United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

March 24, 2025

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Comptroller General Dodaro:

Federal agencies depend on technology systems and electronic data to carry out their missions and operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and to our national security. In addition, many of these systems contain vast amounts of personally identifiable information (PII),[1] thus making it imperative to protect the confidentiality, integrity, and availability of this information.

Recognizing the importance of this issue, Congress and the executive branch have established multiple requirements and guidance aimed at protecting agency systems and their sensitive information.

For example:

1. Under the Federal Information Security Modernization Act of 2014 (FISMA) and its predecessor statute, the Federal Information Security Management Act of 2002, federal agencies are required to establish and implement comprehensive information security programs.[2]

2. The Office of Management and Budget (OMB) has important policy and oversight roles specified in FISMA, as well as responsibility for the information management portfolio responsibilities established in the Paperwork Reduction Act and the Clinger-Cohen Act.[3] Under these authorities, OMB Circular A-130, *Managing Information as a Strategic Resource,* establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy.[4] It also emphasizes the role of both security and privacy in the federal information life cycle and as crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.

3. The National Institute of Standards and Technology (NIST), a component of the Department of Commerce, also has an important role in ensuring the security of federal networks through the issuance of standards and guidance to protect government information, information systems, and privacy. For example, NIST Special Publication 800-53 establishes comprehensive security and privacy controls for federal information systems and organizations,[5] and OMB has required agencies to implement NIST's cybersecurity standards and guidelines for non-national security systems.[6]

4. The Privacy Act of 1974[7] and the E-Government Act of 2002[8] provide foundational privacy protections for federal data containing PII of all Americans, including procedures for the sharing of such data among government organizations.

5. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations provide for the creation, enforcement, and monitoring of information security and privacy standards for electronic health data.[9]

It is imperative that federal organizations—including the administration's newly established United States DOGE Service—follow all applicable laws and guidance. The United States DOGE Service was created by executive order on January 20, 2025 with the mission of implementing the President's DOGE (Department of Government Efficiency) agenda to modernize federal technology and software to maximize government efficiency and productivity.[10] The executive order established this organization by: (1) renaming the United States Digital Service as the United States DOGE Service (USDS); and (2) creating a time-limited U.S. DOGE Service Temporary Organization within the new USDS.[11] The order also calls for the heads of most executive branch agencies to establish DOGE teams at their respective agencies. These teams are to work with USDS and advise agency heads on implementing the President's DOGE agenda.

To further assist USDS, the executive order also calls for agency heads to take all necessary steps to ensure that USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. Of note, the order states that USDS "shall adhere to rigorous data protection standards" and that it shall obtain access from agency heads "to the maximum extent consistent with law."[12]

Given the sensitivity and critical importance of the systems and information to which USDS and agency DOGE teams may have access, we request that GAO evaluate the extent to which:

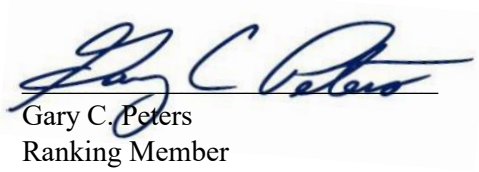
1. USDS and agency DOGE teams have established and implemented processes for protecting the privacy, confidentiality, integrity, and availability of agency systems and information as required by applicable federal laws and guidance, including those that ensure the privacy of the personally identifiable information and other sensitive information of Americans in the possession of federal agencies; and

2. Agencies have established and implemented processes for ensuring that USDS and agency DOGE teams are appropriately protecting the confidentiality, integrity, and availability of federal agency systems and information as required by such laws and guidance, including those that protect the privacy of personally identifiable information; and

3. Agencies have recorded or reported instances where privacy and/or cybersecurity controls allegedly or actually violated by USDS or agency DOGE teams, intentionally or unintentionally, including instances of editing, merging, adding or deleting information in databases, instances of unauthorized access, instances of inappropriate access to sensitive information such as Inspector General investigative or whistleblower records, or instances of transmitting or disclosing data outside of previously established agency systems.

Thank you for your prompt attention to this request. Please contact my staff at (202) 224-4751 to discuss the details and timing of this GAO review.

Sincerely,



Gary C. Peters
Ranking Member
Homeland Security and
Governmental Affairs Committee