United States Senate

WASHINGTON, DC 20510

July 21, 2026

The Honorable Scott Bessent
Secretary
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Dear Secretary Bessent:

We write regarding recent reports from the Government Accountability Office (GAO) and the Treasury Inspector General indicating that the Treasury Department provided two Department of Government Efficiency (DOGE) employees with improper access to the Bureau of the Fiscal Service's (BFS) payment systems in early 2025.[1] Treasury's failure to control access to these systems presented - and may still present - unacceptable risks: BFS handles nearly 90% of all federal payments, facilitates over 1.2 billion transactions per year,[2] and houses a slew of Americans' sensitive personal information. Any disruption of the system or its contents could have catastrophic consequences for the economy. We seek information on the Department's efforts to ensure that such a breach has been repaired and never occurs again.

On February 4, 2025, we asked GAO to conduct a review of reports suggesting that you had granted Elon Musk and other DOGE employees with "unprecedented access to the federal government's payment systems on January 31, 2025."[3] According to public reports at the time, you were "personally involved in granting Mr. Musk and his team access to these systems" and had played a key role in "pushing out the Department of the Treasury (Department)'s top career official, Mr. David Lebryk," who had "resisted requests from members of [President] Trump's transition team for access to the data."[4] On February 12, 2025, GAO agreed to conduct a review, which was released in April 2026.[5]

BFS operates three primary payment systems: the Secure Payment System (SPS), the Payment Automation Manager (PAM), and the Central Accounting Reporting System (CARS). These systems respectively certify payment files, process payment information, and preserve an

---

[1] U.S. Government Accountability Office, "Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls," Apr 28, 2026, https://www.gao.gov/products/gao-26-108131.
[2] Letter from Principal Deputy Assistant Secretary Jonathan Blum to Ranking Member Elizabeth Warren, February 4, 2025, https://www.banking.senate.gov/imo/media/doc/treasury_response.pdf.
[3] Letter from Ranking Member Elizabeth Warren and Ranking Member Ron Wyden to The Honorable Gene L. Dodaro, February 4, 2025, https://www.banking.senate.gov/imo/media/doc/letter_to_gao_on_musk_and_treasury.pdf.
[4] Letter from Senator Elizabeth Warren and Senator Ron Wyden to The Honorable Gene L. Dodaro, February 4, 2025, https://www.banking.senate.gov/imo/media/doc/letter_to_gao_on_musk_and_treasury.pdf;
The New York Times, "Elon Musk's Team Now Has Access to Treasury's Payments System," Andrew Duehren, Maggie Haberman, Theodore Schleifer, and Alan Rappeport, February 1, 2025, https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html.
[5] Letter from GAO officials to Senator Elizabeth Warren and Senator Ron Wyden, February 12, 2025, https://www.banking.senate.gov/imo/media/doc/gao_acceptance_letter.pdf.

electronic system of records. Access to Treasury payment systems is highly controlled – and for good reason. Treasury's systems contain Americans' sensitive payment information and most federal agencies use BFS systems to process payments, making "the integrity and security of these systems … critical to the nation's economy."[6] Yet according to GAO, the Treasury Department – under your leadership – failed to ensure that a DOGE employee agreed to follow Treasury's IT security rules and was unable to detect improper payment information transmissions. Treasury provided a DOGE employee with improper "access to view, copy, and print data for the three payment systems" for over a year.[7] This employee had the ability to view the source code of Treasury systems and was also "granted temporary access to create, modify, and delete data" for SPS.[8] In other words, not only could this employee view Treasury's sensitive financial information, but for a short period of time, they also had the ability to delete information and introduce inaccuracies into the system. This employee also sent unencrypted payment information regarding foreign aid to the General Services Administration (GSA); this security violation potentially exposed Personally Identifiable Information (PII) associated with over 350 individuals.[9] Treasury provided a separate DOGE employee with "over the shoulder access" to BFS systems. Though this employee did not have the ability to access systems themselves, they could request that bureau staff provide any payment system data of interest.[10] Concerningly, BFS has been unable to provide a list of systems and data viewed by this employee, due to the lack of controls regarding this access.[11]

A separate audit report released by Treasury's Office of Inspector General (OIG) in June 2026, corroborated GAO's findings.[12] The OIG found that giving an employee access to "sensitive payment systems and infrastructure" without following IT protocols did not follow NIST standards or Treasury policy, and that an employee improperly sent unencrypted PII outside of Treasury without any prior approval.[13] The OIG also stated that "[n]egligence of access controls could lead to data breaches and system outages," and specifically cited the PAM system as carrying higher data privacy and security risks compared to other BFS systems.[14]

As part of its report, GAO issued six recommendations to BFS on how to improve its data access controls.[15] Though BFS agreed with three of the recommendations, it "did not state whether it

---

[6] U.S. Government Accountability Office, "Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls," Apr 28, 2026, https://www.gao.gov/products/gao-26-108131.
[7] *Id.*
[8] *Id.*
[9] NextGov, "Treasury missed security controls in giving DOGE system access, GAO finds," Natalie Alms, April 28, 2026, https://www.nextgov.com/digital-government/2026/04/treasury-missed-security-controls-giving-doge-system-access-gao-finds/413174/; U.S. Government Accountability Office, "Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls," Apr 28, 2026, https://www.gao.gov/products/gao-26-108131.
[10] *Id.*
[11] *Id.*
[12] U.S. Department of Treasury, Office of Inspector General, Fiscal Service's Sensitive Payment Systems' Controls are Generally Adequate but Weaknesses and Deficiencies Exist (OIG-26-032), June 8, 2026, https://oig.treasury.gov/system/files/2026-06/Audit-of-Fiscal-Service-Sensitive-Payment-Systems-%28OIG-26-032%29---Locked.pdf.
[13] *Id.*
[14] *Id.*
[15] U.S. Government Accountability Office, "Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls," Apr 28, 2026, https://www.gao.gov/products/gao-26-108131.

agreed or disagreed with the other three," including updating policy to define minimum screening requirements for access to Treasury payment system data, verifying employees' acknowledgement of security rules prior to providing access to payment systems, and establishing a process for exit interviews.[16] It is unclear why BFS refused to acknowledge these recommendations. Similarly, the Treasury IG provided nine recommendations, including ensuring adherence to Treasury policy prior to access to Fiscal Service's systems and evaluating additional security measures to reduce the risk of unsecured transmission of personally identifiable information.

It is essential that Congress fully understand the extent of DOGE's improper access to federal payment systems and any threats to the systems posed by this improper access. We request answers to the following questions by August 4, 2026:

1) What specific data was accessed by the DOGE employee improperly granted access to three BFS payment systems?
    a) What was the justification for allowing a DOGE employee who had not agreed to follow the bureau's IT rules "access to view, copy, and print data for the three payment systems," including the Secure Payment System (SPS), the Payment Automation Manager (PAM), and the Central Accounting Reporting System (CARS)?
    b) GAO's study examined DOGE's access to the Treasury between January 20, 2025 and April 11, 2025. After April 11, 2025, did you, or any other Treasury employee or official, grant any additional DOGE employees improper access to BFS payment systems? If so, please provide details around who and what data they had access to.
    c) Did you, or any other Treasury employee or official, grant any non-DOGE employees improper access to BFS payment systems?

2) Please provide more information around the DOGE employee's "[inadvertent]" access to "create, modify, and delete" data on the Secure Payment System (SPS) that was granted on January 31, 2025 and revoked February 1, 2025?
    a) Please provide details around what specific data this system stores.
    b) Please provide details around repercussions if this employee had in fact created, modified, or deleted existing data and what the impact of data inaccuracies in this system would have been.
    c) Have employees ever inadvertently been given access to create, modify and delete data in Treasury systems in the past? If so, which systems, and what actions were taken after identifying this mistake?
    d) This mistake was reportedly made because "the requester amended their access request multiple times before it was approved."[17] If the requester had indeed meant to request "create, modify, and delete" permissions for this DOGE employee, would you have found this an acceptable request in compliance with your department's security regulations?

[16] *Id.*
[17] *Id.*

3) Please provide details around what unencrypted information was improperly sent by a DOGE employee and who specifically it was sent to.
    a) Was any personally identifiable information improperly shared to GSA, anonymized? If so, please provide details.
    b) What actions were taken after Treasury found that unencrypted data was shared?
    c) Were Treasury officials notified of a DOGE employee sending unencrypted data? If so, what actions did they take after notification? Please provide any related documentation.
    d) Were there any additional instances of unencrypted data being shared outside of Treasury by a DOGE employee or any Treasury employee or official? If so, please provide details.

4) Please provide documentation around security audits conducted on Treasury systems accessed by DOGE employees prior to 2025, including associated Authority to Operate (ATO)[18] paperwork and documentation.
    a) Have your security processes changed since your last ATO was granted? If so, how so?

5) Were you aware of existing controls and regulations around access to systems with sensitive data prior to hiring DOGE employees?
    a) If yes, why were these controls and regulations ignored?
    b) If not, had improper access to data been given to other employees prior to DOGE?

6) Please share your plan and timeline for implementing each of the Government Accountability's six recommendations listed below:[19]
    a) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to update BFS policy to define the minimum screening requirements for obtaining broad access to Treasury payment system data."
    b) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to update BFS policy to require employees to take IT security and privacy training before obtaining broad access to Treasury payment systems."
    c) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to establish and implement a process for verifying that employees sign BFS IT security rules of behavior prior to receiving broad access to payment systems."
    d) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to establish and implement a process for verifying that broad access granted to payment systems is consistent with the level approved by the authorizing official."
    e) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to establish and implement processes for conducting exit interviews and obtaining signatures on post-employment documentation in cases where these

[18] Digital.gov, "An introduction to ATOs," https://digital.gov/resources/an-introduction-to-ato.
[19] U.S. Government Accountability Office, "Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls," Apr 28, 2026, https://www.gao.gov/products/gao-26-108131.

cannot occur before individuals with access to payment systems leave the agency. In doing so, the Commissioner should expeditiously implement this process for the anonymized former employee discussed in this report (employee B)."

f) "The Secretary of the Treasury should direct the Commissioner of the Fiscal Service to either (1) configure BFS's data loss prevention tool to identify and block emails containing unencrypted payment information sent outside the agency, or (2) update BFS's process for reviewing emails with unencrypted payment information to include messages sent to other federal agencies and implement the updated process."

7) Please share your plan and timeline for implementing each of the Office of Inspector General's nine recommendations including the below three that focus specifically on improper access controls.[20]
   a) "Evaluate the existing configuration of the DLP solutions to determine whether additional security controls are necessary to mitigate the risk of unsecured external transmission of low-risk PII and implement any additional identified security controls."
   b) "Update Fiscal Service's Email and Instant-Messaging Policy to provide clarity on when low-risk PII constitutes CUI and disseminate the updated policy to all applicable Fiscal Service personnel."
   c) "Ensure Fiscal Service personnel adhere to Treasury policy and follow Fiscal Service onboarding procedures to ensure all users sign a Rules of Behavior form before granting them access to Fiscal Service's systems and infrastructure."

Sincerely,

Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs

Ron Wyden
United States Senator
Ranking Member, Committee
on Finance

[20] U.S. Department of Treasury, Office of Inspector General, Fiscal Service's Sensitive Payment Systems' Controls are Generally Adequate but Weaknesses and Deficiencies Exist (OIG-26-032)), June 8, 2026, https://oig.treasury.gov/system/files/2026-06/Audit-of-Fiscal-Service-Sensitive-Payment-Systems-%28OIG-26-032%29---Locked.pdf.