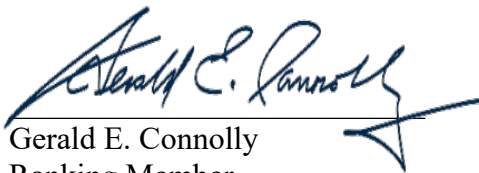
⁷ Government Accountability Office, *Cybersecurity: Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements* (Dec. 4, 2023) (GAO-24-105658) (online at www.gao.gov/products/gao-24-105658).

4. A list of all individuals given administrative or “sudo” access to federal information technology systems during the Trump Transition and after January 20, 2025; and
5. A list of all new vendors used by federal IT systems since the beginning of the Trump Transition.
6. Since January 20, 2025, how many cybersecurity incidents have been identified at federal agencies that may have exposed government systems or data?
7. For each incident, provide detailed information, including:
 - a. The agency involved;
 - b. The date of discovery;
 - c. The nature of the incident (e.g., failure to implement required security controls, unauthorized access, noncompliance with cybersecurity mandates); and
 - d. The specific government systems and data that may have been exposed.
8. What risk assessments were conducted for each identified incident? How were these incidents categorized in terms of their impact on confidentiality, integrity, and availability of federal data and systems? Were any incidents deemed to have posed a national security risk, and if so, how were they handled?
9. What corrective actions have been taken to address these cybersecurity incidents? Were affected systems patched, reconfigured, or isolated? If so, provide details on the remediation timeline.
10. Were any agencies found to have repeatedly violated cybersecurity policies, and if so, what enforcement actions were taken to ensure compliance?
11. Were any agencies and DOGE team members found to have failed to report cybersecurity violations to the appropriate authorities, including the Cybersecurity & Infrastructures Security Agency, the Office of Management and Budget (OMB), or agency inspectors general?
 - a. If so, what actions have been taken to hold those agencies accountable for noncompliance?
 - b. Were any federal employees, contractors, third parties, or DOGE team members found to have engaged in willful negligence or misconduct that contributed to cybersecurity violations?
12. Have any cybersecurity incidents resulted in confirmed or suspected breaches of personally identifiable information (PII) or other sensitive government data? If so, were affected individuals and entities notified as required by relevant breach notification policies?


13. How has the Administration ensured transparency in reporting cybersecurity violations to Congress and the public while safeguarding national security interests?

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. The Committee also has legislative jurisdiction over federal personnel and federal information systems. Full compliance with our requests is necessary, in part to determine whether legislative reforms are needed to ensure the continued security of our federal government systems and privacy of federal employees’ sensitive personnel data. If your staff have any questions regarding this request, please contact Committee Democratic staff at (202) 225-5051. Thank you for your prompt attention to this matter.


Sincerely,



Gerald E. Connolly
Ranking Member



Shontel Brown
Ranking Member
Subcommittee on Cybersecurity,
Information Technology, and
Government Innovation



Melanie Stansbury
Ranking Member
Subcommittee on Delivering
On Government Efficiency

cc: The Honorable James Comer, Chairman

The Honorable Nancy Mace, Chairwoman,
Subcommittee on Cybersecurity Information Technology, and Government Innovation

The Honorable Marjorie Taylor Greene, Chairwoman
Subcommittee on Delivering on Government Efficiency