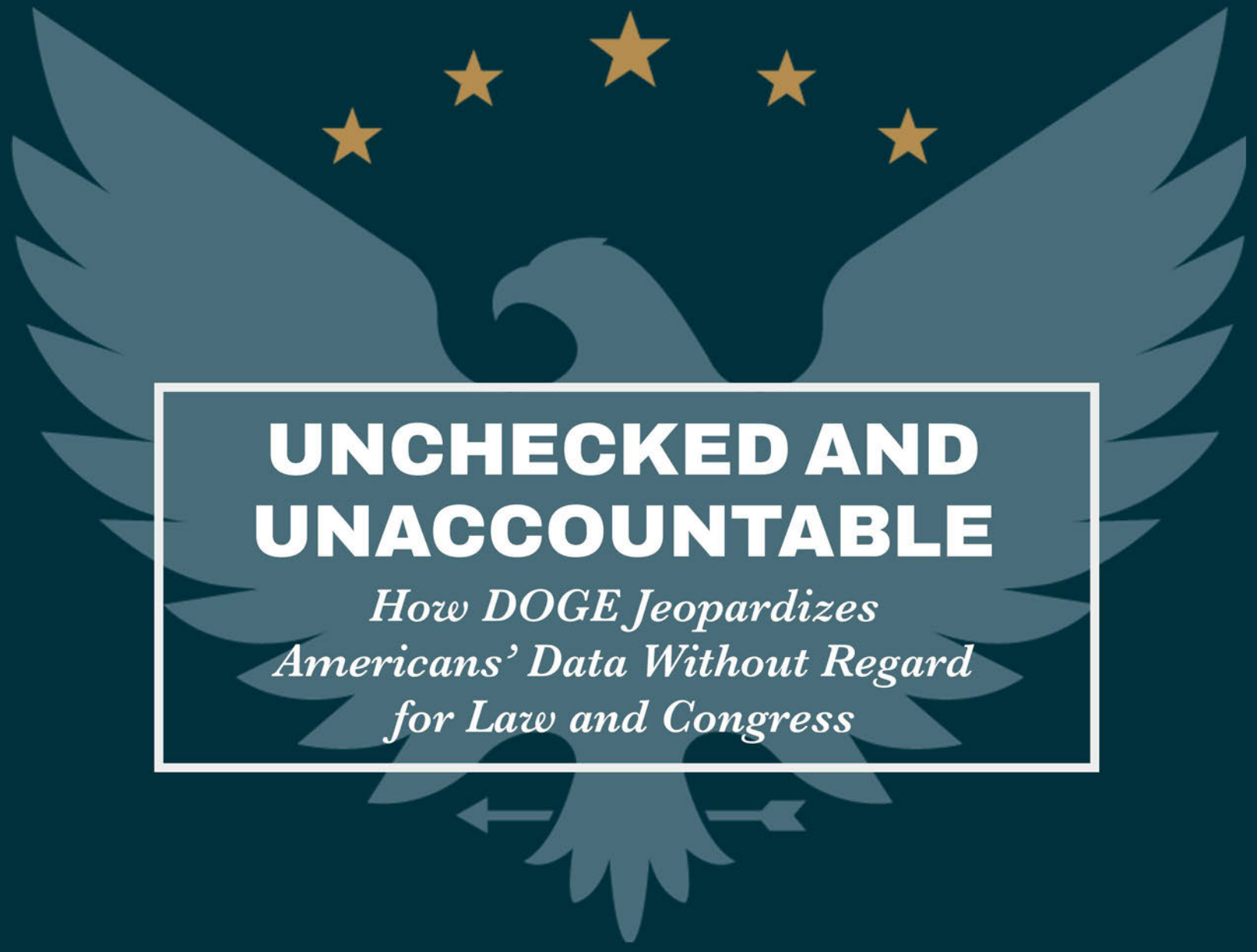
United States Senate Committee On

HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

Ranking Member Gary Peters



UNCHECKED AND UNACCOUNTABLE

How DOGE Jeopardizes Americans' Data Without Regard for Law and Congress

HSGAC Minority Staff Report

September 2025

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

U.S. Senator Gary Peters, Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs (HSGAC), and his Minority Staff (herein after "staff") have found through a series of oversight visits to executive branch agencies and whistleblower disclosures that the Department of Government Efficiency, commonly referred to as DOGE, operates outside of, and even counter to, federal law and their purported efficiency and transparency goals. DOGE, initially led by billionaire Elon Musk, consists primarily of workers with no policy or government experience and significant conflicts of interest, raising questions about both the effectiveness of and the motivations behind their work.

Staff identified, through oversight visits to the Social Security Administration (SSA), the General Services Administration (GSA), and Office of Personnel Management (OPM), that DOGE's actions had significant privacy, security, and cost implications, which called into question who was actually in charge at these agencies. Additionally, through a series of whistleblower disclosures, staff learned that individuals associated with DOGE have effectively ordered agencies to assist with the creation of databases that can be manipulated with little to no oversight, and which contain highly sensitive personally identifiable information on every American. Ranking Member Peters and staff have found that DOGE has, in fact, done little more than put Americans' most private information at risk.

Multiple whistleblowers, including Chuck Borges, the former Chief Data Officer (CDO) at SSA, provided disclosures that, as of the time of the disclosures, DOGE employees at SSA had access to personal data on all Americans, including Social Security numbers (SSNs), ***in a cloud environment without any verified security controls and without standard agency visibility into their use of that data***. Even Borges, as CDO, did not have that level of access to data.[1] Among the DOGE employees who apparently have this unfettered access is Edward Coristine – the same individual who had been fired from a previous job for sharing sensitive data with competitors.[2] Because agency officials allegedly do not have oversight of these DOGE employees' actions, they cannot know whether these individuals have moved any data out of SSA, granted access to the data to unauthorized users, including to private companies, or whether the data has been accessed illicitly.

In a worst-case scenario, one whistleblower noted the possibility that the agency may need to re-issue SSNs to all who possess one.[3] A compromised SSN can be personally devastating. That's because SSNs are the backbone for accessing all kinds of public and private services, from acquiring a driver's license to going to the doctor. Unwinding the harm done by identity thieves can involve years of credit and identity monitoring, mountains of paperwork, and

[1] Interview with Whistleblower by Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Whistleblower disclosure, on file with the Committee).

[2] *Recording reveals new details on controversial DOGE employee,* CNN (Feb. 22, 2025) (www.cnn.com/2025/02/21/politics/doge-musk-edward-coristine-invs); Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (Sep. 8, 2025) (Whistleblower disclosure, on file with the Committee).

[3] Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Whistleblower disclosure, on file with the Committee).

as one victim of the 2015 OPM data breach put it: "endless explaining."[4] If penetrated, this data vulnerability could result in the most significant data breach of Americans' sensitive data in history. Beyond the toll on individuals, if the entirety of U.S. SSN data was compromised, the possible impact on the ability of financial institutions and other major segments of the economy to function could be enormous.

Additionally, it is very likely that foreign adversaries, such as Russia, China, and Iran, who regularly attempt cyber attacks on the U.S. government and critical infrastructure, are already aware of this new DOGE cloud environment.[5] An internal SSA risk assessment determined that the likelihood of a data breach with "catastrophic adverse effect" is between 35 and 65 percent.[6] The potential breach of this sensitive data, and its potential misuse, significantly increase the urgency for DOGE to stop any high-risk projects and disclose its work to Congress and the public.

The findings and recommendations outlined in this report are based on a series of staff visits to federal agencies and supporting information from current and former federal employees. DOGE data security violations at SSA are made possible by the environment of secrecy and lack of oversight that staff encountered at each agency. A clear pattern emerged across agencies -- officials who questioned DOGE were pushed out, and DOGE-affiliated personnel were installed in key positions such as Chief Information Officer. These DOGE associates were then able to grant approval to other DOGE employees to work with sensitive data without restrictions. Another consistent part of the DOGE playbook was establishing networks and environments to avoid oversight from agency officials, such as the cloud environment at SSA and the Starlink setup at GSA.

Perhaps most concerning is that Administration officials during these visits were unable or unwilling to answer one basic question: Who is functionally in charge of significant policy changes at these agencies?[7] DOGE is empowered only to advise the President, given that it was created by Executive Order and is not statutorily authorized.[8] However, following reports that

[4] *One Year After OPM Data Breach, What Has the Government Learned?,* NPR (June 6, 2016) (www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned).

[5] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Assessment* (Feb. 5, 2024) (www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf).

[6] Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Whistleblower disclosure, on file with the Committee).

[7] General Services Administration, Site Visit with Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff and Senate Committee on Environment & Public Works Majority and Minority Staff (May 28, 2025); Social Security Administration, Site Visit with Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff and Senate Committee on Finance Minority Staff (May 29, 2025); Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[8] Under Articles I and II of the United States Constitution, only Congress can create, eliminate, and set funding levels for federal departments and the creation of DOGE through Executive Order does not confer with it the power to unilaterally dismantle agency operations, freeze Congressionally authorized funds decisions, or determine personnel level.

DOGE staff have directed significant agency actions, HSGAC staff asked agencies to account for DOGE activities, access, and authorities.[9]

In response to these questions, senior officials at SSA, GSA, and OPM all failed to provide information about who was in charge; what conduct DOGE teams were engaged in; and what data those teams had been given access to, including the authorities and restrictions guiding their access. None of the agencies could answer simple questions about organizational charts and employee roles. During oversight trips, GSA and OPM would not even directly acknowledge the existence of their DOGE teams – despite the fact that Executive Order 14158 requires each agency to have a DOGE team comprised of at least four people.[10] At the OPM site visit, officials provided staff with information that directly contradicted court documents filed on the agency's behalf.

Senior officials at all three agencies also obstructed staff's oversight efforts. At GSA, officials refused to show staff at least six offices that GSA had allowed DOGE to convert into bedrooms. These same officials also refused to show staff Starlink infrastructure, the satellite internet service controlled by Elon Musk and installed at the agency. Officials reiterated several times that staff were welcome to make a follow-up oversight visit to see these areas, but later rejected a request for a second visit. None of the agencies have responded to staff's follow-up questions, including whether they are in compliance with federal law. None of the agencies have allowed meetings with representatives from agency DOGE teams. In the DOGE spaces staff were permitted to view, armed guards controlled access to work and living spaces, rooms were locked, and office windows appeared to have been hastily covered with black trash bags and tape.

[9] Letter from Senator Gary Peters to Acting Administrator Stephen Ehikian, General Services Administration (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Administrator Janet Petro, National Aeronautics and Space Administration (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Administrator Marco Rubio, United States Agency for International Development (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Commissioner Leland Dudek, Social Security Administration (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Director Charles Ezell, Office of Personnel Management (Mar. 26, 2025); Letter from Senator Gary Peters to Administrator Kelly Loeffler, Small Business Administration (Mar. 26, 2025); Letter from Senator Gary Peters to Administrator Lee Zeldin, Environmental Protection Agency (Mar. 26, 2025); Letter from Senator Gary Peters to Attorney General Pam Bondi, Department of Justice (Mar. 26, 2025); Letter from Senator Gary Peters to Director Sethuraman Panchanathan, National Science Foundation (Mar. 26, 2025); Letter from Senator Gary Peters to Chairman David A. Wright, Nuclear Regulatory Commission (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Brooke Rollins, Department of Agriculture (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Chris Wright, Department of Energy (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Doug Burgum, Department of the Interior (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Doug Collins, Department of Veterans Affairs (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Howard Lutnick, Department of Commerce (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Kristi Noem, Department of Homeland Security (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Linda McMahon, Department of Education (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Lori Chavis-DeRemer, Department of Labor (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Marco Rubio, Department of State (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Pete Hegseth, Department of Defense (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Robert F. Kennedy, Department of Health and Human Services (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Sean Duffy, Department of Transportation (Mar. 26, 2025); Letter from Senator Gary Peters to Secretary Scott Turner, Department of Housing and Urban Development (Mar. 26, 2025).

[10] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025).

This report concludes that DOGE is jeopardizing Americans' most sensitive data, while its employees operate under a layer of secrecy that shields them from meaningful oversight and accountability. This environment results in serious cybersecurity vulnerabilities, privacy violations, and risk of corruption that could open Americans' most sensitive information to targeting by malicious actors or allow it to be used in ways that violate fundamental privacy rights – or serve to benefit DOGE employees and the private companies with which many maintain strong ties.

II. FINDINGS

1. **DOGE practices violate statutory requirements, creating unprecedented privacy and cybersecurity risks.** During the SSA and OPM site visits, staff were provided information on the security practices of the DOGE employees that directly contradicted whistleblower disclosures, public reporting, and court filings. At GSA, senior agency officials could not inform staff on DOGE employee adherence to privacy and cybersecurity policy, guidance, and existing statute. DOGE employees' reported actions appear to violate several provisions of the Privacy Act of 1974 and the E-Government Act of 2002 pertaining to the protection of Americans' personal data and combination of data across agencies. Particularly at SSA, DOGE personnel are reportedly putting the sensitive personal information of all Americans at extraordinary and potentially catastrophic risk – and, given the lack of agency visibility into the cloud environment, we may never know the full extent of any damage done. One risk is that DOGE employees at SSA could potentially provide access to sensitive data to private companies.

2. **Agencies with Senate-confirmed executive officials could not identify who, in practice, was in charge.** Staff learned, through observation and disclosures, that DOGE teams wield an unknown level of authority without oversight from other agency officials. Transformative agency initiatives, including massive reductions in force, agency reorganizations, and large-scale property disposals, should be led by public-facing agency leaders. Agency officials, however, were unable to substantially answer whether Senate-confirmed executive officers or DOGE, oversaw key decisions impacting agencies' missions.

3. **Agencies could not provide a clear chain of command for DOGE operations.** As it stands, the White House claims that Amy Gleason is leading DOGE as the Administrator of the U.S. DOGE Service. However, whistleblowers told staff that Ms. Gleason is just a figurehead with no real power over DOGE staff at agencies and that most DOGE staff actually function outside of the U.S. DOGE Service.[11] Agency officials staff spoke to were also unable or unwilling to answer for DOGE activities at their agencies.[12] It has

[11] Interview with Whistleblower by Senate Committee on Homeland Security and Governmental Affairs (July 7, 2025) (Whistleblower disclosure, on file with the Committee).

[12] General Services Administration, Site Visit with Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff and Senate Committee on Environment & Public Works Majority and Minority Staff (May 28, 2025); Social Security Administration, Site Visit with Senate Committee on Homeland Security and

even been reported that Musk ally Steve Davis was attempting to continue to lead DOGE after he had already left government.[13] This unclear leadership structure prevents Congress from being able to hold relevant officials responsible for significant agency policy initiatives – including any missteps or misconduct.

4. **Secrecy surrounding DOGE operations prevents congressional oversight and public accountability.** The secrecy surrounding DOGE personnel and their work at executive branch agencies raises serious accountability concerns. DOGE's work has been riddled with errors and missteps, legal controversies, and shadowy data-gathering activities that threaten privacy rights.[14] At all the agency site visits, staff requests to speak to DOGE employees were denied. When staff pushed for details on DOGE's activities or even the scope of their power, GSA, OPM, and SSA all failed to answer simple questions about the size, composition, scope, and plans for their DOGE teams. GSA and OPM refused to even acknowledge the existence of their DOGE teams. Furthermore, during the oversight visits, staff were prohibited from taking photos and were met with armed guards, blacked out windows, and locked rooms in DOGE spaces.

5. **DOGE personnel are not subject to the same agency policies and requirements as other agency employees.** During agency site visits, staff observed each DOGE workspace cordoned off with armed guards, providing an unusual layer of protection to their activities. Staff were not provided clear reasons why this was needed. Beyond security, DOGE workspaces were either completely or largely empty as their staff were able to work remotely at their discretion (despite strict in-office requirements for regular federal employees, in many cases without adequate office space). These DOGE employees also appear to be working across multiple federal agencies simultaneously, outside of standard practice and policy. Additionally, DOGE employees have largely been given data access without adequate training or experience, according to court filings and whistleblower disclosures.[15]

Governmental Affairs Majority and Minority Staff and Senate Committee on Finance Minority Staff (May 29, 2025); Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs Majority and Minority Staff and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[13] *DOGE lead Steve Davis did not go quietly*, Politico (July 14, 2025) (www.politico.com/news/2025/07/14/doge-lead-steve-davis-did-not-go-quietly-00452257).

[14] *100 days of DOGE: lots of chaos, not so much efficiency,* Reuters (April 24, 2025) (www.reuters.com/world/us/100-days-doge-lots-chaos-not-so-much-efficiency-2025-04-24/); *Judge blocks OPM, Education Department from sharing personal info with DOGE*, Politico (Feb. 24, 2025) (www.politico.com/news/2025/02/24/judge-blocks-opm-education-dept-from-sharing-info-with-doge-00205699); *Whistleblower says Trump officials copied millions of Social Security numbers,* NPR (Aug. 26, 2025) (www.npr.org/2025/08/26/nx-s1-5517977/social-security-doge-privacy).

[15] Declaration of Tiffany Flick (Mar. 7, 2025), *American Federation of State, County and Municipal Employees v. Social Security Administration,* N.D.M.d. (No. 1:25 CV 00596); Interview with Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (July 7, 2025) (Whistleblower disclosure, on file with the Committee).

III. RECOMMENDATIONS

FOR GSA, SSA, AND OPM:

1. **Immediately shut down the new cloud environment at SSA that contains NUMIDENT data.** SSA must immediately shut down the cloud environment built by/for DOGE personnel to work on Numerical Identification System (NUMIDENT) data, and work to limit the extraordinary risk to Americans' data privacy created by these actions. SSA must also thoroughly audit the use of the cloud environment and attempt to ascertain whether any data breaches or data manipulation occurred.

2. **Revoke all DOGE access to any personally identifiable information across the federal government until agencies certify that all agency personnel are in compliance with the Federal Information Security Management Act (FISMA), the Privacy Act, the Federal Records Act, and any other relevant information management statutes.** Given the unacceptable risk posed by DOGE activities already known to have occurred at SSA and other agencies, the Administration should immediately terminate DOGE personnel access to any personally identifiable information and any other sensitive data across the federal government. DOGE employees, like all federal employees, must be required to adhere to the same statutes, agency policy, and interagency guidance regarding privacy, cybersecurity, and information protections.

3. **Cease all DOGE operations at SSA, GSA, and OPM until agencies can certify that DOGE personnel are beholden to appropriate agency oversight and chain of command.** Agency leadership must ensure that DOGE employees are taking direction from senior agency officials and are not receiving project taskings from individuals outside of their assigned agency or outside government. Moreover, agencies must demonstrate that all DOGE data projects are overseen by agency leadership, and that senior officials have full visibility into data-sharing, cloud environments, and transfer and exfiltration of agency data. Until this can be accomplished in a way that is convincing to Congress and the public, DOGE operations at these agencies must stop.

4. **Release information about the data access privileges of DOGE personnel.** DOGE personnel data access must be made transparent, and subject to congressional oversight.

5. **Release the identities, titles, and position descriptions for all personnel whose principal mission is implementing Executive Orders 14158, 14210, 14219 and 14222.** Agency employees who play significant roles in agency decision making, including major funding, personnel, and policy decisions should not be hidden or removed from employee rosters. Senior agency officials should be accountable for overseeing the activities of DOGE personnel and should not be left in the dark on the whereabouts, work products, and ultimate goals of their DOGE personnel.

6. **Ensure all agency personnel are subject to consistent and/or appropriate trainings, policies, and restrictions.** DOGE employees should not have differing access to data, telework arrangements, personal security, or agency resources compared to other

employees. Additionally, DOGE employees should be held to the same standards as other employees when it comes to completing required cybersecurity, privacy, and other trainings before they received access to agency systems.

FOR INSPECTORS GENERAL:

1. **Conduct a comprehensive audit of access to sensitive data systems at these agencies.** This audit should include an evaluation of existing agency policy, procedures, and adherence and understanding of applicable statute regarding data usage and access to agency systems and data. The audit should evaluate whether DOGE individuals used existing agency processes for requesting and granting access and if access to agency databases were granted due to threats or other coercive tactics.