United States Government Accountability Office

Report to Congressional Requesters

April 2026

DEPARTMENT OF GOVERNMENT EFFICIENCY

Treasury Needs to Fully Implement Data Protection Controls

GAO-26-108131

GAO Highlights

DEPARTMENT OF GOVERNMENT EFFICIENCY

Treasury Needs to Fully Implement Data Protection Controls

GAO-26-108131 April 2026

A report to congressional requesters

For more information, contact: Marisol Cruz Cain at cruzcainm@gao.gov

What GAO Found

The U.S. government disburses payments for various reasons (e.g., income tax refunds, benefit payments, and vendor and salary payments). The majority of federal entities process their payments through the Bureau of the Fiscal Service's (BFS) payment systems. Accordingly, the integrity and security of these systems are critical to the nation's economy.

The preliminary results of GAO's ongoing work show that one Treasury Department of Government Efficiency (DOGE) team employee had access to three BFS payment systems between January 2025 and February 2025. The employee had access to view, copy, and print data for the three payment systems. In addition, the employee was inadvertently granted temporary access to create, modify, and delete data for one of the three systems, but GAO found no evidence of any changes to system data.

The bureau did not fully address three of four selected control areas for ensuring that DOGE team employees with access to BFS systems follow its IT security rules. (See table.) Specifically, BFS implemented five of the 14 selected controls within those four areas.

Extent to Which Bureau of the Fiscal Service (BFS) Implemented the Four Selected Cybersecurity Control Areas

Control area	Area rating
Control System Access (5 controls)	Partially implemented
Control System Integrity (2 controls)	Fully implemented
Control Information Confidentiality (4 controls)	Substantially implemented
Monitor System Usage (3 controls)	Substantially implemented

Source: GAO analysis of BFS documentation. | GAO-26-108131

Key: Fully implemented: BFS provided evidence that satisfied all of the related controls; Substantially implemented: BFS provided evidence that satisfied at least two-thirds, but not all, of the related controls; Partially implemented: BFS provided evidence that satisfied at least one-third, but less than two-thirds, of the related controls.

Examples of BFS not fully implementing specific controls include:

- BFS did not ensure that an employee agreed to follow the bureau's IT security rules before receiving a BFS laptop. As a result, the bureau was not well positioned to hold the employee accountable for not following those rules.
- BFS did not configure its security tools to identify and block unencrypted payment information resulting in an employee improperly transmitting payment information outside of the bureau.

In addition, the Treasury DOGE team did not always follow BFS's IT security rules. Specifically, an employee did not encrypt payment information sent to another agency DOGE team or obtain approval to share this information prior to sending it. This employee did not always follow the IT security rules because, as previously discussed, BFS did not implement all controls needed to ensure compliance with those rules. Until BFS fully implements controls for overseeing users with broad access to payment systems, this important information will be at greater risk of improper access, modification, disclosure, and misuse.

Why GAO Did This Study

The United States DOGE Service (USDS) was created by executive order to implement the President's goals to maximize government efficiency by modernizing technology. The order also calls for the heads of executive branch agencies to establish DOGE teams that work with USDS.

GAO was asked to review the efforts of Treasury DOGE staff to protect BFS systems. Its objectives were to (1) describe the DOGE team access to BFS payment systems, (2) evaluate the extent to which BFS implemented controls to ensure that the DOGE team followed the bureau's IT security rules, and (3) assess the extent that the DOGE team followed those rules.

In addressing its first objective, GAO summarized the preliminary results of its ongoing work describing access to payment systems. For the latter two objectives, GAO completed its audit work and is making recommendations. Specifically, GAO analyzed federal IT security guidance and identified 14 applicable controls in four areas related to managing system access and protecting sensitive information. GAO also analyzed BFS's IT security rules and evaluated documentation related to DOGE access to payment systems.

What GAO Recommends

GAO is making six recommendations to BFS to fully implement controls with identified weaknesses, including to ensure staff agree to follow IT security rules and configure security tools to identify and block the transmission of unencrypted payment information.

BFS agreed with three of the recommendations and did not state whether it agreed or disagreed with the other three. As discussed in the report, GAO maintains the recommendations are appropriate and warranted.

Contents

Figure

Abbreviations

BFS	Bureau of the Fiscal Service
CARS	Central Accounting Reporting System
DOGE	Department of Government Efficiency
FISMA	Federal Information Security Modernization Act of 2014
GSA	General Services Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PAM	Payment Automation Manager
PII	personally identifiable information
SPS	Secure Payment System
Treasury	Department of the Treasury
USAID	United States Agency for International Development
USDS	United States DOGE Service

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 28, 2026

Congressional Requesters

The United States DOGE Service (USDS) was created within the Executive Office of the President by Executive Order No. 14158 on January 20, 2025.[1] The service's mission is to implement the President's DOGE (Department of Government Efficiency) goals to maximize government efficiency and productivity by modernizing federal technology and software.[2] The order also calls for the heads of executive branch agencies to establish DOGE teams at their respective agencies that work with USDS and advise agency heads on the implementation of the goals. In addition, agency heads are to take all necessary steps to ensure that USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. The breadth of this access has led to concerns that agency systems and their sensitive information and data may be vulnerable to unauthorized disclosure or modification.[3]

The security of these agency systems and data is vital to the economy, public confidence, and national security. In addition, many of these

[1]Exec. Order No. 14158, 90 Fed. Reg. 8,441, *Establishing and Implementing the President's "Department of Government Efficiency"* (Jan. 20, 2025). Specifically, the executive order established this organization by: (1) renaming the United States Digital Service as the United States DOGE Service (USDS) and (2) creating a time-limited U.S. DOGE Service Temporary Organization within the new USDS to implement the organization's goals. The order also calls for both the overall USDS and the temporary organization to be led by a USDS Administrator who reports to the White House Chief of Staff.

[2]The executive order calls for USDS to undertake a software modernization initiative to improve the quality and efficiency of government-wide software, network infrastructure, and IT systems. In doing so, the order provides that the organization shall work with agency heads to promote interoperability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.

[3]For example, multiple lawsuits have been filed alleging possible violations of law that USDS and agency DOGE teams' access to federal records would create. Alliance for Retired Americans, et al. v. Bessent, et al. 1:25-cv-00313 (DDC 2025); American Federation of Teachers, et al. v. Bessent, et al. 8:25-cv-00430 (D. Md. 2025); and State of New York, et al. v. Donald J. Trump, in his official capacity as President of the United States, et al. 1:25-cv-01144 (SDNY 2025).

systems contain vast amounts of personally identifiable information (PII),[4] thus making it imperative to protect the confidentiality, integrity, and availability of these systems and their data.

Recognizing the importance of protecting federal systems and data, we have designated information security as a government-wide High-Risk area since 1997.[5] In 2015, we expanded it to include protecting the privacy of PII.[6] In September 2018, we issued an update to this High-Risk area that identified actions needed to address cybersecurity challenges facing the nation—including the need to better secure federal systems and information and protect privacy and sensitive data.[7]

In February 2025, the Department of the Treasury (Treasury) wrote to a U.S. Senator that a member of Treasury's DOGE team will have access to the Bureau of the Fiscal Service's (BFS) payment systems in order to assess the integrity of those systems and business processes. We were asked to review efforts to ensure that Treasury's DOGE team appropriately protected the systems and information they accessed at BFS.

Our objectives were to (1) describe the BFS payment systems at Treasury that the department's DOGE team had been provided access to and how the team planned to use those systems, (2) evaluate the extent to which BFS implemented controls to ensure that the DOGE team followed BFS's IT security rules, and (3) assess the extent that the DOGE team followed those rules.

[4]PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[5]For our most recent High-Risk update see GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

[6]GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[7]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018). For our most recent update on the status of these four challenges, see GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

For all of our objectives, we focused on Treasury DOGE team access to BFS payment systems between January 20, 2025, and April 11, 2025.[8] In addition, although we completed our audit work for the second and third objectives, we summarized the preliminary results of our continuing ongoing work for the first objective.[9]

To address our first objective, we reviewed service request tickets to determine the level of access that the DOGE team was approved to receive for each system.[10] We then observed the systems for which access was received—including accounts provided to DOGE team members, the roles for each account, and privileges assigned to the roles—and compared that account information to the access that was approved. We also observed and reviewed logs for DOGE team user accounts to identify the actions taken by each account.

In addition, we interviewed Treasury and BFS officials, including information security officers and database administrators, to clarify information in the service requests and system information we observed. We also discussed any inconsistencies between the requests and our observations. Further, we reviewed publicly available court documents, including declarations (i.e., sworn statements) made by Treasury and

[8]On April 11, certain court-imposed restrictions on Treasury DOGE team access to agency systems were lifted. State of New York, et al. v. Donald J. Trump, in his official capacity as President of the United States, et al. 1:25-cv-01144-JAV. We are continuing to perform audit work in this area and plan to issue a second report focusing on DOGE access to information systems at Treasury and its other components from January 20, 2025, onward, as well as to systems at BFS from April 11, 2025, onward.

[9]Our first objective focuses on employees with direct and indirect access to the systems. The results presented on this objective are preliminary. We obtained sufficient information on an individual with direct access via system logs, but information on an employee with indirect access was not logged and thus is more difficult to determine. We will continue to try to determine this employee's access as part of our ongoing review of DOGE access to Treasury systems. Our second and third objectives focus solely on the staff with direct access to the systems. Because the one Treasury DOGE team employee who had direct access to the systems left the agency prior to April 11, 2025 (the end of the time frame for this initial report), we were able to complete our work on the latter two objectives.

[10]Service requests tickets are submitted through BFS's Enterprise Service Management tool and are used to request that a user gain or lose access to a bureau system. These requests are then approved by a supervisor and implemented.

BFS officials and a former Treasury DOGE team employee[11] describing how the DOGE team planned to use its access.[12]

To address our second objective, we developed an evaluation framework and compared it to Treasury and BFS efforts to implement controls for ensuring that the DOGE team followed BFS's IT security rules. To develop the framework, we reviewed *NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations*[13] and selected 15 controls that are critical for managing privileged user access to systems and ensuring that sensitive information is protected. The 15 controls relate to the areas of (1) managing system access, (2) maintaining the integrity of agency systems, (3) protecting the confidentiality of information maintained by the agency, and (4) monitoring user activity on agency systems. We then compared BFS efforts to implement 14 of the 15 controls for any DOGE team members that received direct access (i.e., assigned system credentials, such as a username and password) to BFS payment systems between January 20, 2025, and April 11, 2025.[14] We were unable to determine if the 15th control was applicable, so we removed it from our assessment.[15] The following bullets describe our assessment for each of the four areas in the evaluation framework.

- **Control system access**. We analyzed Treasury and BFS policies and procedures for ensuring users meet personnel security requirements, providing IT security and privacy training, granting

[11]Alliance for Retired Americans, et al. v. Bessent, et al. 1:25-cv-00313 (DDC 2025); American Federation of Teachers, et al. v. Bessent, et al. 8:25-cv-00430 (D. Md. 2025); and State of New York, et al. v. Donald J. Trump, in his official capacity as President of the United States, et al. 1:25-cv-01144 (SDNY 2025).

[12]We also attempted to contact the two former Treasury DOGE team employees who had access to BFS payment data during the scope of our audit to discuss the scope of their access and plans for using it; we have not yet received a response to our requests.

[13]NIST, *Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, Md.: September 2020).

[14]As discussed in more detail later in the report, one of the two Treasury DOGE team members received direct access to BFS payment systems. As such, we focused on controls pertaining to this team member.

[15]The 15th control is in the system confidentiality area and pertains to assessing the effectiveness of controls at alternate work sites. BFS was unable to provide evidence describing whether the DOGE team member with access to Treasury payment systems used bureau systems from an alternate work site. As such, we were unable to determine whether the control was applicable.

system access, and securing systems and information after users leave the agency. We then compared the five controls in this area with the processes that BFS established and implemented to manage DOGE system access. In doing so, we analyzed artifacts documenting background investigation results, security and IT training records, access agreements, system service requests, and system logs. In addition, we conducted interviews with relevant BFS and Treasury officials to obtain an understanding of the controls in place to manage system access.[16]

- **Control system integrity**. We analyzed Treasury and BFS policies and procedures for protecting agency systems from the installation or execution of unauthorized software and identifying and analyzing changes made to systems by users. We then compared the two controls in this area with the processes and tools that BFS used to manage the integrity of systems for which the DOGE team was provided access. In doing so, we observed system configurations and analyzed artifacts documenting system logs and BFS's forensic review of the bureau laptop provided to the one DOGE team member with direct access to BFS systems. In addition, we conducted interviews with relevant BFS and Treasury officials to obtain an understanding of the controls in place to manage system integrity.
- **Control system confidentiality.** We analyzed Treasury and BFS policies and procedures for controlling the use of removable media, protecting data stored on agency systems and transmitted outside of the agency, and preventing exfiltration. We then compared the four applicable controls in this area with the tools and processes that BFS used to manage the confidentiality of the systems for which the DOGE team was provided access.[17] In doing so, we observed system configurations and analyzed system logs and BFS's analysis of the bureau laptop provided to one of the DOGE team members. In addition, we conducted interviews with relevant BFS and Treasury officials to obtain an understanding of the controls in place to manage system confidentiality.
- **Monitor system usage**. We analyzed Treasury and BFS policies and procedures for logging actions on agency systems, reviewing system logs, and responding to unauthorized system use. We then compared

[16]We also interviewed former Treasury officials that (1) worked at the department when DOGE team members requested access to payment systems and (2) were in important roles related to managing this access.

[17]As previously mentioned, we were unable to determine whether the control related to assessing the effectiveness of controls at alternate work sites was applicable.

the three controls in this area with the processes and tools that BFS used to monitor the usage of the systems for which the DOGE team was provided access. In doing so, we observed system configurations and analyzed artifacts documenting system logs and BFS's analysis of the bureau laptop provided to a DOGE team member. In addition, we conducted interviews with relevant BFS and Treasury officials to obtain an understanding of the controls in place to monitor BFS systems and devices.

We assessed each control as:

- *Fully implemented*—BFS provided evidence demonstrating the agency carried out the control consistent with agency policy and procedures.
- *Partially implemented*—BFS provided evidence demonstrating that (1) the agency's policies and procedures described some but not all aspects of how the control is to be carried out, or (2) the agency carried out some, but not all portions of the controls defined in agency policy or procedures.
- *Not implemented*—BFS did not provide evidence demonstrating that the agency carried out the control.

We also summarized the results of these assessments for each of the four areas. Specifically, we assessed each area as:

- *Fully implemented*—BFS provided evidence that fully satisfied all of the controls within the control area.
- *Substantially implemented*—BFS provided evidence that satisfied at least two-thirds, but not all, of the related controls.
- *Partially implemented*—BFS provided evidence that satisfied at least one-third, but less than two-thirds, of the related controls.
- *Minimally implemented*—BFS provided evidence that satisfied less than one-third of the related controls.
- *Not implemented*—BFS did not provide evidence that satisfied any of the related controls.

To address our third objective, we analyzed artifacts documenting Treasury DOGE team system activity (e.g., system logs and BFS's forensic analysis of a bureau laptop) for any DOGE team members that received direct access to BFS payment systems between January 20, 2025, and April 11, 2025. In addition, we reviewed declarations made by Treasury and BFS officials and a former Treasury DOGE team employee

describing the DOGE team employee's adherence to BFS's IT security rules. We also interviewed Treasury and BFS security officials to discuss what actions the officials took when they identified an instance where a DOGE team member did not fully follow the IT security rules.[18]

We conducted this performance audit from March 2025 to April 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

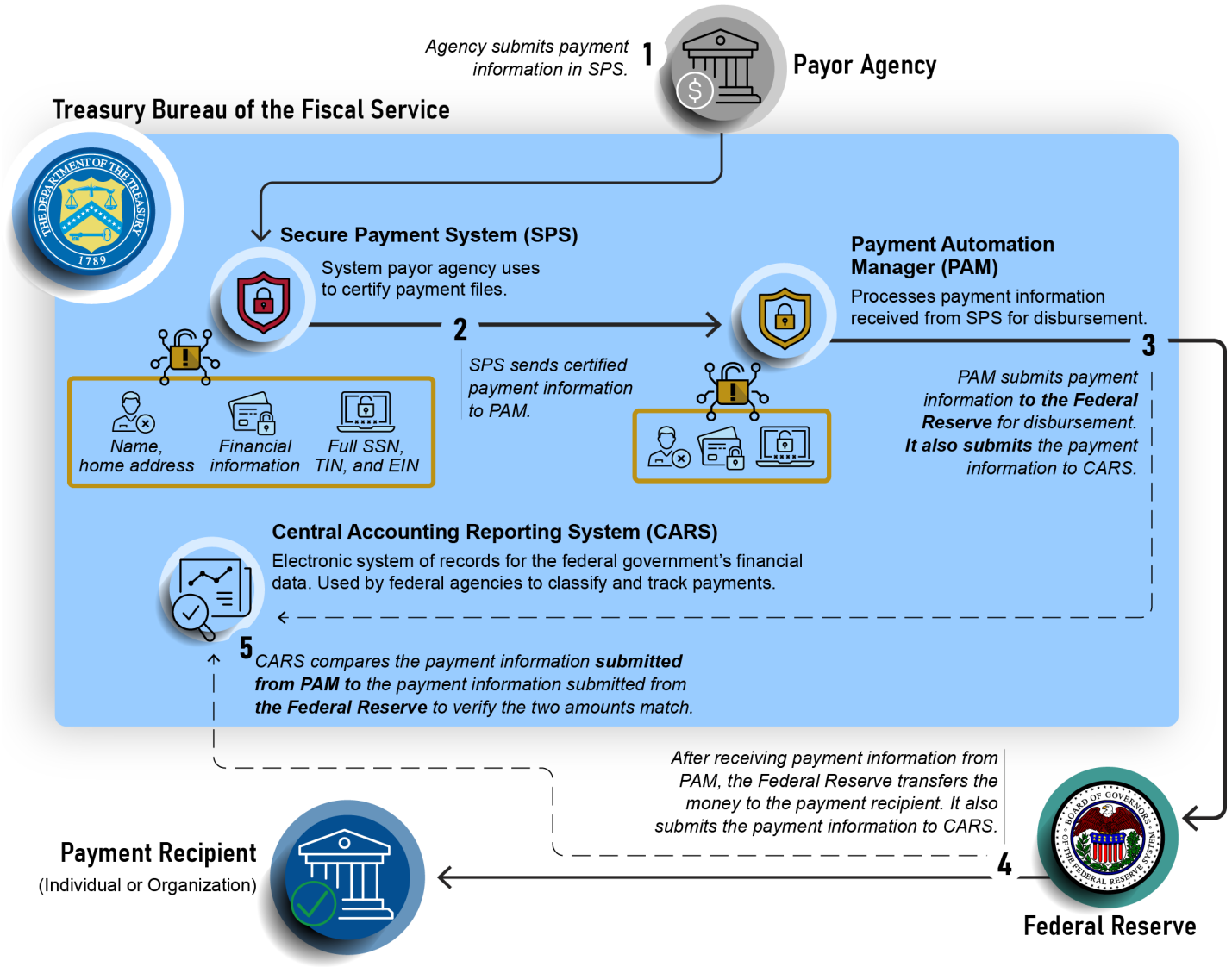
The U.S. government disburses payments for various reasons. This includes federal debt redemptions and interest, federal income tax refunds, benefit payments, vendor and salary payments, and other miscellaneous payments.

Most federal entities, such as individual departments and agencies, process their payments through BFS's payment systems. These federal entities internally review and approve payments to be made and submit certified payment schedules to BFS using the bureau's Secure Payment System (SPS). The bureau then processes the payment schedules via the Payment Automation Manager (PAM) and submits payment files to the Federal Reserve to make the payments, which are primarily made as electronic fund transfers.[19] After payments are made, various bureau systems capture the payment information in the Central Accounting Reporting System (CARS) for accounting and reporting purposes. Figure 1 illustrates the flow of payment information through these BFS payment systems.

[18]We also attempted to contact the former Treasury DOGE team employees to discuss an instance where BFS IT security rules were not followed; we have not yet received a response to our requests.

[19]Although there are other systems involved in the BFS payment process, we focused on the flow of payments through PAM in this report.

Figure 1: Flow of Agency Payment Information Through Bureau of the Fiscal Service (BFS) Payment Systems



SSN = social security number, TIN = taxpayer identification number, EIN = employer identification number

Contains Personally Identifiable Information

Sources: GAO analysis of Treasury data; lovemask/stock.adobe.com (all icons); agencies (logos). | GAO-26-108131

Treasury's DOGE Team

The Treasury DOGE team was established in January 2025 with the goals of modernizing federal technology and software, promoting interoperability between agency networks and systems, and facilitating responsible data collection and synchronization.[20] In pursuit of these goals, the department approved multiple DOGE team projects related to BFS payment processes and systems. The objectives of these projects were to (1) understand and improve the bureau's payment processes, and (2) identify and flag foreign aid payments for review by the Department of State.

In support of these projects, Treasury appointed two DOGE team employees in January 2025 using Schedule C temporary hiring authority; this authority allows agencies to create temporary positions following a change in presidential administration or agency leadership.[21] Treasury then assigned the employees to projects related to BFS payment systems. These employees are referred to as employee A and employee B throughout the report. Table 1 lists the appointment date, departure date, title, and employment status of the two team members who had access to bureau payment systems between January 20, 2025, and April 11, 2025.[22]

[20]Executive Order 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025). Specifically, the executive order directed each agency to establish a DOGE team in order to modernize federal technology and software to maximize governmental efficiency and productivity, to promote interoperability between agency networks and systems, to ensure data integrity, and to facilitate responsible data collection and synchronization.

[21]5 CFR 213.3302. Specifically, federal agencies are permitted to establish temporary transitional Schedule C positions necessary to assist a department or agency head during the 1-year period immediately following a change in presidential administration. Individual appointments made under this authority are not to exceed 120 days, with one extension of an additional 120 days.

[22]Between February and April of 2025, Treasury reported that it appointed five employees as additional DOGE team members under Schedule C transitional hiring authority. The majority of these individuals were appointed to Advisor for IT Modernization roles within Treasury's Office of the Chief of Staff. However, between February 8, 2025, and April 11, 2025, DOGE team members were fully enjoined by court order from accessing Treasury payment information and systems. On April 11, 2025, the court partially dissolved the preliminary injunction, allowing access to systems under particularized conditions (State of New York, et al. v. Donald J. Trump, in his official capacity as President of the United States, et al. 1:25-cv-01144-JAV). This report focuses on the two Treasury DOGE team members with access to Treasury payment systems prior to April 11, 2025. We have additional ongoing work reviewing DOGE access to Treasury payment systems after April 11, 2025.

Table 1: Treasury DOGE Team Employees with Access to the Bureau of the Fiscal Service (BFS) Payment Systems Between January 20, 2025, and April 11, 2025

DOGE team employee	Appointment date	Departure date	Title(s)	Employment status
Employee A	January 23, 2025	June 6, 2025	Senior Advisor for Technology and Modernization	Appointed as a special government employee
			Delegated Duties of the Fiscal Assistant Secretary	Converted to transitional Schedule C employee
Employee B	January 21, 2025	February 6, 2025	Special Advisor for Information Technology and Modernization	Transitional Schedule C, non-special government employee

Source: GAO analysis of BFS documentation. | GAO-26-108131

Notes: A special government employee is an employment classification used to hire outside consultants or experts for a limited period of time. These positions are not subject to certain federal ethics requirements.

A transitional Schedule C employee is an employment classification used to create temporary positions at the start of a new presidential administration or after a change in agency leadership. Unlike special government employees, transitional Schedule C employees are subject to federal ethics requirements.

Federal Laws and Guidance Establish Security Requirements to Protect Federal Systems and Information

Federal laws, along with executive branch policy and guidance, establish agency requirements and responsibilities for protecting federal systems and information, including PII and other sensitive information. These include the following laws and guidance, among others:

- **Federal Information Security Modernization Act of 2014 (FISMA)**. The act is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls in place to protect the information resources that support federal operations and assets.[23] For example, the law requires each agency to develop, document, and implement an agencywide information security program to provide risk-based protections for the information and information systems that support both the operations and assets of the agency. In addition, FISMA requires agencies to comply with National Institute of Standards and Technology (NIST) standards.

  FISMA also requires the Office of Management and Budget (OMB) to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies,

[23]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

except with regard to national security systems. The law assigns OMB the responsibility of requiring agencies to identify and provide information security protections commensurate with assessments of risk to their information and information systems.

- **Privacy Act of 1974**. The act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records.[24] It also requires agencies to issue system of records notices to inform the public when they establish or make changes to a system of record. These notices are to identify, among other things, the types of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and the procedures that individuals can use to review and correct personal information.
- **E-Government Act of 2002**. The act strives to enhance protection for personal information in government information systems by requiring agencies to conduct, where applicable, a privacy impact assessment for each system.[25] This assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. Agencies must conduct a privacy impact assessment before developing or procuring IT that collects, maintains, or disseminates information in an identifiable form. An assessment must also be performed before initiating any new data collections involving identifiable information that will be collected, maintained, or disseminated using IT if the same questions or reporting requirements are imposed on ten or more people.
- **NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations**. This document provides a catalog of security and privacy controls for systems and organizations. While previous revisions of this publication included a separate appendix detailing specific privacy controls, revision 5, issued in September 2020, aims to fully integrate

[24]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (Dec. 31, 1974) (codified as amended at 5 U.S.C. § 552a). A system of records is a collection of information about an individual under control of an agency from which information is retrieved by the name of an individual or other identifier. 5 U.S.C. § 552a(a)(4), (5).

[25]E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921-22 (Dec. 17, 2002).

privacy controls into the security control catalog, creating a consolidated and unified set of controls.[26]

- **OMB Circular A-130, Managing Information as a Strategic Resource**. This document requires agencies to employ a process for selecting and implementing security controls for information systems that satisfies the security control baselines in NIST Special Publication 800-53, tailored as appropriate.[27]

Preliminary Results Show That Treasury's DOGE Team Accessed Several BFS Payment Systems

The preliminary results of our ongoing work reviewing DOGE access to Treasury systems and data show that two Treasury DOGE team employees had access to several BFS payment systems. Specifically:

- BFS officials provided employee A with indirect, "over the shoulder" access to BFS payment systems; this employee did not have the ability to access the systems independently. This access allowed employee A to request that bureau staff access any payment system and show the employee specific data in it. Employee A did not have their own BFS account that they could use to access the payment systems themselves.

  BFS officials explained that they cannot provide a comprehensive list of the systems accessed by DOGE employee A because "over the shoulder" access does not generate logs that are directly linked to the user. We attempted to contact Treasury DOGE team employee A to discuss this access; we have not yet received a response to our request. We will continue to examine which systems were accessed by employee A.
- BFS provided employee B with direct access to view, copy, and print (but not modify or delete) data for three bureau payment systems.[28] Additionally, employee B was able to read a copy of the source code for three payment systems.[29] The bureau removed employee B's

[26]NIST, *Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, Md.: September 2020).

[27]OMB, Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[28]The three systems employee B could view data for were PAM, SPS, and CARS.

[29]Those three systems employee B could review source code for were PAM, SPS, and Automated Standard Application for Payment.

access to these systems on February 6, 2025—the same day that the individual resigned from Treasury.

At one point, the bureau mistakenly granted employee B the ability to modify data in one system between January 31, 2025, and February 1, 2025.[30] A Treasury official reported that the SPS system administrator granted the incorrect access because of confusion in interpreting the approved request. In particular, according to Treasury officials, the requester amended their access request multiple times before it was approved, due to changes in the level of access the employee needed.[31] However, BFS officials did not believe employee B was aware that they had elevated access, and the employee did not make any changes to the system data while they had this access.[32] (We discuss this mistake and the shortcoming that allowed it to occur later in this report.)

Table 2 provides a list of the systems that the bureau reported the Treasury DOGE team members were granted access to between January 20, 2025, and April 11, 2025.

[30]Although employee B's account was given elevated access to the system on January 31, 2025, Treasury and BFS officials reported that the employee was not able to use this access until after it had been corrected to read-only. Specifically, employee B reportedly first accessed the system on February 5, 2025, when the bureau provided the employee with login credentials and conducted a guided walkthrough of the system with them.

[31]Specifically, the ticket included multiple comments changing the requested level of access to SPS between "read-only" and "read/write" access, with the final level of access requested before the ticket was approved being "read/write."

[32]We attempted to contact Treasury DOGE team employee B to discuss this access; we have not yet received a response to our request.

Table 2: Bureau of the Fiscal Service (BFS) Payment Systems Accessed by Treasury DOGE Team Employee B

System name	Description	Date granted access	Level of access
Payment Automation Manager	A system that validates certified payment files, screens the files for certain types of potential improper payments, and organizes the files into payment groups for disbursement.	January 31, 2025	• Could access PII data • Could not create, modify, or delete data • Could read copy of source code
Secure Payment System	A system agencies use to securely create, certify, and submit individual payment files to Treasury.	January 31, 2025	• Could access PII data • Could create modify, or delete data between January 31 and February 1 • Could not create, modify, or delete data between February 1 and February 6[a] • Could read copy of source code
Central Accounting Reporting System	A system that pulls data from BFS payment systems to generate payment reports.	February 3, 2025	• Could access non-PII data • Could not create, modify, or delete data
Automated Standard Application for Payments	A system that allows recipients to withdraw funds (e.g., grants) from an established account.	January 28, 2025	• Could not access data • Could read copy of source code

Source: GAO analysis of BFS documentation. | GAO-26-108131

Note: Treasury DOGE Team employee B left the agency on February 6, 2025.

Bureau officials reported that the Treasury DOGE team requested access to these systems in support of their reviews of payment processes and foreign aid payments. Specifically:

- **BFS payment processes**. The DOGE team requested access to bureau systems as part of their review of the agency's payment processes. According to officials, the goal of the project was for the DOGE team to gain insights into how money flows through the bureau payment systems while identifying potential efficiencies in the overall payment flow.
- **Foreign aid payments**. Officials reported that the goal of the project was for the Treasury DOGE team to assist federal agencies submitting foreign aid payment information through BFS in identifying payments that may be impacted by the executive order on reevaluating and realigning U.S. foreign aid.[33]

[33]Exec. Order No. 14169, 90 Fed. Reg 8619, *Reevaluating and Realigning United States Foreign Aid*, (Jan. 20, 2025).

BFS Did Not Fully Implement All Selected Cybersecurity Controls on Payment Systems

It is important that agencies implement security and privacy controls to help ensure that users with access to agency systems and information follow associated IT system rules of behavior. NIST guidance—particularly *Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations*—identifies many such controls.[34] We relied on this guidance to develop an evaluation framework of 14 applicable cybersecurity controls and four associated control areas related to managing privileged user access to systems and ensuring that sensitive information is protected (see table 3).[35]

[34]NIST, *Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, Md.: September 2020).

[35]As previously discussed, we selected 15 controls. However, we were unable to determine whether one control—assessing the effectiveness of controls at alternate work sites—was applicable.

Table 3: Summary of Selected Controls for Protecting Systems and Associated Control Areas

Control area	Control
Control System Access	Ensure that staff are granted access to systems based on agency policies and procedures.
	Ensure that staff meet personnel security requirements for system access, consistent with agency policies and procedures.
	Ensure that staff take training required for system access, consistent with agency policies and procedures.
	Ensure that staff sign access agreements required for system access, consistent with agency policies and procedures.
	Ensure that access is disabled and other policies and procedures are followed for any staff that have left the agency.
Control System Integrity	Implement one or more controls to ensure that only authorized software is allowed to be installed and/or executed on agency systems.
	Implement staff-led system changes after analyzing the security and privacy implications of those changes.
Control System Confidentiality	Implement one or more controls to increase assurance that staff access, store, transport, and use system media consistent with agency policies and procedures.
	Implement cryptography mechanisms to protect the confidentiality of agency information at rest on equipment used by staff.
	Implement controls that call for or require staff to implement a cryptographic mechanism to protect external transmission of agency-controlled information.
	Implement one or more controls for preventing the exfiltration of information (e.g., data loss prevention tool).
Monitor System Usage	Collect audit logs detailing user activity on agency systems.
	Conduct regular reviews of audit logs, as required by agency policies and procedures.
	Identify unauthorized use of agency systems through organization-defined methods and techniques.

Source: GAO analysis of federal guidance. | GAO-26-108131

The bureau fully implemented five of the 14 selected controls for ensuring that DOGE team employees with access to BFS systems follow its IT security rules. Table 4 summarizes the extent to which the bureau implemented controls in the four areas.

Table 4: Extent to Which Bureau of the Fiscal Service (BFS) Implemented the Four Selected System User Control Areas

Control area	Area rating
Control System Access	Partially implemented
Control System Integrity	Fully implemented
Control System Confidentiality	Substantially implemented
Monitor System Usage	Substantially implemented

Source: GAO analysis of BFS documentation and cybersecurity tool configurations. | GAO-26-108131

Key: *Fully implemented*: BFS provided evidence that fully satisfied all of the controls within the area.

Substantially implemented: BFS provided evidence that satisfied at least two-thirds, but not all, of the related controls.

Partially implemented: BFS provided evidence that satisfied at least one-third, but less than two-thirds, of the related controls.

Minimally implemented: BFS provided evidence that satisfied less than one-third of the related controls;

Not implemented: BFS did not provide evidence that satisfied any of the related controls.

BFS Partially Implemented Controls Associated with System Access

Of the five controls associated with the control system access area, BFS partially implemented four and did not implement one, as shown in table 5. A more detailed discussion on the implementation status of each control follows the table.

Table 5: Bureau of the Fiscal Service (BFS) Efforts to Implement System Access Controls

Control System Access area rating	Control	Control rating
Partially implemented	Ensure that staff meet personnel security requirements for system access, consistent with agency policies and procedures.	◑
	Ensure that staff take training required for system access, consistent with agency policies and procedures.	◑
	Ensure that staff sign access agreements required for system access, consistent with agency policies and procedures.	○
	Ensure that staff are granted access to systems based on agency policies and procedures.	◑
	For any staff that have left the agency, ensure that access is disabled and other policies and procedures are followed.	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented N/A = Not applicable

Source: GAO analysis of BFS documentation and cybersecurity tool configurations. | GAO 26-108131

- **Ensure that staff meet personnel security requirements for system access, consistent with agency policies and procedures.** Treasury security policy requires that every position at the agency be assigned a sensitivity level based on the level of risk associated with

the role. Treasury policy also requires that every individual at the agency undergo screening commensurate with the sensitivity level of their position before authorizing access to agency systems.

Consistent with this policy, Treasury designated employee B as having a "special-sensitive" position—meaning that individuals in this position have the potential to cause "inestimable damage" to national security. In addition, Treasury performed preliminary fingerprint checks and reviewed this employee's personnel security questionnaire (referred to as a Standard Form 86). As a result, Treasury determined that there were no indications (e.g., criminal conduct) that the individual would not be suitable for this position. As such, Treasury granted this individual an interim secret clearance on January 22, 2025. Treasury officials noted that a final clearance would be granted after completion of a background investigation and favorable adjudication.

However, BFS policy did not define the extent to which the screening must be complete (e.g., preliminary checks and completion of investigation) before granting access to all data in federal payment systems. Bureau officials explained that Treasury policy defines a minimum security level for each role and the systems that users with those responsibilities are expected to access. However, the policy did not describe whether an individual's investigation needs to be complete prior to providing broad access to federal payment data. In the absence of these minimum requirements, it is unclear whether employee B received the screening needed to access these data. Until BFS updates its policy to define minimum screening requirements for obtaining broad access to Treasury payment system data, the information in these systems will be at increased risk of compromise.

- **Ensure that staff take training required for system access, consistent with agency policies and procedures.** Treasury and BFS policy requires that all employees complete security and privacy literacy training within 5 days of being granted access to bureau systems, and that employees in specialized roles receive role-based security training before being granted access to bureau systems. Additionally, agency policy requires that any individual who has been granted access to a bureau computer complete IT security and privacy training within 60 days of gaining access, and that training taken by the employee be documented for future reference. This training includes courses on cybersecurity awareness, records management procedures, and agency security requirements.

Bureau officials reported that they briefed employee B of their responsibility to protect agency information prior to providing them access to BFS systems. They believed this briefing addressed the requirement to provide the individual with security training prior to granting them system access. However, although BFS demonstrated that a meeting between employee B and bureau officials occurred, the bureau did not provide associated documentation outlining the topics discussed in the meeting.[36] Additionally, employee B did not complete their required security training before leaving the bureau. BFS officials stated that employee B was not required to complete their assigned IT security and privacy training because the employee's tenure at the bureau lasted less than the 60-day training period. However, employee B was provided access to sensitive payment systems prior to completing this training.

Without such training, there was an increased risk that employee B would not appropriately protect the confidentiality of PII in payment systems. Until BFS requires employees to take IT security and privacy training before obtaining broad access to payment systems, it will have less assurance that its employees will appropriately protect PII.

- **Ensure that staff sign access agreements required for system access, consistent with agency policies and procedures.** Treasury's IT security policy requires that users sign the BFS's IT security rules of behavior document before being granted access to its systems. However, the bureau did not ensure that employee B signed those rules before receiving a bureau laptop and subsequently leaving the bureau.

  Employee B was allowed access to payment systems without signing the rules of behavior document because BFS had not established and implemented a process for verifying the rules of behavior document was signed prior to granting access. Bureau security officials reported that they allowed employee B access to these systems without signing the rules of behavior document because the officials mistakenly believed the employee's possession of a bureau laptop meant they had already signed it. Those officials explained that bureau employees are required to sign the rules of behavior in order

[36]BFS senior officials reported during interviews and in a court filed declaration that they briefed employee B on bureau policies related to protecting agency information and systems prior to granting them access to BFS systems.

to receive a laptop.[37] Until BFS establishes and implements a process for verifying that these rules are signed prior to granting broad access to payment systems, the bureau will not be well positioned to hold employees accountable for following IT security and privacy policies.

- **Ensure that staff are granted access to systems based on agency policies and procedures.** BFS policy and procedures call for relevant system managers and security officers to approve payment system access requests before granting access. Although BFS followed its policy and procedures for approving payment system access for employee B, the bureau did not always ensure that the access granted was consistent with what was approved. Specifically, according to BFS officials, the bureau accidentally provided employee B with "read/write" access to SPS rather than "read-only."[38]

  This mistake was due, in part, to the lack of a process for verifying that the access granted was consistent with the level approved by the authorizing official. In the absence of such a process, as previously mentioned, the SPS system administrator granted the incorrect access because of confusion in interpreting the approved request. In particular, according to Treasury officials, the requester amended their access request multiple times before it was approved, due to changes in the level of access the employee needed, and the final entry in the request for SPS was for "read/write" access. As such, the SPS system administrator was confused regarding the level of access to grant the employee, according to Treasury officials.

  Bureau officials corrected the error within 1 day of providing elevated access, and employee B did not use the system during this time.[39] However, during the period when employee B's account had "read/write" access to SPS, it had the ability to modify federal

[37]BFS officials added that, once they learned employee B had not signed the rules of behavior, they requested that the employee sign the form. However, the individual resigned from the agency the same day, and the employee did not sign the form before leaving the agency.

[38]Unlike "read-only" access, which only allows a user to look at data that is saved in an information system, "read/write" access also allows a user to change, delete, or add data to a system.

[39]As previously discussed, the SPS account logs for employee B indicate that their account was given elevated access to SPS on January 31, 2025 before it was subsequently corrected on February 1, 2025. BFS officials explained that the employee was not able to use this access until February 5, 2025, when the bureau provided the employee with login credentials and conducted a guided walkthrough of the system with them.

payment data (e.g., payment amounts). Until BFS develops and implements a process to ensure that access granted to payment systems is consistent with what was approved, the bureau will have less assurance that users have the lowest level of access needed to protect PII.

- **For any staff that have left the agency ensure that access is disabled, and other policies and procedures are followed.** Treasury and BFS policy require system owners to (1) remove access within 2 business days of employees leaving the bureau, (2) conduct exit interviews with any departing employees to discuss their post-employment data protection requirements, and (3) ensure the departing employees sign associated exit documentation (e.g., classified information nondisclosure agreement). Additionally, if the employee or contractor does not sign their exit documentation upon their departure from the agency, policy requires that they be sent the document via overnight mail in an effort to have it signed, and that this effort be documented.

  Although BFS revoked employee B's access to bureau systems within 2 business days of their departure, neither BFS nor Treasury conducted an exit interview or ensured that the employee acknowledged their post-employment data protection requirements. This weakness was enabled by BFS's lack of a process for conducting exit interviews and signing post-employment documentation in cases where employees leave unexpectedly before these steps can take place.

  BFS officials reported that they did not conduct this interview or ensure that employee B signed an agreement because the employee resigned from the agency unexpectedly.

  - Regarding the **exit interview**, bureau officials noted that because the individual was an employee of Treasury rather than BFS, they believed it was ultimately Treasury's responsibility to complete these efforts; Treasury concurred with this. However, Treasury also did not conduct an exit interview or obtain a signed acknowledgement of the individual's post-employment data protection requirements when they left the agency. Additionally, neither BFS nor Treasury attempted to follow-up with employee B to attempt to conduct an exit interview by phone after they left the agency or provide them with a copy of the exit documentation and obtain their signature.
  - With respect to the **signed agreement**, Treasury reported that it believed the classified information nondisclosure agreement

completed by employee B when they were onboarded addressed this requirement. However, the nondisclosure agreement requires the employee to re-sign it at the conclusion of their employment in order to certify that they have been debriefed, which employee B did not do.

As a result, employee B was never informed of or agreed to their post-employment data protection requirements at the time of their departure from the agency. Nevertheless, the employee possessed an interim secret security clearance and accessed multiple BFS systems containing sensitive federal payment information. Until the bureau establishes and implements a process for conducting exit interviews and signing post-employment documentation in cases where individuals with access to payment systems leave unexpectedly, it will have less assurance that these individuals will appropriately protect this sensitive information.

BFS Fully Implemented the Applicable Control Associated with System Integrity

BFS fully implemented the one applicable control associated with the control system integrity area, as shown in table 6.

Table 6: Bureau of the Fiscal Service (BFS) Efforts to Implement System Integrity Controls

Control System Integrity area rating	Control	Control rating
Fully implemented	Implement one or more controls to ensure that only authorized software is allowed to be installed and/or executed on agency systems.	●
	Implement staff-led system changes after analyzing the security and privacy implications of those changes.	N/A[a]

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented N/A = Not applicable

Source: GAO analysis of BFS documentation and cybersecurity tool configurations. | GAO-26-108131

[a]This control was not applicable because the Treasury DOGE team did not make changes to the systems they accessed during the scope of our review.

Specifically, BFS protected the integrity of its information systems by implementing security controls on bureau laptops that prevent the installation or execution of any unauthorized software and log actions taken by users. By fully implementing this control, the bureau is better positioned to protect the integrity of its information systems.

BFS Substantially Implemented Controls Associated with Information Confidentiality

Of the four controls associated with the control information confidentiality area, BFS fully implemented two and partially implemented two, as shown in table 7.

Table 7: Bureau of the Fiscal Service (BFS) Efforts to Implement Information Confidentiality Controls

Control Information Confidentiality area rating	Control	Control rating
Substantially implemented	Implement one or more controls to increase assurance that staff access, store, transport, and use system media consistent with agency policies and procedures	●
	Implement cryptography mechanisms to protect the confidentiality of agency information at rest on equipment used by staff.	●
	Implement controls that call for or require staff to implement a cryptographic mechanism to protect external transmission of agency-controlled information.	◑
	Implement one or more controls for preventing the exfiltration of information (e.g., data loss prevention tool).	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of BFS documentation and cybersecurity tool configurations. | GAO 26-108131

Specifically, BFS implemented security controls to (1) increase assurance that staff use system media consistent with agency policies, and (2) protect agency information at rest on agency laptops. In particular, the bureau implemented a data loss prevention solution to control system media use and encrypted the hard drives of agency laptops. By fully implementing these controls, BFS is better positioned to protect the confidentiality of its information systems.

However, BFS did not fully implement two controls to prevent the external transfer of agency information. Although the bureau implemented a data loss prevention tool on its laptops to prevent certain types of unencrypted information from being sent outside the bureau, the tool was not configured to detect all important transmissions. In particular, the bureau did not configure the tool to identify and block the transmission of (1) information related to payments made to certain individuals or organizations and (2) unencrypted sensitive information to other federal agencies.

BFS officials reported that their data loss prevention tools are primarily configured to identify instances of PII that are being sent to nonfederal

entities, rather than to other federal agencies, due to the high volume of payment information transmitted by employees each day. In addition, officials added that, although they review emails containing PII sent to nonfederal organizations, they do not review such emails sent to other agencies.

As a result of BFS's configurations, the bureau's data loss prevention tools did not identify or block the instance where employee B improperly transmitted United States Agency for International Development (USAID) payment information to two GSA DOGE team members (discussed in more detail later in this report). In addition, due to BFS's incomplete review of unencrypted emails with PII, the bureau identified this unauthorized use of agency systems after the email was sent and after employee B left the agency, according to officials.[40] Until BFS takes steps to either (1) configure its tool to block external transmission of unencrypted payment information, or (2) regularly review external transmission of unencrypted payment information, the bureau will have less assurance that its sensitive information is being appropriately protected and shared.

BFS Substantially Implemented Controls Associated with Monitoring System Usage

Of the three controls associated with the monitor system usage area, BFS fully implemented two controls and partially implemented the other, as shown in table 8.

Table 8: Bureau of the Fiscal Service (BFS) Efforts to Implement System Usage Monitoring Controls

Monitor System Usage area rating	Control	Control rating
Substantially implemented	Collect audit logs detailing user activity on agency systems.	●
	Conduct regular reviews of audit logs, as required by agency policies and procedures.	●
	Identify unauthorized use of agency systems through organization-defined methods and techniques.	◑

Legend: ●=Fully implemented ◑=Partially implemented ○=Not implemented

Source: GAO analysis of BFS documentation and cybersecurity tool configurations. | GAO 26-108131

Specifically, BFS implemented security controls to (1) collect audit logs detailing user activity performed on bureau laptops and in agency

[40]Specifically, officials identified the email during a forensic review of employee B's laptop after the individual left the agency.

systems, and (2) regularly monitor system usage for suspicious activity. For example, BFS established and implemented processes to review payment system audit logs for signs of malicious usage. By fully implementing these controls, BFS is better positioned to identify and remediate cybersecurity incidents.

However, the bureau did not fully implement the control related to identifying unauthorized use of agency systems. As previously mentioned, Treasury's data loss prevention tool did not identify or prevent employee B from sending USAID payment information, which included employee pay information, to GSA DOGE employees.

According to officials, the bureau identified this unauthorized use of agency systems after the email was sent. Specifically, officials identified the email during a forensic review of employee B's laptop after the individual left the agency. BFS officials explained that, in addition to their data loss prevention tool, they review daily reports of emails sent to external organizations containing PII. However, as previously discussed, those officials noted that the reports do not include emails sent to other federal agencies.

Treasury Office of General Counsel officials stated that reviewing all emails sent to other agencies with unencrypted payment information would be infeasible. However, it appears that such transmissions violate BFS's IT security rules and could be categorized as security incidents. In addition, BFS policy requires cybersecurity personnel to identify and follow-up on potential incidents. Until BFS takes steps to either (1) configure BFS's tool to block external transmission of unencrypted payment information, or (2) regularly review external transmission of unencrypted payment information, it will have less assurance it is identifying and addressing improper use of bureau systems.

The Treasury DOGE Team Employee with Access to BFS Payment Systems Did Not Always Follow IT Security Rules

NIST guidance recommends that agencies establish and make readily available to system users the rules that describe their responsibilities and expected behavior for securing information and IT systems.[41] Consistent with this guidance, BFS established IT system rules of behavior with requirements that all government and contractor personnel of the bureau are to follow—including security requirements. For example, BFS system users are to:

- not read, alter, insert, copy, or delete any data stored on BFS IT systems, except in accordance with assigned job responsibilities, guidance, policies, or regulations;
- not reveal any data processed or stored by BFS except as required by job responsibilities and/or prior written approval;
- not install or use unauthorized software on BFS equipment; and
- use only equipment and software provided by BFS or that has been approved for use by BFS's Chief Information Officer or designee to conduct BFS business.

However, Treasury DOGE team employee B did not always follow BFS's IT security rules. On January 30, 2025, employee B did not encrypt PII sent to another agency or obtain approval for sharing this information prior to sending it.[42] More specifically:

- Employee A requested that a bureau employee send them an Excel file which contained USAID payment information. Specifically, the file contained first and last names and payment amounts made by USAID between January 22 and January 24, 2025, for over 350 individuals, including USAID employees and private individuals.[43]

[41]NIST, Special Publication 800-53, *Revision 5: Security and Privacy Controls for Information Systems and Organizations* (Gaithersburg, Md.: September 2020).

[42]In addition to this event, employee B also attempted to connect removable media (i.e., a universal serial bus device) to their BFS laptop. The laptop's controls prevented the device from mounting (i.e., becoming accessible) to the laptop. Although the act of connecting removable media to a laptop is not a violation of BFS's rules of behavior, this media can be used to violate certain rules (e.g., install unauthorized software, copy BFS data without authorization). We attempted to contact Treasury DOGE team employee B to discuss this topic; we have not yet received a response to our request. We also do not have access to the removable media. As such, we were unable to determine whether this event was consistent with the bureau's IT security rules.

[43]BFS reported in a court filed declaration that this data was obtained from Treasury's Payment Information Repository.

- After receiving the file, bureau officials reported that employee A used their Treasury email account to send the file to employee B's BFS email account.
- On January 30, 2025, employee B used their BFS email account to send an unencrypted copy of the file to two members of the GSA DOGE team at their gsa.gov email addresses.[44]
- Treasury and BFS officials explained that they initially identified this event during a forensic examination of employee B's laptop (performed after this individual left the agency). Treasury subsequently disclosed the details of this event in March 2025, as part of declarations made in litigation.[45]

According to BFS officials, employee B did not obtain approval from the bureau to send this information outside the agency.[46] BFS officials also reported that they discussed the event with their Privacy Office and considered the disclosure of PII to be "low risk" because it did not contain other, more sensitive, information that could be associated with the specific individuals on the list (e.g., Social Security number, address, and date of birth). However, Treasury officials reported that they were unable to provide documentation demonstrating whether the Privacy Officer concurred with their determination because the conversation occurred over the phone and the director of the Office of Privacy, Transparency, and Records has since retired.

Employee B did not always follow the IT security rules because, as previously discussed, BFS did not implement all controls needed to ensure compliance with those rules. Until BFS fully implements all applicable selected controls for ensuring that users follow IT security rules, there is an increased risk that users will misunderstand what is

[44]Although the file was protected with a password, the password was included in the body of the email that transmitted the file. As such, any individual with access to the email message would be in possession of both the file and the password—thus effectively rendering the file unencrypted.

[45]As previously mentioned, lawsuits have been filed alleging possible violations of law that USDS and agency DOGE teams' access to federal records would create. Alliance for Retired Americans, et al. v. Bessent, et al. 1:25-cv-00313 (DDC 2025); State of New York, et al. v. Donald J. Trump, in his official capacity as President of the United States, et al. 1:25-cv-01144 (SDNY 2025).

[46]As previously discussed, we attempted to contact Treasury DOGE team employee B to discuss this topic; we have not yet received a response to our request.

expected of them to secure information and systems and information may not be adequately protected.

Conclusions

As part of their review of foreign aid payments and BFS payment processes, the Treasury DOGE team was granted broad access to information in three BFS payment systems during the scope of our audit. The integrity and security of these systems are critical to the nation's economy and to the security of sensitive personal and financial information.

However, BFS had not fully implemented all controls needed to ensure users with broad access to sensitive information are protecting it appropriately. Consequently, Treasury and BFS had less assurance that Treasury DOGE team members would follow the bureau's IT security rules.

The incomplete implementation of these controls led to an instance of a DOGE team member not appropriately securing information. In addition, the lack of such controls could enable serious incidents in the future involving improper action taken by others (e.g., systems administrators) with broad access to payment systems. Until Treasury and BFS fully establish and implement controls for overseeing users with broad access to payment systems, this important information will be at a greater risk of improper access, modification, disclosure, or misuse.

Recommendations for Executive Action

We are making six recommendations to BFS:

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. (Recommendation 1)

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. (Recommendation 2)

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. (Recommendation 3)

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. (Recommendation 4)

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 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). (Recommendation 5)

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. (Recommendation 6)

Agency Comments and Our Evaluation

We provided a draft of this report to BFS for review and comment. In its written comments, which are reproduced in appendix I, the bureau agreed with recommendations 2, 4, and 6 and described actions it planned to take to address them. In particular,

- With regard to recommendation 2, BFS stated that it will implement a process to ensure mandatory IT security and privacy training is completed prior to being granted access to BFS systems or data.
- In response to recommendation 4, the bureau said that it will update BFS provisioning and access procedures to confirm that access granted to payment systems is consistent with the level approved.
- Regarding recommendation 6, BFS stated that it will implement additional data loss prevention controls for sensitive data being emailed outside the bureau.

In addition, BFS did not state whether it agreed or disagreed with the remaining three recommendations. Specifically:

- In response to recommendation 1, the bureau stated that Treasury's Security Manual defined the minimum screening requirements that are required prior to accessing agency systems and that it will continue to adhere to those requirements. However, as discussed in

this report, although Treasury policy requires that every position within the agency be assigned a sensitivity designation based on the level of risk associated with the role, the policy does not define associated minimum sensitivity levels for the systems themselves, or what level of screening is required for an individual to be granted access to all data in federal payment systems. As such, we continue to believe that this recommendation is warranted.

- Regarding recommendation 3, BFS agreed with the importance of this control and explained that employee B was employed by Treasury—not BFS—and noted that it already has a process in place to ensure that bureau employees sign IT rules of behavior prior to receiving a laptop and being granted system access. In addition, BFS stated that Treasury has subsequently implemented a process to ensure that its employees sign BFS's IT rules of behavior document prior to being granted access to payment systems. However, Treasury and BFS have not yet provided documentation demonstrating that this process has been established or implemented. As such, we continue to believe that this recommendation is warranted.
- In response to recommendation 5, the bureau stated that it has exit procedures in place and that they are not applicable to Treasury employees—including employee B. However, the bureau's information security procedures do not distinguish between employees of the bureau and other agencies and offices within the department. In addition, BFS's procedures call for exit interviews to include a discussion of fiscal service information topics; Treasury may not be positioned to highlight these topics. As such, we continue to believe that this recommendation is appropriate and warranted.

BFS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional addressees and the Commissioner of the Bureau of the Fiscal Service. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Marisol Cruz Cain at cruzcainm@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix II.

//SIGNED//

Marisol Cruz Cain
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Elizabeth Warren
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Ron Wyden
Ranking Member
Committee on Finance
United States Senate

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Alex Padilla
Ranking Member
Committee on Rules and Administration
United States Senate

The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Richard Neal
Ranking Member
Committee on Ways and Means
House of Representatives

The Honorable Richard J. Durbin
United States Senate

The Honorable Christopher S. Murphy
United States Senate

The Honorable Don Beyer
House of Representatives

The Honorable Judy Chu
House of Representatives

The Honorable Danny Davis
House of Representatives

The Honorable Suzan DelBene
House of Representatives

The Honorable Dwight Evans
House of Representatives

The Honorable Steven Horsford
House of Representatives

The Honorable John Larson
House of Representatives

The Honorable Gwen Moore
House of Representatives

The Honorable Jimmy Panetta
House of Representatives

The Honorable Stacey Plaskett
House of Representatives

The Honorable Linda Sanchez
House of Representatives

The Honorable Brad Schneider
House of Representatives

The Honorable Terri Sewell
House of Representatives

The Honorable Thomas Suozzi
House of Representatives

The Honorable Lori Trahan
House of Representatives

The Honorable Mike Thompson
House of Representatives

Appendix I: Comments from the Bureau of the Fiscal Service

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
WASHINGTON, DC 20227

March 20, 2026

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Ms. Cruz Cain:

Thank you for the opportunity to review the Government Accountability Office's (GAO) draft report for engagement GAO-26-108131, entitled *Cybersecurity: Treasury Needs to Fully Implement Data Protection Controls* (Draft Report). The U.S. Department of the Treasury (Treasury) appreciates GAO's analysis and has provided technical comments under separate cover.

The Draft Report examines the Treasury DOGE team's access to Bureau of the Fiscal Service (BFS) payment systems. As the Draft Report acknowledges, BFS has undertaken significant efforts to implement cybersecurity controls over its payment systems, and it is continually working to improve its implementation and monitoring of cybersecurity controls. On January 20, 2025, Executive Order 14158 created the United States DOGE Service to modernize federal technology and software to maximize governmental efficiency and productivity, and it also required agency heads to establish within their respective agencies a "DOGE team." Treasury hired employees to serve as members of the Treasury DOGE team, and in late January 2025, the Treasury DOGE team began working with BFS to understand payment processes and identify opportunities to advance payment integrity and fraud reduction goals.

The Draft Report contains six recommendations. The first two recommendations respectively call for the Treasury Secretary to direct the Commissioner of the Fiscal Service to update BFS's policy to (1) define the minimum screening requirements for obtaining broad access to Treasury payment system data, and (2) require employees to take IT security and privacy training before obtaining broad access to Treasury payment systems. As to the first recommendation, we agree that minimum screening requirements are important. To that end, and as we have disclosed to GAO, Treasury's Security Manual defines the minimum screening requirements prior to access to Treasury's data systems. BFS will continue to adhere to those requirements. We agree with the second recommendation and will implement a process to ensure mandatory IT security and privacy training is completed prior to being granted access to BFS systems or data.

The third recommendation calls for the Treasury Secretary to direct the Commissioner of the Fiscal Service to establish and implement a process for verifying that employees sign BFS's IT security rules of behavior document prior to receiving broad access to payment systems. As detailed in the Draft Report, a Treasury employee – not a BFS employee – had accessed payment

systems without having signed this document.[1] We agree with GAO that this is an important control, and as the Draft Report acknowledges, BFS already has a process in place to ensure that its employees sign this document prior to receiving a laptop and being granted access. And, following the incident detailed in the Draft Report, Treasury confirmed to BFS that it had since implemented a similar process to ensure that its employees must sign BFS's Rules of Behavior document prior to being granted access to payment systems.

BFS agrees with the fourth recommendation, which calls for the Treasury Secretary to direct the Commissioner of the Fiscal Service to establish and implement a process for verifying that that broad access granted to payment systems is consistent with the level approved by the authorizing official. We will update BFS provisioning and access procedures to confirm that access granted to payment systems is consistent with the level approved.

The fifth recommendation calls for the Treasury Secretary to 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 cannot occur before individuals with access to payment systems leave the agency. We agree that it is important to have such procedures in place for departed employees, and indeed we already do. The Draft Report acknowledges that it describes a non-standard departure of a Treasury employee – not a BFS employee – for which BFS's exit processes were inapplicable.

BFS also agrees with the sixth recommendation, which calls for the Treasury Secretary to direct the Commissioner of the Fiscal Service to either configure BFS's data loss prevention tool to identify and block emails containing unencrypted payment information sent outside the agency, or to update BFS's process for reviewing emails with unencrypted payment information to include messages sent to other federal agencies. BFS will implement additional data loss prevention controls for sensitive data being emailed outside the Bureau.

BFS appreciates GAO's work assessing our data protection controls. Thank you again for the opportunity to review the Draft Report and for your consideration of our comments.

Sincerely,

Timothy E. Gribben
Commissioner

[1] As you know, BFS is a bureau within the Treasury Department. BFS does not manage the employment requirements of employees from its parent agency.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, cruzcainm@gao.gov

Staff Acknowledgments

In addition to the contact named above, John Bailey, Jillian Clouse, Michael Lebowitz, and Andrew Stavisky (among others), made key contributions to the report.