U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

September 29, 2026 Accessible Version

Congressional Requesters

DOGE: Congress and the Public Lack Assurance That Systems and Data Were Protected at Multiple Agencies

The Department of Government Efficiency (DOGE) was created by Executive Order No. 14158 on January 20, 2025 with the mission of implementing the President's DOGE goals by modernizing federal technology and software to maximize governmental efficiency and productivity.[1] DOGE includes members of DOGE teams at federal agencies and the U.S. DOGE Service (USDS)—an organization within the Executive Office of the President that included a U.S. DOGE Service Temporary Organization.[2] This temporary organization was established to advance DOGE initiatives and under the terms of the executive order terminated on July 4, 2026. Since the order does not call for the termination of the broader USDS entity, it is possible that USDS and agency DOGE team personnel could continue work after the temporary organization's termination.

The executive order also called agency heads to take all necessary steps to ensure that USDS had full and prompt access to all unclassified agency records, software systems, and information technology (IT) systems. The breadth of this access has led to concerns by members of Congress and others that agency systems and their sensitive information and data may have been 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 systems contain vast amounts of personally identifiable information (PII),[4] thus making it imperative to protect the confidentiality, integrity,

[1]Exec. Order No. 14158, 90 Fed. Reg. 8,441, *Establishing and Implementing the President's "Department of Government Efficiency"* (Jan. 20, 2025). 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.

[2]Subsequent executive orders have assigned agency DOGE team staff with additional responsibilities, including those related to workforce optimization, deregulation, and contract and grant efficiency. Exec. Order 14210, *Implementing the President's "Department of Government Efficiency" Workforce Optimization Initiative*, 90 Fed. Reg. 9669 (Feb. 11, 2025); Exec. Order 14219, *Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative*, 90 Fed. Reg. 10583 (Feb. 19, 2025); and Exec. Order 14222, *Implementing the President's "Department of Government Efficiency" Cost Efficiency Initiative*, 90 Fed. Reg. 11095 (Feb. 26, 2025).

[3]For example, multiple lawsuits have been filed involving several federal agencies where concerns were raised about USDS or agency DOGE teams' access to federal data.

[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.

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]

Several departments and agencies—including the Departments of Education (Education) and Veterans Affairs (VA), as well as the Consumer Financial Protection Bureau (CFPB), National Oceanic and Atmospheric Administration (NOAA), Securities and Exchange Commission (SEC), and Small Business Administration (SBA)—have taken steps to establish agency DOGE teams. For example:

- In February 2025, Education sent correspondence to several Senators explaining that its DOGE team was reviewing department and Federal Student Aid contracts to identify possible efficiencies and that one employee was granted access to two internal systems to support this work.

- In February 2025, the Secretary of VA stated that the department had DOGE representatives who were reviewing contracts to ensure operations were efficient and resources were directed toward services for veterans.

We have previously reported on DOGE team access and whether systems and data were appropriately protected at the Bureau of the Fiscal Service (BFS) (a component of the Department of the Treasury) and the National Labor Relations Board (NLRB). Specifically:

- **BFS**. In April 2026, we reported that the Treasury DOGE team was granted broad access to information in three BFS payment systems between January 20, 2025, and April 11, 2025.[6] However, we found that BFS had not fully implemented applicable security and privacy controls needed to ensure users with broad access to sensitive information were protecting it appropriately. In addition, we reported that the incomplete implementation of these controls led to an instance of a DOGE team member not appropriately securing information. We made six recommendations to BFS to fully implement security and privacy controls with identified weaknesses. BFS agreed with three of the recommendations and did not state whether it agreed or disagreed with the other three. As of September 2026, BFS has not implemented the recommendations.

- **NLRB**. In April 2026, we reported that the board's DOGE team requested access to NLRB human resources systems, but we found no evidence that the DOGE team staff accessed any of these systems between April 16, 2025, and July 25, 2025.[7]

---

[5]In 2015, we expanded information security as a high risk area to include protecting the privacy of PII. In 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. 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]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. See GAO, *Department of Government Efficiency: Treasury Needs to Fully Implement Data Protection Controls*, GAO-26-108131 (Washington, D.C.: Apr. 28, 2026).

[7]GAO, *Department of Government Efficiency: National Labor Relations Board Detailees Did Not Access IT Systems Between April 16, 2025, and July 25, 2025*, GAO-26-108774 (Washington, D.C.: Apr. 28, 2026).

We were asked to review efforts to ensure that agency DOGE teams appropriately protected the systems and information they accessed at multiple agencies. Our objectives were to (1) describe the systems that DOGE teams at the six agencies in our review had been provided access and (2) evaluate the extent to which these agencies implemented controls to ensure that the DOGE team followed the agency's IT security rules and the DOGE team followed those rules.

This report focuses on the following six agencies: CFPB, Education, NOAA, SEC, SBA, and VA. See enclosure I for information on our scope and methodology.

We conducted this performance audit from March 2025 to September 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.

In summary,

- Four agencies—CFPB, Education, NOAA, and SEC—established DOGE teams and collectively reported that those teams had access to more than 23 systems used for various functions (e.g., managing contracts, grants, human resources, and finances). The extent and level of access that the DOGE team members had to the four reviewed agencies' systems could not be determined based on information the agencies provided.[8]

- Three of the six reviewed agencies—CFPB, Education, and SEC—provided us with limited documentation related to the extent to which they implemented controls for ensuring adherence to their IT security rules, and their DOGE team members followed the rules.

Four Reviewed Agencies Reported They Provided DOGE Teams Access to IT Systems, but the Extent and Level of Access Could Not Be Determined Based on Information Provided

Four agencies—CFPB, Education, NOAA, and SEC—established DOGE teams and collectively reported that those teams had access to more than 23 systems used for various functions, such as managing contracts, grants, human resources, and finances. The systems also contained sensitive information, including PII. The extent and level of access to the reviewed agencies' systems could not be determined because the agencies did not provide us with all the information we needed to confirm the access. Four agencies provided partial information and two agencies did not provide any information.

CFPB. On February 7, 2025, the CFPB Acting Director and a USDS Special Advisor, listed as the USDS Approver, executed an agreement to assign a DOGE team to CFPB for the purpose of carrying out projects for the furtherance of integrated, efficient, secure, and effective uses of IT.[9] That same day, the CFPB Acting Director sent an email with the Assignment Agreement to

[8]The other two reviewed agencies—SBA and VA—did not respond to requests for information regarding which systems DOGE team members had access to.

[9]The period of agreement paragraph of the document states that the terms and conditions described are effective from January 20, 2025, through July 4, 2026. On February 14, 2025, CFPB and USDS executed a separate terms and conditions agreement outlining the parameters for the assignment of up to five employees from USDS to CFPB.

one of the six team members being assigned, stating that the Acting Director was authorizing work to begin under the agreement. According to the Chief Operating Officer, six team members reported to the CFPB Acting Director and served as the core team.[10] The employees are referred to as CFPB team members A, B, C, D, E, and F for the remainder of this report. Table 1 lists the title and employment status of the six team members.

Table 1: Consumer Financial Protection Bureau (CFPB) Department of Government Efficiency (DOGE) Team Members' Titles and Employment Status

DOGE team employee	Title	Employment status
CFPB team member A	Special Government Employee	Detailed from the Office of Personnel Management
CFPB team member B	Senior Advisor for Technology and Delivery	Detailed from the Office of Personnel Management
CFPB team member C	No official title[a]	Detailed from the Office of Personnel Management
CFPB team member D	Senior Advisor	Detailed from the General Services Administration
CFPB team member E	Tech Support	Detailed from the General Services Administration
CFPB team member F	Senior Advisor	Initially detailed from United States DOGE Service Subsequently converted into a direct hire, according to the bureau's Chief Operating Officer

Source: GAO analysis of CFPB documentation. | GAO-26-108192

[a]CFPB officials told us that team member C's title was unknown. The individual this report refers to as CFPB team member C is also Commerce team member A, as described later in table 6.

According to CFPB officials, DOGE team members were given access to 19 systems used for administrative functions, but the bureau has not provided us with the information needed to confirm the extent and level of system access provided, as discussed in more detail later in this report. The staff did not have access to systems containing market monitoring information or supervision, enforcement, and fair lending data, according to the bureau.[11]

The following bullets and tables describe additional details on the 19 systems and levels of access based on (1) a written response provided by CFPB officials and (2) our review of a court filing that was affirmed by the bureau's Chief Information Officer.[12]

- CFPB provided DOGE team members with varying levels of access (e.g., full, view-only) to eight systems used by the bureau for several functions (e.g., managing contracts, controlling

The agreement also establishes the terms and conditions for reimbursable and nonreimbursable work by USDS for CFPB.

[10]The Chief Operating Officer made this statement as part of a declaration in a court filing. See *AFL-CIO et al. v, Dep't of Labor, et al,* 1:25-cv-339, ECF 31-3 (D.D.C. Feb. 13, 2025).

[11]According to CFPB, two DOGE team members—B and F—had sufficient permission rights to grant themselves and others access to these systems but did not do so. See *AFL-CIO et al. v, Dep't of Labor, et al.,* 1:25-cv-339, ECF No. 80- 5 (D.D.C. Apr. 18, 2025). The CFPB Chief Information Officer affirmed that this information was accurate.

[12]In a written response, CFPB identified the 19 systems and summarized the level of access provided to the team members or stated that the team members did not access the system (or only accessed the system on one occasion). We also relied on a court filing in which CFPB identified the access provided to each team member. See *AFL-CIO et al. v, Dep't of Labor, et al.,* 1:25-cv-339, ECF No. 80- 5 (D.D.C. Apr. 18, 2025). As previously mentioned, the CFPB Chief Information Officer affirmed that the information was accurate.

finances, and managing human resources). The bureau provided one team member—F—access to all eight systems and two other team members—B and E—access to one of the systems. See table 2 for a description of each system and the level of access provided to the three team members.

Table 2: Reported Department of Government Efficiency (DOGE) Team Access to Consumer Financial Protection Bureau (CFPB) Systems

System name	Description	Level of access	Team member(s) with access
Entra ID	A system to govern access for users in the Microsoft environment.	Full access	CFPB team members B, E, and F
Procurement Request Information System Management	A system for managing CFPB's procurement contracts.	Could view data Could not modify or terminate any contracts in the system	CFPB team member F
Data Insight	A system containing information on employees and the divisions in which they work.	Could view data Could not create, modify, or delete data	CFPB team member F
Invoice Processing Platform	A system to manage government invoicing that contains information regarding CFPB's finances.	Could view data Could not change any of the underlying data	CFPB team member F
oneARC	A system that contains information regarding CFPB's finances.	Could view data Could not change any of the underlying data	CFPB team member F
Oracle Business Intelligence	A system that contains information regarding CFPB's finances.	Could view data Could run reports Could not change any of the underlying data	CFPB team member F
HRConnect	A system serving CFPB's primary human resource function.	Could view, modify, and delete data	CFPB team member F
USAStaffing	A system that contains information related to employment vacancies and new hires.	Could view data Could not create, modify, or delete data	CFPB team member F

Source: GAO analysis of CFPB information and officials' statements in court filing. | GAO-26-108192

- CFPB provided access to five systems that were either never used by the DOGE team or the team logged-in only once to confirm access or receive a tutorial, according to bureau officials.[13] The bureau provided one team member—F—with access to three of the five systems, one team member—B—with access to two of the systems, and a third team member—E—access to one system. See table 3 for a list of these systems and which team members had access to them.

[13]The bureau did not identify the level of access that it provided to each team member.

Table 3: Systems for Which Consumer Financial Protection Bureau (CFPB) Department of Government Efficiency (DOGE) Team Members Were Provided Access but Generally Did Not Use, as Reported by CFPB

System name	Description	Team member(s) with access
Active Directory	A system directory used to store information about user accounts, providing services such as authentication and access control.	CFPB team members B and E
Physical Access Control	Unknown	CFPB team member B
Concur	Unknown	CFPB team member F
G-Invoicing	A system for agencies to manage intragovernmental buy/sell transactions.	CFPB team member F
WebTA	A system that provides time and attendance information tracking.	CFPB team member F

Source: GAO analysis of CFPB information and officials' statements in court filing. | GAO-26-108192

- CFPB provided one or more DOGE team members with access to the remaining six systems. For four systems, the bureau provided the levels of access but did not identify associated staff[14] and for two systems it did not identify the levels of access or associated team members.[15]

Education. Between January 23, 2025, and February 12, 2025, six individuals were onboarded as members of the Education DOGE team, according to department officials. During this period, the department entered into agreements with other agencies to detail four individuals to the team and onboarded the other two as employees. According to officials, the team was established to review the department's contracts, including the Office of Federal Student Aid's contracts, to identify possible efficiencies. The individuals are referred to as Education team members A, B, C, D, E, and F for the remainder of the report. Table 4 lists the title, appointment date, and employment status of the six team members.

[14]The four systems and reported access are as follows: (1) CFPB email system (administrator), (2) Integrated Talent Management (read, write, delete access), (3) Audit Monitoring System (read, write, delete access), and (4) Wagtail (full access).

[15]The two system names are Travel Services Applications and AKAMAI, according to CFPB.

Table 4: Education's Department of Government Efficiency (DOGE) Team Members' Titles, Appointment Dates, and Employment Status

DOGE team member	Title(s)	Appointment date	Employment status
Education team member A	Senior Advisor in the Office of the Secretary and Special Government Employee	February 12, 2025	Detailed from Office of Personnel Management and also a Special Government Employee while on duty at the Social Security Administration[a]
Education team member B	Senior Advisor in the Office of the Secretary	January 31, 2025	Schedule C appointment[b]
Education team member C	Special Government Employee	February 12, 2025	Detailed from the General Services Administration
Education team member D	Consultant in the Office of the Secretary	February 4, 2025	Consultant appointment[c]
Education team member E	Unknown	January 23, 2025	Detailed from United States DOGE Service (USDS)
Education team member F	Unknown	Unknown	Detailed from USDS

Source: GAO analysis of Education documentation. | GAO-26-108192

[a]A special government employee is defined, in part, as "an officer or employee of the executive or legislative branch…who is retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days, temporary duties either on a full-time or intermittent basis," under 18 U.S.C. §202(a). The term also includes employees and officers in certain miscellaneous positions who are deemed special government employees, without regard to the number of days of service. See, e.g., 42 U.S.C. § 12651b(e) (members of Board of Directors, Corporation for National and Community Service).

[b]5 CFR 213.3301(a). Positions filled under this authority are excepted from the competitive service and constitute Schedule C. Specifically, federal agencies are permitted to make appointments to positions that are of a confidential or policy-determining character.

[c]5 CFR 304.102(b). Under this authority, federal agencies are permitted to hire individuals to serve as consultants who can provide valuable and pertinent advice generally drawn from a high degree of broad administrative, professional, or technical knowledge or experience. Agencies may appoint consultants on a temporary basis (i.e., not to exceed 1 year) or an intermittent basis (i.e., without a regularly scheduled tour of duty).

According to department officials and a system access document, two of the six members on Education's DOGE team were granted access to its systems and IT network. However, the department has not provided us with the information needed to confirm the extent and level of system access, as discussed in more detail later in the report.

The following bullet points and table provide additional details regarding access to systems based on (1) a letter written to Senators from an Education official in its Office of Legislation and Congressional Affairs, (2) our review of a department official's declaration in a court filing, and (3) two system access requests provided by Education.[16]

- The department reportedly provided Education team member E with limited access to two systems in the Office of Federal Student Aid to support a review of contracts to identify possible efficiencies. Department officials stated that the team member did not have access to PII in one of the two systems; however, it is unclear whether the team member had

[16]In a letter written to Senators in February 2025, Education identified one DOGE team member's access to two systems and the status of the access. We also relied on a court filing in which Education discussed the access provided to each DOGE team member. See *Am. Fed. of Teachers, et al. v. Bessent, et al.*, 8:25-cv-430, ECF No. 62-1 (March 10, 2025).

access to PII in the other system. Team member E reportedly accessed one of the systems one time, but access to both systems has since been deactivated. See table 5 for a description of each system and the level of access provided to Education team member E.

Table 5: Education's Office of Federal Student Aid System Access Provided to Education Team Member E, as Reported by Education Officials

System name	Description	Level of access
Financial Management System	The primary source of financial data for the Office of Federal Student Aid's Title IV loan and grant programs; used to perform statistical analysis, produce financial reports, and maintain funds control.	Could access non-personally identifiable information (PII) data Could not create, modify, or delete data
Partner Connect	The primary portal that supports institutions of higher education that participate in federal student aid programs under Title IV of the Higher Education Act of 1965.	Could access data; unclear whether this included PII Could not create, modify, or delete data

Source: GAO analysis of Education information. | GAO-26-108192

- The department also provided Education team member E an administrative account with privileged user access to the "Ed Domain."[17] However, it is unclear what privileges this access included and what team member E was able to do with these privileges, as Education did not provide the information needed to validate this statement.

- Another member of the DOGE team requested access to the ED.gov system with the ability to publish and delete website content, but Education did not provide information needed to validate this access, including if the individual was ultimately granted access and with what privileges.[18]

NOAA. On February 3, 2025, and April 15, 2025, the Department of Commerce (Commerce) entered into formal agreements with the Office of Personnel Management (OPM) and General Services Administration (GSA) to detail three individuals to Commerce (one from OPM and two from GSA) to perform USDS work.[19] According to these agreements, the detailees' responsibilities included assessing the efficiency of agency operations and making recommendations, supporting the leadership team with the assessment and enhancement of internal processes, and identifying inefficiencies and areas for improvement. After being detailed to Commerce, these individuals were onboarded at NOAA to carry out this work.[20] The detailees

[17]According to the National Institute of Standards and Technology, a domain is environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

[18]Education did not provide the information needed to determine which of the DOGE team members in table 4 requested this access.

[19]According to the agreements Commerce entered with GSA on April 15, 2025, there was a prior oral agreement between the agencies for two of the three detailees. The agreements also stated that these two detailees from GSA began their assignment at Commerce on March 11, 2025, prior to the date of their signed agreements.

[20]Two documents we received from NOAA refer to a fourth individual being onboarded to the agency. However, NOAA indicated that it would not cooperate further with our review before we could follow-up to clarify the status of this individual and their system access.

are referred to as Commerce team members A, B, and C for the remainder of the report. Table 6 lists the title and employment status of the three team members.

Table 6: Titles and Employment Status of National Oceanic and Atmospheric Administration (NOAA) Detailees That Performed United States Department of Government Efficiency Service (USDS) Work

DOGE team member	Title	Employment status
Commerce team member A	No title provided[a]	Detailed from the Office of Personnel Management
Commerce team member B	Senior Advisor	Detailed from the General Services Administration
Commerce team member C	Senior Advisor	Detailed from the General Services Administration

Source: GAO analysis of NOAA documentation. | GAO-26-108192

[a]NOAA did not provide this information for Commerce team member A. This individual is also CFPB team member C, as described earlier in table 1.

According to NOAA officials and descriptions in agency documentation, the detailees that performed USDS work were given access to at least three systems and the agency's internal websites. However, NOAA has not provided us with the information needed to identify or confirm all system access granted to the three team members.

According to descriptions in NOAA documentation, Commerce team members B and C were provided access to at least three systems at the agency. NOAA officials stated that this access was for them to assist with contract and financial assistance reviews. (See table 7.) However, the agency did not provide us with the information needed to identify and confirm all access granted to these two individuals.

Table 7: Reported Detailee Access to National Oceanic and Atmospheric Administration Systems

System name	Description	Level of access	Team members with access
Procurement Request Information System Management	A system that automates the entire contract lifecycle, from planning and requisitions to vendor management and closeout.	Could access data; unclear whether this includes personally identifiable information (PII) Could not create, modify, or delete data	Commerce team members B and C
Electronic Research Administration	A cloud-based federal shared service managed by the National Institute of Health that supports the full federal grants lifecycle—from application to closeout—for both research and nonresearch grants.	Could access data; unclear whether this includes PII Could not create, modify, or delete data	Commerce team members B and C
Grants Enterprise Management Solution	A system that provides a centralized hub for Commerce's grant administration activities.	Could access data; unclear whether this includes PII Could not create, modify, or delete data	Commerce team members B and C

Source: GAO analysis of National Oceanic and Atmospheric Administration information. | GAO 26-108192

In addition, according to NOAA officials, the agency provided Commerce team member A with access to systems.[21] However, NOAA did not identify the systems or the associated levels of access provided.

Further, NOAA officials stated that they provided Commerce team member A with access that enabled them to create, modify, and delete content on the agency's internal websites. These websites included Google sites that provide employees with agency-related information and resources. According to NOAA officials, the purpose of the access request was for team member A to change or remove website content related to diversity, equity, and inclusion. However, NOAA did not provide the information needed to confirm these statements.

SEC. Between March 31, 2025, and April 25, 2025, two individuals—one detailee from GSA and one SEC employee—were onboarded as members of SEC's DOGE team, according to agency officials.[22] Specifically, on March 31, 2025, SEC onboarded a DOGE team member as a temporary transitional Schedule C appointment.[23] This team member was to serve as senior advisor in the Office of the Executive Staff, providing expert advice and counsel on complex issues. In addition, SEC entered into a formal agreement with GSA to detail one individual to SEC to assist with DOGE-related efforts, starting on April 25, 2025.[24] According to the agreement, the detailee's responsibilities included supporting leadership with enhancing internal processes, identifying areas for improvement, and ensuring administrative and programmatic functions align with best practices for effectiveness.

The DOGE team members are referred to as SEC team members A and B throughout the report. Table 8 lists the title and employment status of the two team members.

Table 8: Titles and Employment Status of the U.S. Securities and Exchange Commission (SEC) Department of Government Efficiency (DOGE) Team Members

DOGE team member	Title	Appointment date	Employment status
SEC team member A	Senior Advisor	March 31, 2025	Schedule C appointment
SEC team member B	Advisor	April 25, 2025	Detailed from General Services Administration

Source: GAO analysis of SEC documentation. | GAO-26-108192

[21]NOAA officials noted that the systems did not contain classified information.

[22]Before the two individuals were onboarded, SEC reported to the Executive Office of the President that it had designated five of its own employees as the agency's DOGE team, in accordance with EO 14158. However, the agency did not provide us with the information needed to validate this statement or provide further documentation to confirm these employees were members of its DOGE team.

[23]5 CFR 213.3302(a). Federal agencies may establish and make appointments to temporary, transitional positions of a confidential or policy-determining character. Positions filled under this authority are Schedule C positions, established to assist in the 1-year period following a change in administration, and time limited to 120 days, with one 120-day extension permittable.

[24]This agreement formalized a prior oral agreement, and was signed on April 23, 2025, by a Director in SEC's Office of Human Resources and on May 1, 2025, by a White House Liaison from GSA. The period of the detail assignment in the agreement was for April 25, 2025, to July 24, 2025.

According to agency officials, SEC gave team member A read-only access to PRISM—a procurement and contract management system.[25] However, although the agency provided emails and documentation related to access requests and approvals for this system, SEC has not provided us with all the information needed to validate these statements.

The remaining two agencies—SBA and VA—did not respond to requests for information needed to determine the access DOGE team members had to their systems. Specifically:

- **SBA**. The agency has not identified the systems the DOGE team was given access to or the permissions granted to each individual and has not provided the documentation needed to confirm access to each system.

- **VA**. Although department officials told us that contractors and employees serving as DOGE liaisons were given access to all systems which employees had standard access to,[26] VA has not provided us with a specific list of these systems, the level of access granted to them, or the information needed to confirm access to each system.[27]

The Extent to Which Selected Cybersecurity Controls for IT Security Rules Were Implemented or Followed at the Reviewed Agencies Could Not Be Determined Based on the Information Provided

NIST guidance recommends that agencies (1) implement security and privacy controls to help ensure that users with access to agency systems follow the agency's IT security rules and (2) establish and make readily available to users the rules that describe their responsibilities and expected behavior for following these rules.[28] Three of the six reviewed agencies—CFPB, Education, and SEC—provided us with limited documentation related to the extent to which DOGE team members followed IT security rules and agency controls for ensuring adherence to those rules.

Specifically, these agencies provided limited documentation related to the extent to which their DOGE teams (1) followed the IT security rules, (2) took training required for system access, (3) signed agreements required for system access, and (4) completed relevant background investigations.

- **Followed the IT security rules.** Two of the three agencies—CFPB and SEC—reported that there had not been any cybersecurity or privacy incidents pertaining to the DOGE team at

[25]SEC officials stated the agency provided both DOGE team members with the standard level of SEC network access that all personnel receive upon onboarding. Those officials added that the agency also discussed providing the DOGE team members with access to the financial payments system, Delphi. However, SEC officials stated that access to this system was never granted for either individual.

[26]VA also did not identify the contractors or employees serving as DOGE liaisons.

[27]An agency not included in this report provided evidence showing that a member of that agency's DOGE team had access to Veterans Health Administration's instance of the Electronic Official Personnel Folder (i.e., a system that provides agency staff with access to their employment records). However, we were not able to validate this access with VA or obtain more information on the extent and level of access.

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

their agencies.[29] However, these agencies did not provide us with an opportunity to observe their systems used to identify compliance with their IT security rules, such as those used to (1) track cybersecurity and privacy incidents and (2) log user activity. Consequently, Congress and the public lack information needed to confirm if DOGE team members followed the IT rules of behavior they agreed to at these agencies.

- **Took training required for system access.** Two of the three agencies—CFPB and SEC—provided limited documentation related to this control.[30] With respect to CFPB, the bureau provided documentation demonstrating that six DOGE team members received a privacy briefing and four members completed security training. Such training is important for ensuring that system users are fully informed of relevant cyber and privacy risks associated with system use and their responsibilities for addressing those risks. However, CFPB did not respond to our request for documentation showing that all team members completed the security training.

  Regarding SEC, the two DOGE team members completed the agency's initial privacy and cyber awareness training. However, SEC did not respond to our requests for information on whether additional training was required to access the system used to manage contracts. As a result, Congress and the public lack information on whether DOGE team members at CFPB and SEC were aware of their responsibilities for addressing cyber and privacy risks.

- **Signed agreements required for system access.** Two agencies—CFPB and Education—provided limited documentation relevant to this control.[31] CFPB provided agreements signed by five of the six team members indicating that they would not knowingly (1) take any measures that create cybersecurity risks or (2) take any measures that could undermine CFPB's responsibilities under governing statutes, regulations, or directives. The bureau also provided documentation showing that four of the six team members reviewed the acceptable use policy. However, CFPB did not respond to our request for documentation showing that all DOGE team members acknowledged the bureau's policy on acceptable use of its IT resources and agreed to abide by those rules, consistent with the bureau's information security policy. Acknowledgment of these documents is key to holding system users accountable for not following IT security rules.

  Education provided IT system rules of behavior documents signed by five of the six team members. The department also provided privileged user rules of behavior documents signed by all six reported DOGE team members and an ED.gov rules of behavior document signed by the one DOGE team member with requested access. However, Education did not respond to our repeated requests for IT system rules of behavior signed by the remaining team member. Consequently, Congress and the public lack assurance that CFPB and Education were positioned to hold DOGE team members accountable for not following these rules.

- **Completed background investigations**. One agency—SEC—provided documentation demonstrating that a background check was underway for one team member and had been

[29]Education did not respond to this request for information.

[30]Education did not respond to this request for information.

[31]SEC did not respond to this request for information.

conducted for another in 2017.[32] These investigations are important for ensuring that system users meet requirements for accessing sensitive information. However, the agency did not respond to our request to confirm that the 2017 investigation was favorably adjudicated. Therefore, Congress and the public lack assurance that this team member met relevant security requirements.

In addition, one of the three agencies—CFPB—stated that it implemented several other controls. In particular, bureau officials stated that they (1) ensured DOGE team staff were granted access to systems based on policies and procedures[33] and (2) collected audit logs detailing user activity. However, CFPB did not respond to our requests for information needed to corroborate the implementation of these controls.

The agencies provided varying rationales for not providing the requested information needed to fully answer this objective. Specifically:

- **CFPB**. In January 2026 and April 2026, CFPB declined to provide information that we had requested, asserting, among other things, that the information was redundant of information provided to us, was unnecessary, or that providing it would unnecessarily disrupt bureau operations.

- **Education**. In May 2026, an official in the Executive Secretariat stated that the department could not send us any further information as there is ongoing litigation that is intertwined with the subject matter under review. The official also stated that the department had concerns with sending us PII for the DOGE individuals without a guarantee of confidentiality.

- **SEC**. In a June 2026 letter, SEC's General Counsel stated that the agency would decline to further participate in our review as it believes we only have the authority to perform work if it stems from the request of a congressional committee (or the committee chair) and that certain agency information was protected from disclosure to GAO.

The remaining three reviewed agencies—NOAA, SBA, and VA—did not respond to our requests for information needed to determine agency controls for ensuring adherence to the IT security rules and the extent to which DOGE team members followed those rules. Specifically:

- **SBA**. We requested this information on multiple occasions between May 2025 and February 2026. As of September 2026, SBA has not explained why it has not addressed these requests.

- **VA**. We requested this information on multiple occasions between April 2025 and May 2026. In June 2026, the department confirmed that it would not be addressing our requests or providing us with a reason for not doing so.

- **NOAA**. In a February 2026 letter, NOAA's General Counsel stated that the agency would not participate in the review due to the agency's view that we do not have the necessary

[32]CFPB and Education did not provide documentation related to this control.

[33]CFPB also added that the Chief Information Officer conducted a risk assessment prior to arranging access for DOGE staff.

statutory authority to conduct an audit at the request of a ranking member of a congressional committee.

Without the ability to examine the requested information, Congress and the public lack assurance that these agencies implemented controls needed to ensure DOGE team members appropriately secured information.

GAO has the authority to carry out this work at each of these agencies in support of Congress and to obtain the requested information. In particular, GAO has ample statutory authority to conduct audit work on the initiative of the Comptroller General under 31 U.S.C. § 717(b)(1), despite views expressed by SEC and NOAA. This authority has long supported work conducted in response to requests from ranking members of congressional committees as recognized over decades by Congress and numerous administrations.

In addition, the concerns raised by CFPB, Education and SEC—including pending litigation and the nature of the information—do not alter or diminish GAO's statutory right to the requested information.[34] Indeed, GAO has routinely obtained this kind of information from these and other agencies in the past on other cybersecurity audits. Moreover, GAO has routinely protected this type of information, maintaining the same level of confidentiality as is required of the head of the agency. GAO has a long history of reaching successful accommodations with agencies, including CFPB, Education and SEC, to address concerns about protecting their sensitive information and to obtain the information necessary to complete our audit work.

Agency Comments and Our Evaluation

We provided a draft of this report to the six agencies for review and comment. Education, NOAA, SBA, SEC, and VA stated that they did not have any comments. In written comments, reproduced in enclosure II, CFPB expressed concerns with the accuracy of the report, stating that it is misleading and inaccurately characterizes the information the bureau provided as well as the timely and prompt attention CFPB provided to this review.

In particular, the bureau highlighted the concerns raised in the bullets below. As discussed in more detail in those bullets, we conducted this work in an objective, independent, and nonpartisan manner and stand by the accuracy of the facts presented in our report.

- The bureau stated that our report did not make any effort at neutral reporting and reads as if there was an inherently malicious intent among DOGE staff and their hosting agencies. In support of this statement, CFPB wrote that our report states that DOGE had access to systems and that "many of these systems contain vast amounts of … PII." According to the bureau, this statement implies that DOGE staff were searching through the public's personally identifiable information when the systems DOGE accessed at CFPB had only limited information regarding bureau staff.

  The bureau is mischaracterizing our report. Although our report does use the phrase "many of these systems contain vast amounts of . . . PII", it does so in reference to all unclassified systems owned by all federal agencies.[35] This language can be found near the beginning of the report where we explain the importance of protecting the confidentiality, integrity, and

[34]See 31 U.S.C. § 716.

[35]See this report, page 1.

availability of these systems and their data. In addition, CFPB's written response acknowledged that our report describes the systems that DOGE accessed at the bureau, including the types of data that those systems process and maintain. We accurately reported CFPB-provided data on the systems that DOGE accessed in accordance with *Government Auditing Standards*.[36]

- According to CFPB, the bureau-provided statements indicating that DOGE staff did not misuse agency systems were not accounted for in the report. This is not a fully accurate characterization. Our draft report noted that "CFPB … reported that there had not been any cybersecurity or privacy incidents pertaining to the DOGE team at their agencies."[37] We updated our report to also include CFPB's more detailed statements related to conducting a risk assessment prior to granting access, granting access in accordance with bureau policies, and monitoring that access through system logs. However, as our report states, CFPB did not provide us with an opportunity to corroborate these statements by observing its systems, such as those used to (1) track cybersecurity and privacy incidents and (2) log user activity. *Government Auditing Standards* call for us to corroborate testimonial evidence with other evidence (e.g., observation) where possible.[38] We regularly observe systems when reviewing IT and cybersecurity topics at federal agencies.

- The bureau stated that it provided us with access level information on systems used by the DOGE team and that we continued to demand increasing amounts of redundant or burdensome data. CFPB added that the bureau offered to provide more information if we would articulate a detailed justification but stated that we declined to do so and mistakenly concluded that the extent and level of DOGE team member access to CFPB systems could not be determined.

  This is not an accurate summary of our correspondence with CFPB on this topic. On January 26, 2026, CFPB provided a written summary of the systems that DOGE team members accessed at CFPB and the highest level of access provided to team members for some, but not all, systems. On February 5, 2026, we requested screenshots of user account details and copies of user activity logs.[39] In doing so, we explained that (1) CFPB had not yet identified the access provided to each team member and (2) that *Government Auditing Standards* call for us to corroborate testimonial evidence with other evidence (e.g., observation) where possible.[40]

---

[36]GAO, *Government Auditing Standards: 2018 Revision (Technical Update April 2021)*, GAO-21-368G (Washington, D.C.: April 2021).

[37]See this report, pages 11-12.

[38]GAO-21-368G. In particular, paragraph 8.104 explains that evidence obtained through auditors' direct physical examination, observation, computation, and inspection is generally more reliable than evidence obtained indirectly (e.g., through interviews or written responses). In addition, paragraph 8.94 of these standards calls for auditors to evaluate the objectivity, credibility, and reliability of testimonial evidence. For example, paragraph 8.105 explains that documentary evidence may be used to help verify, support, or challenge testimonial evidence.

[39]On December 3, 2025, we requested meetings for us to observe these account details and user activity logs. On February 5, 2026, we modified this request to instead ask for documentation as temporary accommodation in light of CFPB's concerns regarding the burden that these meetings would place on the bureau.

[40]GAO-21-368G.

On February 17, 2026, a CFPB Assistant General Counsel stated that the bureau declined to provide more information. That official explained that CFPB provided (1) two separate submissions containing pertinent and responsive information to our requests for information and (2) a carefully crafted response that balanced the bureau's concerns while respecting our legal authority to examine executive branch operations. However, the bureau did not provide us with the information needed to confirm the extent and level of system access (e.g., meetings to observe system accounts and logs), as previously discussed.

- According to CFPB, our requests for more information demonstrate a fundamental lack of understanding of federal executive personnel management. CFPB explained that the DOGE staff members at the bureau initiated their work as time-limited detailees from their home agencies and that most of their training and onboarding were managed by their home agencies. The bureau added that other bureau-specific training may not have been required due to the extremely short duration of these detail assignments. According to CFPB, the bureau nonetheless provided us with information related to training completed by DOGE staff, but we were unsatisfied and sought to continue to request further information imposing an undue burden on its operations.

  CFPB's comments are not consistent with the bureau's policies and guidance on taking training, signing security agreements, and completing background agreements.

  - With respect to training, CFPB's policy requires data users (i.e., individuals who have access to bureau information resources, including employees and contractors) to complete information security and privacy training prior to accessing data.[41] As previously discussed, the bureau provided documentation demonstrating that six DOGE team members received a privacy briefing and four members completed security training. However, CFPB did not respond to our request for documentation showing that all team members completed the security training.

  - Regarding security agreements, CFPB's Information Security Standards Policy 800-53 Standard Operating Guidance calls for individuals requiring access to bureau systems to acknowledge that they have read, understand, and agree to abide by the IT rules before CFPB authorizes system access.[42] As previously discussed, CFPB provided documentation showing that four of the six team members reviewed the acceptable use policy. However, CFPB did not respond to our request for documentation showing that all DOGE team members acknowledged the bureau's policy on acceptable use of its IT resources and agreed to abide by those rules.

  - With regard to background investigations, CFPB's Information Security Standards Policy 800-53 Standard Operating Guidance calls for the bureau to screen individuals prior to authorizing access to systems.[43] In a written response, CFPB stated that personnel investigations were verified where possible based on the Visit Authorization Requests submitted by the DOGE staff home agencies. However, CFPB did not

[41]CFPB, Policy on Data Access, COO-OCDO-01-2019 (Sept. 23, 2019). Although this policy allows for exceptions to be approved by the Chief Data Officer and Data Governance Board, the bureau did not provide us with any such exceptions for the members of the DOGE team.

[42]The guidance does not make any exceptions for time-limited detailees.

[43]The guidance does not make any exceptions for time-limited detailees.

respond to our request for documentation demonstrating that the bureau verified the investigation status.

In addition, CFPB requested that we reproduce a letter that the bureau sent us in April 2026 in response to a statement of facts document that we sent to the bureau in March 2026.[44] In the bureau's letter, reproduced in enclosure III, it expressed concerns with our statement of facts document, explaining that it contained gross inaccuracies and misleading information.

On May 18, 2026, we responded by explaining that although we disagreed with several points in the letter, we expressed our desire to engage with CFPB officials to address the comments in a complete and constructive manner. For those reasons, we stated that we believed that an exit conference would be the appropriate forum to work through and potentially address the concerns (e.g., making corrections and incorporating any additional information).[45] On June 3, 2026, a CFPB senior counsel stated that the bureau declined our offer of an exit conference. Nevertheless, we incorporated the comments in CFPB's April 2026 letter into our report as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretaries of Commerce, Education, and Veterans Affairs; the Acting Director of the Consumer Financial Protection Bureau, the Chairman of the SEC, and the Administrator of SBA. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Nick Marinos at marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. Other key contributors to this report include Marisol Cruz Cain (Director), Jillian Clouse, Michael Lebowitz, and Andrew Stavisky.

//SIGNED//

Nick Marinos
Managing Director,
Information Technology and Cybersecurity

Enclosure I
Enclosure II:

[44]Consistent with our agency protocols, we use statement of facts to confirm that the critical facts and key information used to formulate our analyses and findings are current, correct, and complete.

[45]An exit conference is a meeting with agency officials and GAO that gives both organizations an opportunity to reach a mutual understanding of relevant facts, statements, and other information.

List of Requesters

The Honorable Elizabeth Warren
Ranking Member
Committee on Banking, Housing, and Urban Affairs
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 C. “Bobby” Scott
Ranking Member
Committee on Education and Workforce
House of Representatives

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Bill Foster
Ranking Member
Subcommittee on Financial Institutions
Committee on Financial Services
House of Representatives

The Honorable Al Green
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Financial Services
House of Representatives

The Honorable Jared Huffman
Ranking Member
Committee on Natural Resources
House of Representatives

The Honorable Maxine Dexter
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Natural Resources
House of Representatives

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

The Honorable Mark Takano
Ranking Member
Committee on Veterans' Affairs
House of Representatives

The Honorable Nydia M. Velázquez
Ranking Member
Small Business Committee
House of Representatives

The Honorable Richard J. Durbin
United States Senate

The Honorable Andy Kim
United States Senate

The Honorable Christopher S. Murphy
United States Senate

The Honorable Mark R. Warner
United States Senate

The Honorable Lori Trahan
House of Representatives

Enclosure I: Objectives, Scope, and Methodology

Our objectives were to (1) describe the systems that DOGE (Department of Government Efficiency) teams at the six agencies in our review had been provided access and (2) evaluate the extent to which these agencies implemented controls to ensure that the DOGE team followed the agency's information technology (IT) security rules and that the DOGE team followed those rules.

This report focuses on six agencies: the Departments of Education (Education) and Veterans Affairs (VA), as well as the Consumer Financial Protection Bureau (CFPB), National Oceanic and Atmospheric Administration (NOAA), Securities and Exchange Commission (SEC), and Small Business Administration (SBA).

To address our first objective, we requested documentation describing the (1) systems that members of the DOGE teams at reviewed agencies had received access to and (2) level of access that members were approved to receive for each system. In response to our request, four agencies—CFPB, Education, NOAA, and SEC—provided information that fully or partially addressed these requests. The remaining two agencies—VA and SBA—have not responded to these requests, as of September 2026.

For the four agencies that fully or partially addressed our initial requests, we then asked to observe the systems for which access was provided to the DOGE teams. Specifically, we requested to observe the roles for each account, privileges assigned to the roles, and the logs identifying actions taken by each account. As of September 2026, the four agencies have not responded to these requests.

With respect to our second objective, we developed an evaluation framework (i.e., sets of selected areas and practices) and compared it to agency efforts to implement security and privacy controls for ensuring that the DOGE team followed 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* and selected 15 controls and four associated control areas related to managing privileged user access to systems and ensuring that sensitive information is protected (see table 9).

Table 9: 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 at alternate work sites and assess the effectiveness of controls at alternate work sites.
	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-26-108192

For the four agencies that fully or partially addressed our initial requests to describe systems that members of the DOGE teams had received access, we requested (1) documentation describing relevant policies and procedures and (2) to observe system configurations and logs. Three of these agencies—CFPB, Education, and SEC—provided us with documentation related to several controls, such as ensuring that staff took training required for system access and signed access agreements required for system access. However, the agencies did not respond to our requests for additional documentation needed to determine the extent to which the controls were implemented. In addition, the fourth agency—NOAA—has not responded to our requests for this information as of September 2026.

The remaining two agencies—SBA and VA—did not respond to our request for information on the systems that the members of the DOGE teams received access. As such, we did not receive the information that we needed to inform a request to observe system configurations and logs.

In addition, we requested (1) agency policies and procedures regarding IT security rules and (2) reports of any security or privacy incidents. Three agencies—CFPB, Education, and SEC—fully

or partially responded to these requests and the remaining three agencies have not responded to them, as of September 2026.

For the three agencies that fully or partially responded to our requests, we then asked to observe agency systems used to (1) track cybersecurity and privacy incidents and (2) log user activity. As of September 2026, the agencies have not responded to these requests.

Enclosure II: Comments from Consumer Financial Protection Bureau

1700 G Street, N.W., Washington, DC 20552

September 4, 2026

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

The Consumer Financial Protection Bureau ("CFPB" or "Bureau") writes this letter to comment on the Government Accountability Office's ("GAO") draft report ("Report") in the engagement 108912 ("USDS Data Protection"). This engagement and the Report discuss the activities of Department of Government Efficiency ("DOGE") staff assigned to the Bureau. The Bureau previously shared its concerns with GAO in our April 2, 2026 letter, which is included as an attachment to this letter. We request GAO include that prior correspondence as part of our formal comment letter to fully inform the congressional requesters of the Bureau's position and its efforts to respond to this intrusive engagement.

GAO's Report is misleading and inaccurately characterizes the information that CFPB provided as well as the timely and prompt attention the Bureau devoted to this engagement. Below are just some of the Bureau's concerns with GAO's Report in addition to those we have previously raised.

First, GAO makes no effort at neutral reporting. The Report reads as if there was an inherently malicious intent among DOGE staff and their hosting agencies. For example, the Report states that DOGE had access to systems and that "many of these systems contain vast amounts of personally indefinable information (PII)." Report pp. 1-2. The implication is that DOGE staff were rifling through the public's information even though GAO later noted, to less dramatic effect, that CFPB confirmed that DOGE staff "did not have access to systems containing market monitoring information or supervision, enforcement, and fair lending data." Report p. 5. In addition, the systems DOGE accessed at CFPB had only limited personal information regarding Bureau staff, i.e., HR data. See Report p. 6. Indeed, DOGE staff access to Bureau operational data – contracts, finances, employment data, etc. is mundane information often subject to Freedom of Information Act ("FOIA") requests. Of course, that is not as sensational to highlight in the Report.

Second, the Bureau responded to all GAO inquiries regarding this engagement. CFPB made an official attestation that no DOGE staff improperly accessed or misused any CFPB systems. These are the official responses provided to GAO that are completely unaccounted for in the Report:

> DOGE staff were granted access to systems in accordance with Bureau policies.

> The Chief Information Officer (CIO) conducted a risk assessment prior to arranging access for DOGE staff . . . . Access to Bureau systems was provided to DOGE staff as required for them to perform their work as CFPB detailees. All DOGE access to CFPB systems was monitored and captured through system logs.
>
> The Bureau has no reports or awareness of any potential or actual misuse of agency systems [to]date by DOGE staff.

CFPB Response to GAO dated January 27, 2026. Yet, GAO concluded that these official statements are useless and not relevant.

Moreover, in connection with those attestations, the Bureau did provide GAO with access level information on systems used by the DOGE team. This is self-evident by Report's Table on p. 6. Although the information CFPB provided was more than sufficient, GAO continued to demand increasing amounts of redundant or burdensome data. CFPB offered to provide more information if GAO would articulate a detailed justification, but GAO declined to supply such a justification. GAO then misleadingly concludes in the report that "[t]he extent and level of access that the DOGE team members had to the four reviewed agencies' [including CFPB] systems could not be determined based on information the agencies provided." Report p. 3.

Third, GAO's obsession with ever greater information demands on the Bureau regarding DOGE staff members is baffling and demonstrates a fundamental lack of understanding of federal executive personnel management. The DOGE staff members at the Bureau initiated their work as time-limited detailees from their home agencies. Most of their training and on-boarding personnel policies were managed by their home agencies as is the normal course of executive branch operations. Other Bureau specific training may not have been required due to the extremely short duration of these detail assignments. Despite this, the Bureau provided GAO with information concerning trainings completed by DOGE staff but GAO was unsatisfied and sought to continue its fishing expedition, imposing an undue burden on operations of an executive branch agency.

Regards,

Victoria Dorfman
General Counsel
Consumer Financial Protection Bureau

2

GAO Note 1: As discussed in more detail earlier in this report, we conducted this work in an objective, independent, and nonpartisan manner and stand by the accuracy of the facts presented in our report.

GAO Note 2: The is mischaracterizing our report. Although our report does use the phrase "many of these systems contain vast amounts of . . . PII", it does so near the beginning of the report where we explain the importance of protecting unclassified systems owned by all federal agencies.

GAO Note 3: This is not a fully accurate characterization. Our draft report indeed noted "CFPB … reported that there had not been any cybersecurity or privacy incidents pertaining to the DOGE team." Nonetheless, we updated the report to include the more detailed statements.

GAO Note 4: This is not an accurate summary of our correspondence with CFPB on this topic. On February 5, 2026, we explained that Government Auditing Standards call for us to corroborate testimonial evidence with other evidence (e.g., observation) where possible. On February 17, 2026, CFPB declined to provide more information.

GAO Note 5: CFPB's comments are not consistent with the bureau's policies and guidance on taking training, signing security agreements, and completing background agreements. See the "Agency Comments and Our Evaluation" section of this report for additional details.

Accessible Text for Enclosure II: Comments from Consumer Financial Protection Bureau

Consumer Financial Protection Bureau
1700 G Street, N.W., Washington, DC 20552

September 4, 2026

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

The Consumer Financial Protection Bureau ("CFPB" or "Bureau") writes this letter to comment on the Government Accountability Office's ("GAO") draft report ("Report") in the engagement 108912 ("USDS Data Protection"). This engagement and the Report discuss the activities of Department of Government Efficiency ("DOGE") staff assigned to the Bureau. The Bureau previously shared its concerns with GAO in our April 2, 2026 letter, which is included as an attachment to this letter. We request GAO include that prior correspondence as part of our formal comment letter to fully inform the congressional requesters of the Bureau's position and its efforts to respond to this intrusive engagement.

GAO's Report is misleading and inaccurately characterizes the information that CFPB provided as well as the timely and prompt attention the Bureau devoted to this engagement. Below are just some of the Bureau's concerns with GAO's Report in addition to those we have previously raised.

First, GAO makes no effort at neutral reporting. The Report reads as if there was an inherently malicious intent among DOGE staff and their hosting agencies. For example, the Report states that DOGE had access to systems and that "many of these systems contain vast amounts of personally identifiable information (PII)." Report pp. 1–2. The implication is that DOGE staff were rifling through the public's information even though GAO later noted, to less dramatic effect, that CFPB confirmed that DOGE staff "did not have access to systems containing market monitoring, information or supervision, enforcement, and fair lending data." Report p. 5. In addition, the systems DOGE accessed at CFPB had only limited personal information regarding Bureau staff, not PII. Id., see Report p. 6. Indeed, DOGE staff access to Bureau operational data — consumer complaint data, etc. — is mundane information often subject to Freedom of Information Act ("FOIA") requests. Of course, that is not as sensational to highlight in the Report.

Second, the Bureau responded to all GAO inquiries regarding this engagement. CFPB made an official assertion that no DOGE staff improperly accessed or misused any CFPB systems. These were the official responses provided to GAO that are completely unaccounted for in the Report:

> DOGE staff were granted access to systems in accordance with Bureau policies.

> The Chief Information Officer (CIO) conducted a risk assessment prior to arranging access for DOGE staff… Access to Bureau systems was provided to DOGE staff as required for them to perform their work as CFPB detailees. All DOGE access to CFPB systems was monitored and captured through system logs.
>
> The Bureau has no reports or awareness of any potential or actual misuse of agency systems [to date] by DOGE staff.

CFPB Response to GAO dated January 27, 2026. Yet, GAO concluded that these official statements are useless and not relevant.

Moreover, in connection with those attestations, the Bureau did provide GAO with access level information on systems used by the DOGE team. This is self-evident by Report's Table on p. 6. Although the information CFPB provided was more than sufficient, GAO continued to demand increasing amounts of redundant or burdensome data. CFPB offered to provide more information if GAO would articulate a detailed justification, but GAO declined to supply such a justification. GAO then misleadingly concludes in the report that "[t]he extent and level of access that the DOGE team members had to the four reviewed agencies [including CFPB] systems could not be determined based on information the agencies provided." Report p. 3.

Third, GAO's obsession with ever greater information demands on the Bureau regarding DOGE staff members' roles is baffling and demonstrates a fundamental lack of understanding of federal executive personnel management. The DOGE staff members at the Bureau initiated their work as time-limited detailees from their home agencies. Most of their training and on-boarding personnel policies were managed by their home agencies as is the normal course of executive branch operations. Other Bureau-specific training may not have been required due to the extremely short duration of these detail assignments. Despite this, the Bureau provided GAO with information on training assignments completed by DOGE staff but GAO was unsatisfied and sought to continue its fishing expedition, imposing an undue burden on operations of an executive branch agency.

Regards,
Victoria Dorfman
General Counsel
Consumer Financial Protection Bureau

consumerfinance.gov

Enclosure III: Comments from Consumer Financial Protection Bureau

1700 G Street, N.W., Washington, DC 20552

April 2 2026

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

The Consumer Financial Protection Bureau ("CFPB" or "Bureau") writes this letter to comment on the Government Accountability Office's ("GAO") draft statement of facts ("SOF") in the engagement 108912 ("USDS Data Protection"). This engagement and the SOF concern the activities of Department of Government Efficiency ("DOGE") staff assigned to the Bureau. After reviewing the SOF, the Bureau must formally notify you of our significant concerns regarding GAO's gross inaccuracies and misleading characterizations. To be blunt, the SOF is incoherent and demonstrates no effort to report on the information provided by CFPB. Rather, GAO has cobbled together a hodgepodge of misleading, confusing statements and then blames its muddled reporting on the Bureau's alleged unwillingness to provide information.

GAO's stated objectives for this engagement were to "(1) describe the CFPB systems that the bureau's DOGE team had been provided access to and how the team planned to use those systems, (2) evaluate the extent to which CFPB 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." For over a year, CFPB has sought to accommodate GAO's requests while protecting the CFPB's legitimate interests, including its ability to defend a lawsuit, *AFL-CIO v. Department of Labor, et al, 1:25-cv-00339*, that was substantially related to the questions in this incredibly broad engagement. Despite these concerns, the CFPB quickly provided responsive materials that would address GAO's stated objectives without impairing this litigation. Not satisfied with the Bureau's reasonable approach, GAO repeatedly asked for the same information during the litigation.[1] After the litigation was resolved, GAO reengaged with the Bureau and CFPB provided a second tranche of responsive materials and information, comprehensively responding to GAO. The CFPB has provided information necessary to address all of GAO's stated objectives, including providing information to identify the level of access for each system accessed by a DOGE team member, non-disclosure agreements, and information about the training completed by DOGE team members. The CFPB also informed GAO that it has no reports or awareness of any instances of actual or potential misuse of agency systems by DOGE team staff, and that at all times their access to CFPB systems was monitored and captured through system logs. Your agency, however, was

[1] CFPB acknowledges that GAO attempted to find "accommodations" with the Bureau during the litigation, but fundamentally there was never a true appreciation or acknowledgment by GAO that the Bureau was constrained the underlying litigation, and so GAO was unyielding in its demands.

never satisfied with CFPB's responses and sought additional materials to verify information already provided by the Bureau. Now, GAO has drafted a dubious SOF that attempts to falsely cast blame on the Bureau for not participating in this engagement. I'd like to highlight just a few of the many issues with GAO's approach to this engagement and its resulting SOF.

First, the Bureau has consistently engaged with GAO in good faith to provide information for this engagement. The Bureau provided documentation on May 29, 2025, again on January 28, 2026 and additional clarification and information on March 6, 2026. The Bureau has also repeatedly, both formally and informally, shared its concerns regarding the breadth and intrusiveness of this engagement. In contrast, GAO only made minimal efforts to constrain its inquiry to a reasonable scope. Nonetheless, the Bureau provided GAO with substantive responses and documentation. In its SOF, GAO provides no context for the Bureau's efforts and responsiveness to GAO. Rather, GAO creates a false narrative of CFPB somehow being obstructionist:

> "In February 2026, CFPB declined to provide [] information or confirm whether such information exists" SOF p.10 n.23.
>
> "We [GAO] requested this information multiple occasions . . . . the bureau declined to provide more information." SOF p.13.
>
> We [GAO] requested this information multiple occasions . . . . the bureau declined to provide more information. SOF p.14.

The Bureau did, in fact, provide you with requested information on three separate occasions. CFPB only declined to provide information that was duplicative, unnecessary or disruptive to our operations. Even in those situations, the Bureau offered to reconsider providing information to GAO. For example, in CFPB's January 28, 2026 submission we noted that "if GAO has a specific, detailed inquiry regarding a particular system GAO may submit that inquiry and the Bureau will evaluate the request." Rather than following up in earnest with the Bureau's offer, GAO reiterated the prior requests with a generic, unsupportable justification: "[t]he above requested information provides our team with important <u>context</u> for understanding CFPB's processes for ensuring that personnel, including the DOGE staff, are appropriately protecting the confidentiality, integrity, and availability of the bureau's systems." (emphasis added). GAO's follow-up did not: (i) identify the system of interest, (ii) provide any specificity to the request, or (iii) make any effort to narrow the scope of inquiry. Odd that GAO was so concerned with "context" when asking for unnecessary information from CFPB and yet provides no context in the SOF to illustrate the Bureau's work and effort to be responsive.

Second, the SOF implies that statements from Bureau officials are of limited or questionable relevance to this inquiry:

> The CFPB Chief Information Officer affirmed that this information was accurate. However, the Bureau did not provide us with information needed to confirm . . . . SOF p.8 n.18.

> The CFPB Chief Information Officer affirmed that this information was accurate. However, the Bureau did not provide us with information needed to confirm . . . . SOF p.13 n.27.

GAO's repeating of this statement and inclusion of similar ones appears intended to cast doubt on the veracity of statements of Bureau officials. This is offensive and disparages the character of Bureau staff. The Bureau's official responses to GAO even re-confirmed some of the information from the Chief Information Officer and yet this was still somehow suspect to GAO: "According to CFPB, DOGE team staff members were given access to 19 systems . . . but the bureau has not provided us the with the information needed to confirm this system access." SOF p.7. An affirmed statement from a Bureau official coupled with an official response to GAO's inquiry is still somehow not enough for GAO's congressional clients. Perhaps GAO's clients are disappointed in the facts not fitting their predetermined narratives.[2]

Last, the SOF takes a misleading tone or misstates basic facts throughout. For example, on page 4 GAO states that the Bureau has six divisions. CFPB is organized into seven divisions as is presented on our public website - https://www.consumerfinance.gov/about-us/the-bureau/bureau-structure/. In another instance, GAO states that CFPB provided documentation that DOGE staff "reviewed" the Bureau's Acceptable Use Policy ("AUP"). SOF p.13 n.27. In fact, CFPB provided documentation that DOGE staff had been assigned and completed the AUP requirement similar to other Bureau personnel. Whether these misstatements are due to rushed efforts to issue the SOF or intentionally designed to mislead is unclear, but the impact is the same – faulty reporting on Bureau operations.

This SOF is the latest in a series of redundant, unnecessary, and burdensome engagements initiated by GAO against the Bureau. Most of the GAO engagements in the past year were not required by statute or congressional committees. Rather, GAO is serving at the behest of a few congressional members to harass and impede the CFPB and its efforts to implement the President's agenda.

It is the Bureau's sincere hope that GAO will address CFPB's concerns and arrest its efforts to produce biased and flawed materials.

Regards,

Mark Paoletta
Chief Legal Officer

---

[2] To be clear GAO staff have been professional and courteous in their engagement with CFPB staff. Nonetheless, the GAO's engagements and work products are deeply troubling to CFPB.

GAO Note 1: CFPB sent this letter in response to our request for an exit conference (a meeting between agency officials and GAO to close out audit work and gives both organizations an opportunity to reach a mutual understanding of relevant facts, statements, and other information).

On May 18, 2026, we responded by explaining that although we disagreed with several points in the letter, we expressed our desire to address them in a complete and constructive manner. For those reasons, we stated that we believed that an exit conference would be the appropriate forum to work through and potentially address the concerns. On June 3, 2026, a CFPB senior counsel stated that the bureau declined our offer of an exit conference.

GAO Note 2: This is not a fully accurate summary of our correspondence on this topic. We provided multiple justifications in our February 5, 2026, request, including the need for important context. Other justifications we provided highlighted missing information (e.g., level of access for each system account), answered questions from CFPB (e.g., to define the terms security awareness training and role-based security training), and explained that Government Auditing Standards call for us to corroborate testimonial evidence with other evidence.

Our February 2026 response also offered alternative methods to obtain information in order to not disrupt bureau operations, such as for CFPB to provide us with screenshots of systems in lieu of meetings for us to observe relevant systems.

GAO Note 3: This is not a fully accurate summary of our correspondence on this topic. We provided multiple justifications in our February 5, 2026, request, including the need for important context. Other justifications we provided highlighted missing information (e.g., level of access for each system account), answered questions from CFPB (e.g., to define the terms security awareness training and role-based security training), and explained that *Government Auditing Standards* call for us to corroborate testimonial evidence with other evidence.

Our February 2026 response also offered alternative methods to obtain information in order to not disrupt bureau operations, such as for CFPB to provide us with screenshots of systems in lieu of meetings for us to observe relevant systems.

GAO Note 4: We could not fully assess the accuracy and reliability of the testimonial evidence we received from CFPB because the bureau did not always provide us with corroborating information (e.g., documentation or an opportunity to observe relevant systems).

As previously mentioned, *Government Auditing Standards* call for us to corroborate testimonial evidence with other evidence (e.g., observation) where possible.

GAO Note 5: The information we presented on CFPB's divisions was published in an April 2024 GAO report (see GAO-24-107512). When we visited the website cited in the bureau's letter in April 2026, it did not describe CFPB's divisions. That site also explained that the page was being updated and will be back up soon.

GAO Note 6: This is not a fully accurate summary of the evidence provided by CFPB. As discussed earlier in this report, CFPB did not respond to our request for documentation showing that all DOGE team members acknowledged the bureau's policy on acceptable use of its IT resources and agreed to abide by those rules, consistent with the bureau's information security policy.

Accessible Text for Enclosure III: Comments from Consumer Financial Protection Bureau

Consumer Financial Protection Bureau
1700 G Street, N.W., Washington, DC 20552

April 2, 2026

Daniel Garcia-Diaz
Managing Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G St. NW
Washington, DC 20548

Dear Mr. Garcia-Diaz:

The Consumer Financial Protection Bureau ("CFPB" or "Bureau") writes this letter to comment on the Government Accountability Office's ("GAO") draft statement of facts ("SOF") in the engagement 108912 ("USDS Data Protection"). This engagement and the SOF concern the activities of Department of Government Efficiency ("DOGE") staff assigned to the Bureau. After reviewing the SOF, the Bureau must formally notify you of our significant concerns regarding GAO's gross inaccuracies and misleading characterizations. To be blunt, the SOF is incoherent and demonstrates no effort to report on the information provided by CFPB. Rather, GAO has cobbled together a hodgepodge of misleading, confusing statements and then blames its muddled reporting on the Bureau's alleged unwillingness to provide information.

GAO's stated objectives for this engagement were to "(1) describe the CFPB systems that the bureau's DOGE team had been provided access to and how the team planned to use those systems, (2) evaluate the extent to which CFPB 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." For over a year, CFPB has sought to accommodate GAO's requests while protecting the CFPB's legitimate interests, including its ability to defend a lawsuit, AFL-CIO v. Department of Labor, et al., 1:25-cv-00033, that was substantially related to the questions in this incredibly broad engagement. Despite these concerns, the CFPB quickly provided responsive materials that would address GAO's stated objectives without impairing this litigation. Not satisfied with the Bureau's reasonable approach, GAO repeatedly asked for the same information during the litigation.[1] After the litigation was resolved, GAO reengaged with the Bureau and CFPB provided a second tranche of responsive materials and information, comprehensively responding to GAO. The CFPB has provided information necessary to address all of GAO's stated objectives, including providing information to identify the level of access for each system accessed by a DOGE team member, non-disclosure agreements, and information about the training completed by DOGE team members. The CFPB also informed GAO that it has no reports or awareness of any instances of actual or potential misuse of agency systems by DOGE team staff, and that at all times their access to CFPB systems was

[1] CFPB acknowledges that GAO attempted to find "accommodations" with the Bureau during the litigation, but fundamentally there was never a true appreciation or acknowledgment by GAO that the Bureau was constrained by underlying litigation, and so GAO was unyielding in its demands.

monitored and captured through system logs. Your agency, however, was never satisfied with Bureau for not participating in this engagement. I'd like to highlight just a few of the many issues with GAO's approach to this engagement and its resulting SOF.

First, the Bureau has consistently engaged with GAO in good faith to provide information for this engagement. The Bureau provided documentation on May 29, 2025, again on January 28, 2026 and additional clarification and information on March 6, 2026. The Bureau has also repeatedly, both formally and informally, shared its concerns regarding the breadth and intrusiveness of this engagement. In contrast, GAO only made minimal efforts to constrain its inquiry to a reasonable scope. Nonetheless, the Bureau provided GAO with substantive responses and documentation. In its SOF, GAO provides no context for the Bureau's efforts and responsiveness to GAO. Rather, GAO creates a false narrative of CFPB somehow being obstructionist:

> "In February 2026, CFPB declined to provide [ ] information or confirm whether such information exists" SOF p.10 n.23.
>
> "We [GAO] requested this information multiple occasions . . . . the bureau declined to provide more information." SOF p.13.
>
> "We [GAO] requested this information multiple occasions . . . . the bureau declined to provide more information. SOF p.14.

The Bureau did, in fact, provide you with requested information on three separate occasions. CFPB only declined to provide information that was duplicative, unnecessary or disruptive to our operations. Even in those situations, the Bureau offered to reconsider providing information to GAO. For example, in CFPB's January 28, 2026 submission we noted that "if GAO has a specific, detailed inquiry regarding a particular system GAO may submit that inquiry and the Bureau will evaluate the request." Rather than following up in earnest with the Bureau's offer, GAO reiterated the prior requests with a generic, unsupportable justification: "[t]he above requested information provides our team with important context for understanding CFPB's processes for ensuring that personnel, including the DOGE staff, are appropriately protecting the confidentiality, integrity, and availability of the bureau's systems." (emphasis added). GAO's follow-up did not: (i) identify the system of interest, (ii) provide any specificity to the request, or (iii) make any effort to narrow the scope of inquiry. Odd that GAO was so concerned with "context" when asking for unnecessary information from CFPB and yet provides no context in the SOF to illustrate the Bureau's work and effort to be responsive.

Second, the SOF implies that statements from Bureau officials are of limited or questionable relevance to this inquiry:

> "The CFPB Chief Information Officer affirmed that this information was accurate. However, the Bureau did not provide us with information needed to confirm . . . ." SOF p.8 n.18.
>
> "The CFPB Chief Information Officer affirmed that this information was accurate. However, the Bureau did not provide us with information needed to confirm . . . . SOF p.13 n.27.

GAO's repeating of this statement and inclusion of similar ones appears intended to cast doubt on the veracity of statements of Bureau officials. This is offensive and disparages the character of Bureau staff. The Bureau's official responses to GAO even re-confirmed some of the information from the Chief Information Officer and yet this was still somehow suspect to GAO:

“According to CFPB, DOGE team staff members were given access to 19 systems . . . but the bureau has not provided GAO with the information needed to confirm this system access.” SOF p.7. An affirmed statement from a Bureau official coupled with an official response to GAO’s inquiry is still somehow not enough for GAO’s congressional clients. Perhaps GAO’s clients are disappointed in the facts not fitting their predetermined narratives.[2]

Last, the SOF takes a misleading tone or misstates basic facts throughout. For example, on page 4 GAO states that the Bureau has six divisions. CFPB is organized into seven divisions as is presented on our public website – https://www.consumerfinance.gov/about-us/the-bureau/bureau-structure/. In another instance, GAO states that CFPB provided documentation that DOGE staff “reviewed” the Bureau’s Acceptable Use Policy (“AUP”). SOF p.13 n.27. In fact, CFPB provided documentation that DOGE staff had been assigned and completed the AUP requirement similar to other Bureau personnel. Whether these misstatements are due to rushed efforts to issue the SOF or intentionally designed to mislead is unclear, but the impact is the same – faulty reporting on Bureau operations.

This SOF is the latest in a series of redundant, unnecessary, and burdensome engagements initiated by GAO against the Bureau. Most of the GAO engagements in the past year were not required by statute or congressional committees. Rather, GAO is serving at the behest of a few congressional members to harass and impede the CFPB and its efforts to implement the President’s agenda.

It is the Bureau’s sincere hope that GAO will address CFPB’s concerns and arrest its efforts to produce biased and flawed materials.

Regards,

Mark Paoletta
Chief Legal Officer

[2] To be clear GAO staff have been professional and courteous in their engagement with CFPB staff. Nonetheless, the GAO’s engagements and work products are deeply troubling to CFPB.