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.