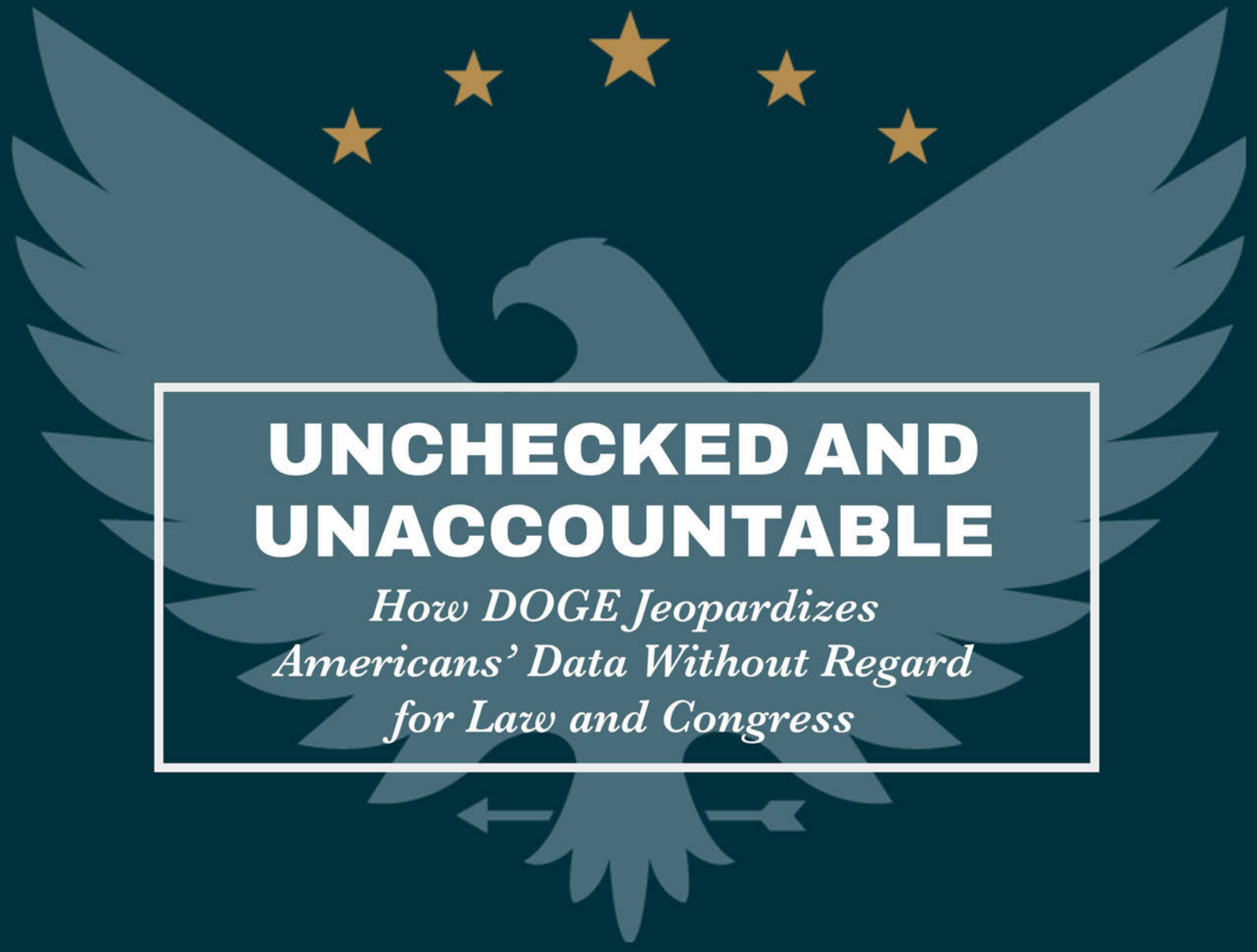
United States Senate Committee On

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.

IV. AGENCY OVERSIGHT VISITS

For months, under the direction of Ranking Member Gary Peters, Senate Committee on Homeland Security and Governmental Affairs (HSGAC) Minority Staff (herein after "staff") repeatedly requested information from GSA, OPM, and SSA on their compliance with congressionally mandated functions, including information on their adherence to privacy and other data laws, and their ability to fulfill their statutory mandates.[16] Reports widely indicated that DOGE was in violation of the law across multiple federal agencies.[17] These three agencies hold sensitive information on millions of Americans, countless businesses, and the most senior public officials in the country. Staff requested information relating to actions across government by individuals associated with DOGE and DOGE personnel's compliance with statutory requirements and agency policies and procedures. Staff never received more than an acknowledgment of receipt from GSA, SSA, OPM, and several other agencies. In the absence of any meaningful compliance with requests for information, Senator Peters directed staff to conduct oversight visits at these agencies.

President Trump created DOGE by Executive Order (EO) on January 20, 2025.[18] The administration and Elon Musk portrayed DOGE as a product of Musk's creation, ostensibly

[16] Email from Committee Staff to GSA Staff (Feb. 11, 2025) (on file with Committee); Email from GSA Staff to Committee Staff (Mar. 5, 2025) (on file with Committee); Email from Committee Staff to OPM Staff (Feb. 7, 2025) (on file with Committee); Email from Committee Staff to OPM Staff (Feb. 24, 2025) (on file with Committee); Email from Committee Staff to OPM Staff (Feb. 26, 2025) (on file with Committee); Letter from Ranking Member Gary Peters, to Charles Ezell, Acting Director of OPM (Feb. 7, 2025); Letter from Senator Gary Peters to Acting Director Charles Ezell, Office of Personnel Management (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Administrator Stephen Ehikian, General Services Administration (Mar. 26, 2025); Letter from Senator Gary Peters to Acting Commissioner Leland Dudek, Social Security Administration (Mar. 26, 2025).

[17] *DOGE's access to federal data is 'an absolute nightmare,' legal experts warn,* Politico (February 02, 2025) (www.politico.com/news/2025/02/03/doge-treasury-usaid-donald-trump-011538); *DOGE Gains Access to Confidential Records on Housing Discrimination, Medical Details — Even Domestic Violence,* ProPublica (February 26, 2025) (www.propublica.org/article/doge-elon-musk-hud-housing-discrimination-privacy-domestic-violence).

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

intended to cut wasteful spending and combat fraud in government programs.[19] The EOs establishing DOGE place it in the Executive Office of the President in the White House, with mandatory agency DOGE teams at each federal agency to further the DOGE mission.[20] The EOs also gave DOGE access to wide swaths of government data.[21] DOGE is not authorized by statute, however, and therefore is restricted to advising the President on matters such as cutting contracts, directing layoffs, or altering agency data structures, rather than making policy decisions. Nevertheless, information from both public and non-public sources suggests DOGE is directly involved in administering policy.[22]

White House statements since January claim that DOGE is headquartered at the U.S. DOGE Service (USDS), successor of the U.S. Digital Service, under the leadership of Administrator Amy Gleason.[23] While Musk repeatedly claimed DOGE as his own, and President Trump himself proclaimed that Musk was the head of DOGE during his 2025 address to Congress, Musk did not have the authority to serve as USDS Administrator given his status as a short-term special government employee (SGE).[24] One whistleblower who worked directly with Ms. Gleason confirmed to the committee that she was not effectively in charge and did not even have the ability to make decisions related to several projects that USDS oversaw.[25] While reports indicate Musk has left government, dozens of DOGE employees reportedly remain.[26] Staff is unable to determine whether former DOGE employees continue to have access to DOGE personnel, government data, and agency software. Whistleblower accounts to staff, supported by public reporting and court documents, suggest that the primary DOGE operations occur

[19] The White House, *Issues: Government Accountability* (Accessed Sept. 8, 2025) (www.whitehouse.gov/issues/doge/).

[20] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025); Exec. Order No. 14210, 90 Fed. Reg. 9669 (Feb. 11, 2025).

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

[22] The National Constitution Center, *Is DOGE Breaking the Law?* (Mar. 13, 2025) (www.constitutioncenter.org/media/files/Is-DOGE-Breaking-the-Law-WTP-transcript.pdf).

[23] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 20, 2025); *Who is Amy Gleason, the Person Named DOGE's Acting Administrator by the White House?*, Associated Press (Feb. 25, 2025) (www.apnews.com/article/doge-acting-administrator-amy-gleason-65af638e646fdd5dd6d5fcc5cc04a2e7).

[24] Government Accountability Office, *Federal Workforce: Opportunities Exist to Improve Data on Selected Groups of Special Government Employees* (GAO-16-548) (July 2016) (www.gao.gov/assets/d16548.pdf)("The special government employee (SGE) category was created to allow certain non-government experts to advise the federal government on a short-term basis without all of the same conflict of interest rules as permanent federal employees. This allows SGE advisors to provide recommendations on a specific set of problems without giving up their outside career, which they are expected to return to once their 130-day term has expired. A GAO study found that the overwhelming majority of SGEs serve on federal advisory committees and boards, while just 3 percent serve as expert consultants outside of committees and boards. SGEs are not intended to serve as federal policy makers.").

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

[26] *See, This DOGE project is still full steam ahead*, Politico, (Aug. 4, 2025). (www.politico.com/news/2025/08/04/doge-government-retirement-00493140); *Pentagon's DOGE Unit to Scrutinize 400,000 Contracts for Cuts*, Bloomberg, (Aug. 27, 2025) (www.bloomberg.com/news/articles/2025-08-27/pentagon-s-doge-unit-to-scrutinize-400-000-contracts-for-cuts).; *The U.S. DOGE Service is still hiring*, Nextgov, (July 15, 2025) (www.nextgov.com/people/2025/07/us-doge-service-still-hiring/406735/); *DOGE plows on without Elon Musk, Rep. Sessions says*, Politico (Sept. 16, 2025) (www.politico.com/news/2025/09/16/doge-plows-on-without-elon-musk-rep-sessions-says-00565396).

separately from USDS.[27] Moreover, whistleblowers have reinforced public reporting about the consolidation of datasets across government with little to no oversight or accountability, threatening Americans' privacy, access to government programs, and the security of their data.[28] Staff ultimately decided to conduct oversight visits to GSA, SSA, and OPM because information staff received from these whistleblower sources suggested that these agencies are DOGE focal points.

I. SSA

Highlights

- **Whistleblowers told staff that, at the time of their disclosures, DOGE staffer Edward Coristine had unrestricted access to SSA data, including the personal information of all Americans, and that the agency did not have visibility into his work. He is apparently storing the information in a cloud environment without any verified security controls, risking possible breaches.**
- **An internal SSA risk assessment found that the likelihood of a "catastrophic adverse effect" resulting from a data breach was between 35 and 65 percent.**
- **SSA officials acknowledged the existence of an agency DOGE team but claimed that all DOGE personnel were appropriately onboarded and trained before accessing agency data, in contradiction of the statements of former agency officials.**
- **SSA officials were unable to provide specific details on what their DOGE team was working on, and to whom they were accountable at the agency beyond other DOGE-affiliated officials.**
- **The DOGE workspace at SSA was guarded by armed security, segregating DOGE operations from visibility of other agency employees.**

The Social Security Administration (SSA) was a particular target for DOGE from its earliest days. SSA maintains systems of records containing highly sensitive information for all Americans.[29] This includes administrative data used to determine eligibility and payment amounts for social insurance programs like Social Security and Supplemental Security Income (SSI) that deliver benefits to tens of millions of Americans every month. It also includes other highly sensitive information, such as home addresses, spousal information, and the social security numbers of everyone from infants to former Presidents.

[27] Interview with Whistleblower by Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Whistleblower disclosure, on file with the Committee); *DOGE Keeps Gaining Access to Sensitive Data. Now It Can Cut Off Billions to Farmers*, NPR (July 10, 2025) (www.npr.org/2025/07/10/nx-s1-5455779/doge-usda-farmers-data).

[28] *DOGE aims to pool federal data, putting personal information at risk*, Washington Post (May 7, 2025) (www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/); *DOGE keeps gaining access to sensitive data. Now, it can cut off billions to farmers*, NPR (July 11, 2025) (www.npr.org/2025/07/10/nx-s1-5455779/doge-usda-farmers-data).

[29] Social Security Administration, Privacy Act Systems of Records Notices (https://www.ssa.gov/privacy/sorn.html) (accessed Sept. 23, 2025).

According to court documents, senior officials who stood in the way of DOGE access to data, including former Acting Commissioner Michelle King and former Chief of Staff Tiffany Flick, were forced to retire or removed from their positions at SSA.[30] From both public and non-public sources, staff learned concerning information about DOGE access to and use of government data at SSA. This included remarkably broad access to highly sensitive agency data systems, which was blocked by a court order at the time of the staff visit to the agency.[31] One former USDS employee attended a February meeting with Amy Gleason, USDS Administrator and purported head of DOGE, and SSA DOGE staff including then-Chief Information Officer Scott Coulter. The employee told staff that Gleason did not contribute substantively to the meeting and was clearly not directing DOGE operations at the agency.[32]

Perhaps the most alarming reports concerned attempts to add SSA data to a master database that would pool data from multiple federal agencies.[33] This would likely violate the Privacy Act, the law that governs how agencies can collect, maintain use, and disseminate information about individuals.[34] Whistleblower disclosures to staff reveal that John Koval, a former SSA DOGE employee, had inquired about uploading data from agencies into a cloud environment for the alleged purpose of sharing with DHS, and was rebuffed, as far as the whistleblower knew.[35] Koval, however, has reportedly since worked both at DHS and DOJ, where SSA data has popped up in interagency projects that raised concerns among privacy experts.[36] One of the whistleblowers shared that data from SSA's Numerical Identification System (NUMIDENT) had appeared at DHS in an unusual format, suggesting that the data was not shared via a normal interagency data sharing agreement.[37]

Staff visited SSA both because of concerns about DOGE activities at the agency, and because of concerns about the OIG's lack of oversight and lack of cooperation with

---

[30] *American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration*, No. 1:25-cv-00596, (D. Md. April 17, 2025)(memorandum opinion granting preliminary injunction).

[31] *American Federation of State, County and Municipal Employees v. SSA,* No. ELH-25-0596, 1 (D.Md. March 10, 2025) (order granting preliminary injunction); *see also,* Plaintiff's Motion for Temporary Restraining Order, Preliminary Injunction, and/or other 5§ U.S.C. 705 Stay, *American Federation of State, County and Municipal Employees v. Social Security Administration*, N.D.M.d. (No. 1:25 CV 00596). This access has since been restored, but the case is still pending.

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

[33] *DOGE aims to pool federal data, putting personal information at risk*, Washington Post (May 7, 2025) (www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/); *DOGE keeps gaining access to sensitive data. Now, it can cut off billions to farmers*, NPR (July 11, 2025) (www.npr.org/2025/07/10/nx-s1-5455779/doge-usda-farmers-data).

[34] The Privacy Act of 1974, Pub. L. 93-579.

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

[36] *The Trump Administration is Building a National Citizenship Data System,* NPR (June 29, 2025) (www.npr.org/2025/06/29/nx-s1-5409608/citizenship-trump-privacy-voting-database); *Top DOGE Officials Moved from Social Security Administration to Justice Dept.*, New York Times (Apr. 18, 2025) (www.nytimes.com/2025/04/18/us/politics/doge-musk-social-security-justice-department.html).

[37] Interview with Whistleblower by Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Whistleblower disclosure, on file with the Committee). Interagency computer matching agreements have a specified format. Irregular formatting may suggest data was shared outside a formal computer matching agreement.

congressional inquiries. Ranking Member Peters requested a meeting with Michelle Anderson, the Assistant Inspector General for Audit and the senior official performing the functions and duties of the IG, on April 30, 2025, but the meeting has not occurred. Additionally, one OIG whistleblower spoke to staff about concerns that Ms. Anderson has created an informal policy at the OIG of not contradicting or criticizing DOGE.[38] Following the oversight visit, SSA OIG did respond to staff's follow-up questions, however the request for a meeting between Ms. Anderson and Senator Peters remains outstanding.

On Thursday, May 29, 2025, Majority and Minority HSGAC staff and Minority staff of the Senate Committee on Finance visited SSA Headquarters in Woodlawn, Maryland. SSA officials first hosted Senate staff at a briefing that included information about DOGE presence at the agency. The briefing was led by Dustin Brown, the then Chief Operating Officer; Brian Peltier, the Deputy Chief Information Officer; Joe Cunningham, the Acting Chief Information Security Officer; Sean Brune, the Acting Deputy Commissioner for Mission Support; Dan Callahan, Assistant Commissioner for Building and Facilities Management; and other senior officials.[39]

SSA officials informed Senate staff that SSA onboarded a 10-person DOGE team in February and March of 2025, which included four SGEs and six detailees from other agencies, including GSA, OPM, the Department of Labor, USDS, and NASA.[40] Committee staff were told that two of these individuals were no longer at SSA, and that some may have changed from SGE to permanent federal employees, although SSA would not be more specific on this point.[41]

Staff were also told that DOGE individuals underwent standard onboarding as appropriate for their positions, including background checks and privacy, cybersecurity, and ethics training.[42] These statements, however, contradict the declaration made by former Acting Chief of Staff Tiffany Flick in a March court filing. Flick said that while Akash Bobba was given some level of onboarding, trainings were done in a "truncated manner and outside normal processes."[43] Additionally, Flick said that DOGE-affiliated officials within SSA had pushed for Bobba to receive full access to SSA systems, contrary to Privacy Act requirements and without any demonstrated need – and that Flick and Acting Commissioner Michelle King were pushed out of SSA when they refused.[44]

Controlling access to agency systems and data by requiring standardized onboarding documentation and training are not just adhering to requirements in statute, OMB guidance, and

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

[39] 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).

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] 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) at 7.

[44] 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) at 9.

SSA agency policy, they are considered baseline practices for cybersecurity and privacy.[45] DOGE individuals also purportedly challenged the necessity of using SSA established processes for requesting access to SSA data.[46]

Officials said that they could not provide the names of DOGE personnel due to privacy and safety concerns. When asked if they could release the names to Congress rather than to the public, the agency told staff that they would follow up.[47] As of publication, SSA has not provided responses to any questions staff provided in writing. Staff had also received information from a whistleblower that the names of DOGE personnel had been removed from OrgChart – the software system the agency uses as its directory and to map its organizational structure.[48] The software also provides information about the nature of employees' work, including important details about their level of data access to sensitive databases. When asked, SSA officials confirmed that DOGE employees were no longer visible within the system, again invoking privacy and security concerns.[49]

Mr. Peltier told staff that he was not aware of any agreements to allow DOGE staff to share or use SSA data outside of the agency. He said that employees are not allowed to use non-SSA devices, including personal devices or devices issued by another federal agency, to access SSA data, and that it would not be possible to transfer downloaded data to a non-SSA device.[50] According to SSA, agency policy dictates that personal devices or devices issued by another federal agency are not permitted to access SSA data, except through approved data exchange agreements.[51] However, former SSA and USDS employees told staff that while real-time access to a database may not be possible without triggering data protection protocols, it *would* be possible to download a point-in-time snapshot of agency data and move that to another device and then combine it with data from another agency.[52]

Staff were told that DOGE personnel at SSA report to the Chief Information Officer, Scott Coulter, and "can't cancel contracts" themselves.[53] However, Coulter himself was a DOGE employee, at one point identified by SSA as the "lead for DOGE concerning SSA matters."[54]

---

[45] Computer Security Act of 1987; Privacy Act; FISMA; OMB 5 CFR 930.301.

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

[47] 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).

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

[49] 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).

[50] *Id.*

[51] Email from SSA to Committee Staff (Sept. 23, 2025) (on file with Committee).

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

[53] 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).

[54] SSA OIG answers to follow-up questions posed by HSGAC Minority Staff, on file with the Committee.

Staff were able to see the DOGE workspace in the Altmeyer building on SSA's main campus, which was guarded by armed security (See Exhibit A). SSA officials providing the tour confirmed that this level of security was unusual.[55] When staff asked why the additional security for the DOGE workspace was needed, Mr. Callahan said that DOGE staff were concerned about threats to their safety. Staff asked whether these were direct threats and whether officials informed law enforcement. Officials explained that there had not been a specific threat, rather that some DOGE staff felt threatened based on a communication with an SSA employee that "included cursing."[56]

Exhibit A. SSA's Guarded DOGE Wing

When staff viewed the DOGE workspace, the entire suite of offices was empty on a Thursday afternoon. The security guard, however, was still posted at the empty suite. When asked about the agency telework policy, one official told staff that all agency employees are mandated to report to the office five days a week.[57] Staff inquired about the DOGE team's whereabouts, and officials informed staff that DOGE staff had telework agreements with the agency.[58] SSA officials confirmed that DOGE were the only individuals who had this approved telework structure in the entire CIO's office.[59] SSA officials could not answer questions about the telework agreements, including a reason for the telework exception and who approved the agreements. In her affidavit, Ms. Flick stated that at least Mr. Bobba had a telework agreement to work on SSA projects while

[55] 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).
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*

based at OPM -- an arrangement she found concerning because employees are required to telework in a secure space with no other individuals present to ensure the protection of SSA data.[60]

Whistleblowers, including the former Chief Data Officer (CDO) at SSA, Charles Borges, later informed staff that Edward Coristine, the 19-year-old DOGE staffer who was previously fired from a job for leaking company data to a competitor, and other DOGE personnel had been granted permission to move highly sensitive SSA data into an unmonitored cloud environment.[61] The whistleblowers said that DOGE has uploaded a live copy of NUMIDENT, which contains highly sensitive personal data on anyone who has held a social security number, including every American.[62] This includes social security numbers (SSNs), place and date of birth, work permit status, and parents' names, among other sensitive personal information, for all Americans, to a cloud environment.[63] Authorization to upload live SSA data to the cloud environment was apparently granted, according to whistleblower disclosures, by Michael Russo and Aram Moghaddassi, both of whom are DOGE-affiliated.[64] It is highly 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.[65]

According to a whistleblower disclosure, Moghaddassi and Russo granted approval for the data move despite a June 12, 2025 internal risk assessment flagging a high level of risk and potentially catastrophic impact to SSA beneficiaries and SSA programs absent additional controls to safeguard against unauthorized access (*See* Exhibit B).[66] Based on the internal risk assessment, SSA employees evaluated the likelihood of such catastrophic impact to be between 35 and 65 percent.[67] Some of the potential events that could be expected from such a breach, according to SSA, include "widespread PII [personally identifiable information] disclosure or loss of data" and "catastrophic damage to or loss of agency facilities and infrastructure with fatalities to individuals."[68] Borges, speaking about the risks involved in the DOGE cloud set-up, said "you become the quarterback of the data and the referee," as DOGE personnel have apparently been granted administrator status without the supervision of the SSA officials who

[60] 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) at 9.

[61] Borges resigned from his position in August 2025. *Social Security data chief resigns after whistleblower complaint over DOGE data access*, Politico (Aug. 29, 2025) (www.politico.com/news/2025/08/29/social-security-data-chief-resigns-00537974).

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

[63] *Id.*

[64] Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 20255) (Whistleblower disclosure, on file with the Committee).

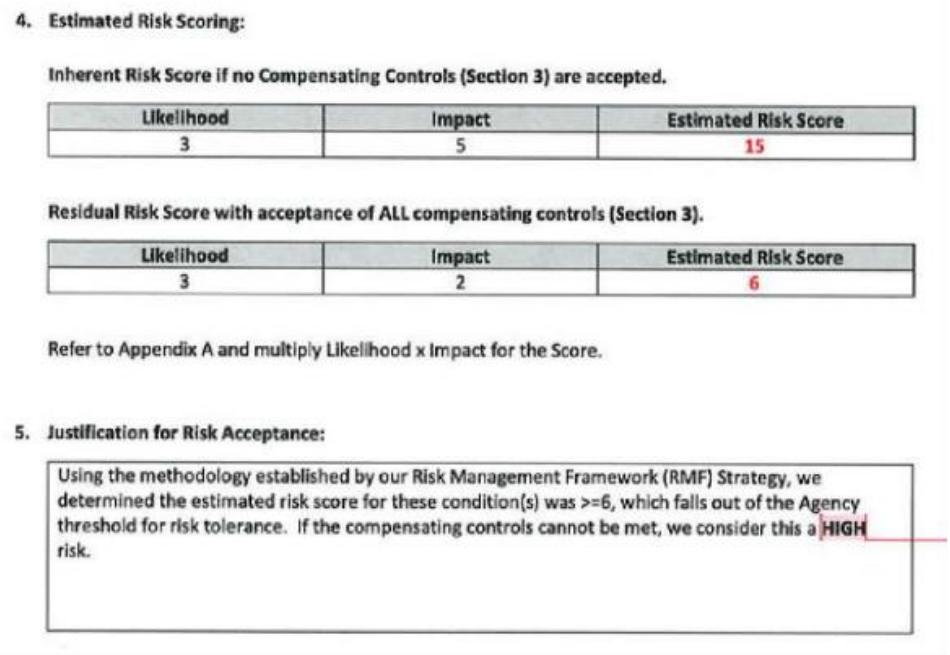
[65] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Assessment* (Feb. 5, 2024) (www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf).

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

[67] *Id.*

[68] *Id.*

otherwise administer all SSA cloud infrastructure and ensure data is secure.[69] Officials did not provide any information as to whether a subsequent risk analysis was ever conducted.



4. **Estimated Risk Scoring:**

Inherent Risk Score if no Compensating Controls (Section 3) are accepted.

Likelihood	Impact	Estimated Risk Score
3	5	15

Residual Risk Score with acceptance of ALL compensating controls (Section 3).

Likelihood	Impact	Estimated Risk Score
3	2	6

Refer to Appendix A and multiply Likelihood x Impact for the Score.

5. **Justification for Risk Acceptance:**

Using the methodology established by our Risk Management Framework (RMF) Strategy, we determined the estimated risk score for these condition(s) was >=6, which falls out of the Agency threshold for risk tolerance. If the compensating controls cannot be met, we consider this a HIGH risk.

Exhibit B. SSA internal risk assessment[70]

It is unclear why such a high-risk project is needed, or why DOGE personnel require the use of live data free from the supervision of agency officials. One whistleblower told staff that the purpose of the database might be to provide free SSN verification for other federal agencies, but circumventing basic safeguards suggests the project may have other purposes.[71]

The disclosures revealed that SSA officials do not have insight into DOGE's work in the cloud environment, including whether they have manipulated or deleted data, or whether they have given any external entities access to the data. In a highly unusual step, the NUMIDENT data uploaded to the cloud environment is considered "production data," meaning that DOGE personnel have the ability to directly manipulate the data (*See* Exhibit C).[72] This is in clear violation of federal data privacy laws, SSA policies for handling sensitive data, and OMB cybersecurity guidance.[73] In other words, according to whistleblowers, DOGE would be able to

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

[70] *Id.* Complete document included in Appendix A.

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

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

[73] Pub. L. No. 113-283 (2014); Pub. L. No. 93-579 (1974); Pub. L. No. 107-347 (2002); OMB Circular A-130; *SSA Information Security And General Privacy Requirements*, Social Security Administration (Accessed Sept. 8, 20255) (www.ssa.gov/oag/acq/SSA%20Information%20Security%20and%20General%20Privacy%20Requirements.pdf).

grant private companies or foreign bad actors access to the data and the agency would not know.[74] Concerns about the database itself are exacerbated by Coristine's involvement. The cybersecurity firm where Coristine was previously an intern was reportedly not willing to risk giving him access to sensitive company information after he leaked information to a competitor.[75] SSA has apparently given him access to the personal data of all Americans. Because of the lack of oversight and controls over the cloud environment, there is increased risk that someone like Coristine, with his personal history, could intentionally give data access to private companies for his own personal gain. The whistleblowers did not share any information to suggest that such a breach had occurred, however one whistleblower also acknowledged that we may never know if data was manipulated, leaked, or stolen because of the secretive nature of the cloud environment DOGE is using and lack of oversight.[76]

From: Cunningham, Joe
Sent: Monday, June 16, 2025 9:21 AM
To: Moghaddassi, Aram; Peltier, Brian
Subject: AWS Admin access
Attachments: RA-AWS Admin access.pdf

Aram/Brian,

The team in Information Security (IS) has been collaborating with the Systems Operations and Hardware Engineering (SOHE) regarding the access request for administrative access to AWS. After a thorough review, we have determined that this request poses a high risk.

The primary concern stems from the inclusion of a replica copy of NUMI in the development environment. NUMI is classified as a High-Value Asset (HVA), and our standard policy prohibits the use of production data in development environments. Additionally, it is important to note that most security exposures and breaches occur within development environments due to reduced control measures and oversight.

Given the high-risk nature of this request, our current policy requires signoff from the Chief Information Officer (CIO) to accept these risks. I have attached our detailed write-up for your review. If you concur with granting this access, I kindly request that you digitally sign the attached document.

Please feel free to reach out if you have any questions or concerns.

Thanks
Joe

Exhibit C. SSA CISO Joe Cunningham tells Moghadassi that SSA policy prohibits the use of production data in such environments given heightened security risks (highlights added)[77]

If compromised, the highly sensitive data that SSA collects and stores would render hundreds of millions of Americans vulnerable to identity theft and imperil vital benefits for programs like Social Security and Medicare, likely far exceeding the devastating impact of the 2015 OPM hack.[78] Since all Americans' data is included in this database – including Members of Congress, former Presidents, Supreme Court Justices, and law enforcement or national security operatives

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

[75] *Recording reveals new details on controversial DOGE employee,* CNN (Feb. 22, 2025) (www.cnn.com/2025/02/21/politics/doge-musk-edward-coristine-invs).

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

[77] Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs (Sep. 8, 2025) (Whistleblower disclosure, on file with the Committee). Complete document included in Appendix A.

[78] The 2015 OPM hack led to the exfiltration of 21.5 million individuals' data. See: "Impact of OPM breach could last more than 40 years", FedScoop (Jul. 10, 2025) (www.fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community/).

whose identities are not public – there could be potentially severe physical security concerns if the database is purposefully or inadvertently leaked.[79] Concerningly, since Coristine in particular has a history of disregard for protecting data at his previous positions, he is a ripe candidate for targeting by a foreign intelligence service or a private company in the U.S. that wishes access to this data.[80]

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.[81] Victims of data breaches face a tangled web of paperwork and outreach to banks, medical providers, government agencies, and others to unwind the harm done by identity thieves. One victim of the 2015 OPM breach, for example, said that his bank account was frozen after someone opened a PayPal account and made large purchases at Best Buy in his name. The experience was "exhausting and frustrating" and just caused "endless explaining."[82] The OPM data breach ultimately impacted 20 million people.[83] Now imagine the unmitigated disaster that a breach of a much larger scale could cause, with potentially hundreds of millions of Americans refuting false Best Buy purchases, tracking down phony PayPal accounts, and otherwise rigorously monitoring and worrying about their credit and identity protection. Credit lending, home and vehicle purchases, and other financial processes would likely grind to a halt nation-wide until other means of identity verification could be secured. Opportunities for bad actors to wreak havoc on the United States would be readily available. This is not a distant hypothetical. According to Mr. Borges, one of his superiors noted the possibility that SSA may need to re-issue SSNs to all who possess one, a potential worse case outcome.[84]

[79] *DOGE's Data Digging at the Social Security Administration Puts Millions of Americans at Risk,* CAP (Apr. 28, 2025) (www.americanprogress.org/article/doges-data-digging-at-the-social-security-administration-puts-millions-of-americans-at-risk/).

[80] *Recording reveals new details on controversial DOGE employee*, CNN (Feb. 22, 2025) (www.cnn.com/2025/02/21/politics/doge-musk-edward-coristine-invs).

[81] Social Security Administration, *Social Security Bulletin: The Story of the Social Security Number* (Vol. 69, No. 2) (July 2009) (www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html#exhibit2).

[82] *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).

[83] *Id.*

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

II. GSA Headquarters

Highlights

- **Staff visited the executive suite of GSA, which was occupied by a handful of DOGE staff and segregated from the rest of the agency by armed security guards.**
- **GSA officials were unable to answer basic questions about which employees were working in the suite, what their roles were, and who at the agency oversees their work. Some officials were clearly seeing parts of the DOGE setup for the first time.**
- **GSA prevented staff from taking photos or interviewing GSA employees during the visit, failed to answer follow-up questions, and refused a staff request for a follow-up visit.**
- **The Acting Administrator does not work out of the Administrator's office – instead, DOGE programmers do amid stacks of laptops of unknown origin.**
- **GSA officials attempted to prevent staff from seeing cloud architecture diagrams in the DOGE workspace.**
- **DOGE has installed a Starlink network at GSA, potentially allowing them to circumvent agency IT oversight as required under OMB guidance and agency policy, and creating a potentially significant cybersecurity risk.**

GSA is an agency at the heart of federal operations, providing essential support services across government. Amid reports of significant policy and personnel changes at GSA, Senate Committee on Homeland Security and Governmental Affairs (HSGAC) Minority Staff (herein after "staff") requested briefings.[85] These requests were routinely ignored or denied.[86]

In May, HSGAC and Environment and Public Works (EPW) Minority staff requested to visit the Agency. On the morning of Wednesday, May 28, 2025, both committees visited GSA with the offices of Senators Paul, Peters, Capito, and Whitehouse, the respective Chairs and Ranking Members of HSGAC and EPW, in attendance.

In a May 27 confirmation email from GSA, officials stated that they would be unable to accommodate any in-person interview requests, including several for individuals that staff would later witness in the building during the tour.[87] The confirmation email also listed a set of strict ground rules that inexplicably cited sections of federal code pertaining to media access in federal buildings, restricted the visit to "approved public spaces," and warned visitors about the

[85] *DOGE Officials Across Government Appear on GSA's Shortlist of Vetted Personnel*, Federal News Network (Apr. 8, 2025) (www.federalnewsnetwork.com/agency-oversight/2025/04/many-doge-officials-appear-on-gsas-security-shortlist-acting-head-says-nobody-working-for-doge-here/); Email from Committee Staff to GSA Staff (Feb. 5, 2025) (on file with Committee).

[86] These include the following: Email from Committee Staff to GSA Staff (Feb. 11, 2025) (on file with Committee); Email from GSA Staff to Committee Staff (Mar. 5, 2025) (on file with Committee).

[87] Email from GSA Staff to Committee Staff (May 27, 2025) (on file with Committee).

consequences for disruptive conduct.[88] This provision does not apply to Congress, and when asked about this specific code citation, officials were unable to provide any information about the applicability of such rules to Senate staff.[89]

On May 28, Senate staff were greeted at the GSA headquarters lobby by Acting Chief-of-Staff Saul Japson, Deputy Associate Administrator for Congressional and Intergovernmental Affairs Mark O'Connell, and members of the Office of Strategic Communications and the Office of Mission Assurance.[90] GSA officials continually promised the tour would demystify DOGE operations at the agency.[91]

Several times, Mr. Japson pointed to GSA's creative use of space to accommodate return to office requirements.[92] Mr. Japson noted that GSA employees must reserve desk space ahead of coming into the office given the scarcity of usable space in the building.[93]

On the sixth floor, however, office occupancy changed drastically. A security guard was posted in a quiet hallway entrance to GSA's executive suite.[94] There, committee staff asked to take photos. GSA officials denied this request, stating that it was prohibited by federal regulation.[95] Staff pointed out that the regulations GSA cited in its email applied to the media, not congressional oversight. However, Mr. O'Connell said he would end the tour unless staff agreed not to take photos.[96] GSA officials were not able to provide a legal citation applicable to Congress.

GSA officials confirmed that a Starlink device was active at the agency but would not permit staff to view it.[97] GSA, like all federal agencies, already has an existing, secure internet service across its campus, raising questions about the duplicative use of this system and potential

[88] GSA would later hold firm on a prohibition on photos and videos but did escort staff to non-public areas, including bedrooms where GSA employees live "intermittently." GSA also asked that both the Majority and Minority limit attendance to two people but ultimately accommodated a larger group when HSGAC Minority offered to schedule additional shifts for the tour or return visits. 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).

[89] 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).

[90] Later, Bob Stafford, the Chief Administrative Services Officer, and other career and non-career staff joined the tour. 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).

[91] 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).

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] Starlink is a satellite internet company owned by Elon Musk; 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).

security vulnerabilities it represents.[98] Officials also could not confirm or comment on who at GSA, outside of the DOGE team, has access to the Starlink network or if the network was secured using existing agency policies.[99]

As of September 2025, it does not appear that any certifications, privacy impact assessments, risk assessments, or continuous monitoring of information sent and received on Starlink networks at GSA have been implemented, as required by the Federal Information Security Modernization Act of 2014, the E-Government Act of 2002, Office of Management and Budget guidance and policy, and internal GSA information technology security policy.[100] Without such monitoring and controls, one whistleblower told HSGAC staff that use of the Starlink network could allow DOGE employees to evade typical agency IT oversight, particularly when it comes to the use of non-GSA devices or interagency data work.[101] HSGAC staff's request to view GSA's security operations center and talk to the Chief Information Security Officer were also denied.[102]

According to public reporting, court documents, and whistleblower reporting, the DOGE teams have actively pursued high levels of access to a multitude of databases with highly sensitive personal information and to the full datasets within them for unknown reasons.[103] One former DOGE individual, Sahil Lavingia, said that the "core group of pre-inauguration engineers joked about how many laptops they had," and that it was "almost like a competition in the sense to have seven, eight different laptops that they would run around with."[104] On the visit, staff

[98] *White House Security Staff Warned Musk's Starlink is a Security*, The Washington Post (June 7, 2025) (www.washingtonpost.com/technology/2025/06/07/starlink-white-house-security-doge-musk/); 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).

[99] 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).

[100] Federal Information Security Modernization Act of 2014, Public Law No. 113-283; Office of Management and Budget, *Managing Information as a Strategic Resource* (Circular No. A-130) (revised July 28, 2016) (www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf); Office of Management and Budget, *Management of Federal High Value Assets* (M-17-09) (Dec. 9, 2016) (obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-09.pdf); Office of Management and Budget, *Policy to Require Secure Connections Across Federal Websites and Web Services* (M-15-13) (June 8, 2015) (obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf); General Services Administration, *GSA Information Technology (IT) Security Policy* (No. 2100.1Q CIO) (Oct. 16, 2024) (www.gsa.gov/directives-library/gsa-information-technology-it-security-policy-16); General Services Administration, *GSA IT General Rules of Behavior* (No. 2104.1C CIO) (Nov. 5, 2025) (www.gsa.gov/directives-library/gsa-information-technology-it-general-rules-of-behavior-4).

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

[102] Email from Committee Staff to GSA Staff (May 27, 2025).

[103] *DOGE staffer who shared Treasury data now has more access to government systems*, NPR (Mar. 31, 2025) (www.npr.org/2025/03/31/nx-s1-5345708/doge-data-access-labor-cfpb-hhs); *Privacy under siege: DOGE's one big, beautiful database*, Brookings (June 25, 2025) (www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/); *DOGE Aims to Pool Federal Data, Putting Personal Information at Risk,* Washington Post (May 7, 2025) (www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/).

[104] *Big Balls' No Longer Works for the US Government,* Wired (June 24, 2025) (www.wired.com/story/big-balls-coristine-doge-resigned-us-government/).

corroborated at least some of these concerns. DOGE workspaces had stacks of laptops on them, and GSA officials were unable to confirm whether all of them were GSA-issued.[105] In one room, cloud infrastructure and enterprise network infrastructure diagrams were drawn on a whiteboard, but GSA officials attempted to block views of it with their bodies.[106]

This poses significant risks and seems to violate the Privacy Act of 1974 and the E-Government Act of 2002, which established safeguards to restrict governmental use and sharing of Americans' sensitive data and required proactive notification to the public when any new programs or technologies are using personally identifiable information.[107] There have been reports that DOGE is working to build one or several "master databases" containing data from multiple government agencies without any concern for data quality or any consideration that data collected for a particular purpose should not be used for an unrelated purpose.[108] Further, the Privacy Act requires agencies to report to HSGAC and the House Committee on Oversight and Government Reform (COGR) when proposing any significant changes to systems of records or computer matching programs.[109] As of the publication of this report, HSGAC has received no such notification relating to DOGE activity at these agencies.

On the sixth floor, just beyond the security entry point, there is an open-concept workspace.[110] On the day of the visit, only one employee was present there: Akash Bobba, the 22-year-old coder and Palantir alumnus who, according to federal judges, has violated federal privacy laws by accessing federal records, including Social Security Administration data.[111]

When congressional staff reached the executive suite corridor, Mr. Japson and Mr. Stafford confirmed that the agency had procured furniture to outfit seven bedrooms for intermittent sleeping.[112] GSA initially indicated staff would be permitted to see all the rooms but

---

[105] 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).

[106] *Id.*

[107] The Privacy Act of 1974, Pub. L. 93-579; The E-Government Act of 2022, Pub. L. 107-347.

[108] *DOGE staffer who shared Treasury data now has more access to government systems*, NPR (Mar. 31, 2025) (www.npr.org/2025/03/31/nx-s1-5345708/doge-data-access-labor-cfpb-hhs); *Privacy under siege: DOGE's one big, beautiful database*, Brookings (June 25, 2025) (www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/); *DOGE Aims to Pool Federal Data, Putting Personal Information at Risk,* Washington Post (May 7, 2025) (www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/).

[109] The Privacy Act of 1974, Pub. L. 93-579, Sec. 552a(o).

[110] 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).

[111] *DOGE Says It Needs to Know the Government's Most Sensitive Data, But Can't Say Why,* NPR (Mar. 26, 2025) (www.npr.org/2025/03/26/nx-s1-5339842/doge-data-access-privacy-act-social-security-treasury-opm-lawsuit); 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).

[112] 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).

later recanted. Ultimately, Senate staff saw just one bedroom in the executive suite corridor, perfectly tidied, with one queen bed, a wardrobe and a big screen TV.[113]

GSA officials leading the tour seemed unfamiliar at times with the executive suite space or what it would look like on the day of the congressional staff visit.[114] In particular, when staff were in the Administrator's office, Mr. Japson was initially surprised when staff discovered the makeshift bedroom directly adjoining the Administrator's suite and he remarked, "What's in there?" The room contained two twin beds on the floor, with sheets unmade.[115]

In the GSA Administrator's office itself, staff observed an estimated 10 workstations filling the wood-paneled office.[116] GSA officials told staff that the Acting Administrator had been moved to the seventh floor.[117] The setup was markedly different from the other office spaces viewed at GSA. Workstations were furnished with wide-screen monitors, stacks of laptops (staff estimated 8 - 10 per person) and multiple cellphones on the desks.[118] When asked, GSA could not confirm whether the laptops were GSA-issued, nor could they provide details on GSA's policy for bringing non-GSA equipment into the building for usage on GSA networks.

When HSGAC staff asked GSA what the individuals were doing and who they report to, GSA officials only said, "they are GSA employees" and offered no further details.[119] Staff pressed for clarification on what agency department the employees belonged to, given that they had displaced the Administrator, Chief of Staff, and other senior officials. Officials only repeated that these individuals were "GSA employees." HSGAC staff asked if they were implementing the DOGE Executive Orders but GSA officials could not answer this question. Staff asked if any of the employees were detailees but GSA could not answer the question.[120]

Staff were rebuffed from seeing additional spaces, including the remaining bedrooms. At one point, GSA officials said they did not have the key to open a locked room that had windows

[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] While touring other sections of GSA HQ, GSA staff were able to identify other offices, federal employees, and the work being done to HSGAC staff. It is unclear why on the sixth floor, GSA staff could not or would not offer information other than, "They are GSA employees." 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).
[120] The following exchange occurred at this point:
Mr. Japson: They're all GSA employees… we'll have to get back to you.
HSGAC Staffer: When you say you'll get back to us on the DOGE information, do you all just not know who's on the agency DOGE team, or are you not sure what you can share with us right now?
Mr. O'Connell: I've been here two weeks, I can get you the information, I'm more than happy to.
GSA has yet to provide staff with this information. 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).

covered with black paper, trash bags, and tape.[121] When staff asked why the most senior officials in offices charged with building management and security could not open an office door, GSA could not provide an answer. GSA staff seemed not to know what was in the room themselves. HSGAC staff received several different explanations on what was inside.[122]

GSA officials made repeated commitments to respond to staff questions after the visit. However, GSA has yet to respond to follow-up questions sent by HSGAC and EPW Minority staff on June 2, 2025.[123] Mr. O'Connell also assured staff that a follow-up visit would be welcomed if there were further questions.[124] Staff requested a follow-up visit (sent June 25, 2025) to see the other sleeping spaces on the sixth floor, Starlink equipment, and to take photographs. Mr. O'Connell initially refused, saying only that "GSA is not able to facilitate a tour at this time."[125]

Staff continued to reassert Congress' constitutional duty to conduct oversight but did not hear anything from GSA until staff observed GSA preparing to meet with HSGAC Majority.[126] However, Mr. O'Connell noted that staff would now need an official letter from the Ranking Member to return, further breaking with oversight norms.[127] At the end of July, public reporting indicated that the furniture, bedding and children's' toys for DOGE's living and sleeping spaces had been disassembled and moved.[128] GSA declined to provide further details on what this move meant for future plans for DOGE and their work and living setup at the agency.[129]

---

[121] 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); GSA officials had earlier obtained the key to open the door to the washer/dryer unit that had been installed but refused to do the same for this room.

[122] The following exchange occurred at this point:

Mr. Japson: It's like a storage room.

HSGAC Staffer: Storage for what?

Mr. Japson: For multiple things...whatever needs storing.

Despite not providing any indication that the room contained sensitive materials, officials refused to obtain the key to open it. 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).

[123] Email from Committee Staff to GSA Staff (June 2, 2025).

[124] 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).

[125] Email from Committee Staff to GSA Staff (June 25, 2025); Email from GSA to Committee Staff (June 26, 2025).

[126] Email from Committee Staff to GSA Staff (June 25, 2025).

[127] 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); On July 15, Mr. O'Connell called staff noting photos would be allowed in a return visit conditional on a letter from the Senator. However, when staff asked if the 6th floor set-up was the same, he noted: "expect to see a lot of changes." When pressed for particulars, O'Connell said staff would need to "see for [them]selves." O'Connell also declined to provide details on why this happened and what this meant for DOGE's operations at the agency, noting "that's above my pay grade." Call from Mark O'Connell to Committee Staff (July 23, 2025).

[128] *Photos: Here Are the Piles of Used Bedding and Children's Play Sets Left Near DOGE's Old Offices*, WIRED, (July 23, 2025)(www.wired.com/story/photos-bedding-childrens-play-sets-doge-old-offices/).

[129] Call from Mark O'Connell to Committee Staff (July 23, 2025).

III. OPM

Highlights

- **Throughout the tour, OPM leadership were unaware of or unwilling to share with Congress basic details about the agency's staffing and organization.**
- **OPM officials denied the presence of DOGE staff at the agency, contradicting the federal government's own statements in federal court.**
- **OPM officials claimed that "no shortcuts were made" to give DOGE personnel access to agency databases and that all data access was compliant with agency policy, contradicting court findings.**
- **Like at GSA, staff observed largely empty office spaces in workspaces set aside for DOGE staff, and officials failed to confirm their presence at the agency or account for their whereabouts.**
- **OPM officials would not allow staff to conduct an oversight visit without the participation of majority staff, in contravention of congressional oversight authority.**

OPM was one of the earliest targets of DOGE, given the agency's role as the chief human resources agency for the federal government. In this capacity, OPM maintains systems of records containing sensitive information for millions of Americans, including past and current federal employees and their family members. This includes social security numbers, health care information, and banking information. OPM systems also contain security clearance data, including for federal employees in sensitive undercover roles.[130] Individuals do not have the choice to opt out of having their information stored in OPM systems, including for some systems that retain information permanently, even after individuals stop working for the federal government.[131]

A former OPM employee told the committee that, even before the inauguration, the incoming administration expressed a "strong interest" in government-wide email servers and centralizing communications.[132] Additionally, this individual told the committee that the incoming CIO, Greg Hogan, had asked OPM staff whether they could deploy an AI system in an off-cloud environment, an environment that would allow for less agency oversight and fewer safeguards.[133] Similar to issues HSGAC staff encountered at SSA, this raises questions of whether the agency was trying to circumvent agency oversight and privacy policies. Soon after inauguration, OPM began consolidating employee data and email addresses to send mass emails through HR[@]OPM[.]gov in contravention of existing communication practices and without

[130] U.S. Office of Personnel Management, Privacy Policy Page (www.opm.gov/information-management/privacy-policy/#url=SORNs) (Accessed Sept. 8, 2025).

[131] *Id.*

[132] Interview with a former OPM employee by Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Disclosure, on file with the Committee).

[133] *Id.*

public notice.[134] On January 28, the DOGE team at OPM announced the deferred resignation program, also known as the "Fork in the Road" email, offering workers pay through September if they agreed to resign.[135] In February, the same email address requested all federal employees, including some non-executive branch employees in the judiciary and at the Government Accountability Office (GAO), reply with five bullets of what they accomplished in the last week.[136] The OPM DOGE team then reportedly used AI to analyze responses to this email.[137]

Senate Committee on Homeland Security and Governmental Affairs (HSGAC) Minority Staff (herein after "staff") initiated the visit request only after OPM failed to respond to multiple oversight requests for documents and information related to these efforts.[138] When HSGAC staff first requested this visit, OPM's Deputy Chief of Staff, Christina Bonarrigo Villamil, told staff that OPM would not accommodate a visit unless HSGAC Majority staff attended as well, a requirement that is without precedent and unsupported by law.[139]

OPM's DOGE team was a key focus of the committee's oversight, based on reports and court findings of their legal violations. From staff's first interactions with OPM, their political leadership were determined to deny any existence of DOGE at the agency.

While setting up the committee's visit, Ms. Bonarrigo Villamil told staff over email that "OPM does not have 'DOGE' team members."[140] Her claim is contradicted by OPM's own staff in court documents and public reporting.[141] It also contradicts President Trump's Executive

---

[134] *Federal workers start to get a new email demanding their accomplishments*, Associated Press (February 28, 2025) (www.apnews.com/article/elon-musk-donald-trump-doge-federal-workers 53e59ab9a4bc52ce5553e0e83bb8cc7b).

[135] Office of Personnel Management*, Deferred Resignation Email to Federal Employees* (Jan. 28, 2025) (www.opm.gov/fork/original-email-to-employees/).

[136] *DOGE Email Throws Federal Agencies into Chaos and Confusion,* Wired (Feb. 22, 2025) (www.wired.com/story/doge-elon-musk-federal-workers-chaos-confusion/).

[137] *DOGE Will Use AI To Assess the Responses of Federal Workers Who Were Told to Justify Their Jobs Via Email*, NBC News (Feb. 24, 2025) (www.nbcnews.com/politics/doge/federal-workers-agencies-push-back-elon-musks-email-ultimatum-rcna193439).

[138] These include the following: a March 24, 2025, letter requesting documents and information regarding DOGE access to agency databases and systems; a February 7, 2025, letter requesting documents and information regarding the "Fork in the Road" email and the deferred resignation program, cosigned with Senator Blumenthal; and another February 7, 2025, letter urging OPM to pause all activity on HR@OPM.gov and related servers, complete a third-party audit of the systems for potential malicious activity, and provide additional information.

[139] Email from Christina Bonarrigo, Deputy Chief of Staff at the Office of Personnel Management to Senate Committee on Homeland Security and Governmental Affairs Staff (June 20, 2025)("We are already going out of our way to accommodate your unusual request. If you would like to tour OPM, you will need to be with majority staff as well… Until then, we will not be providing anyone outside of OPM officials inside of our building.").

[140] Email from Christina Bonarrigo, Deputy Chief of Staff at the Office of Personnel Management, to Senate Committee on Homeland Security and Governmental Affairs Staff (June 20, 2025).

[141] Email from Christina Bonarrigo, Deputy Chief of Staff at the Office of Personnel Management, to Senate Committee on Homeland Security and Governmental Affairs Staff (June 20, 2025)("OPM does not have 'DOGE' team members here. We do not have any detailees from USDS either. Everyone here is an OPM employee"); *Musk's DOGE agents access sensitive personnel data, alarming security officials,* Washington Post (Feb. 6, 2025) (www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/); *American Federation of Government Employees v. U.S. Office of Personnel Management*, No. 25 CV 1237, 79 (S.D.N.Y. June 9, 2025) (order and opinion granting preliminary injunction)("The administrative record reflects

Order (EO), which mandates that "each Agency Head shall establish within their respective Agencies a DOGE Team of at least four employees."[142] When pressed, Ms. Bonarrigo Villamil told staff that OPM did have, at one time, two employees working under the EO.[143] This is also incorrect. Department of Justice attorneys representing OPM in official court documents have agreed to a definition of "DOGE Agents" that includes nearly 20 individuals at OPM.[144]

On June 20, 2025, Majority and Minority staff from HSGAC and the Senate Committee on Appropriations visited OPM Headquarters at 1900 E St NW, Washington, D.C.[145] The visit was led by Ms. Bonarrigo Villamil and Greg Hogan, OPM's Chief Information Officer.[146] OPM did not comply with HSGAC Minority's request for staff to meet with any individual in at least 10 different offices, including any member of OPM's DOGE team, and the visit was accompanied by a pair of armed guards.[147]

Throughout the visit, staff encountered very few OPM employees working in person. In the open-concept wing of the fifth floor for the Office of the Chief Information Officer (OCIO), staff counted fewer than a dozen employees.[148] According to the Office of Personnel

---

that, beginning on January 20, OPM gave administrative access to its data systems to seventeen individuals working on the DOGE agenda, as well as to Ezell, Hogan, and Scales.").

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

[143] Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[144] Letter from David Farber, Assistant United States Attorney, Department of Justice, to The Honorable Denise J. Cote, United States District Judge in No. 25 Civ. 1237 (June 27, 2025). In a FOIA response to the Project on Government Oversight in May, OPM also claimed several individuals as OPM employees who are known DOGE affiliates.

[145] A pair of armed security guards accompanied the tour party throughout the visit. When asked, guards said this was not typical but that they needed the additional staff to support the size of the group. Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[146] Greg Hogan was previously a Vice President at an autonomous driving technology startup backed by the venture-capital firm Andreessen-Horowitz. The firm's co-founder, Marc Andreessen has described himself as an "unpaid volunteer" for DOGE, and the Trump Administration's pick for OPM Director, Scott Kupor, was one of the first employees at the firm. Andreessen Horowitz and Marc Andreessen have close business ties with Elon Musk and have support several of his companies. Staff understand that Mr. Hogan has left OPM as of September 2025. *DOGE Agent: Greg Hogan*, Revolving Door Project (Mar. 4, 2025) (therevolvingdoorproject.org/greg-hogan-doge-agent/); *Elon Musk Isn't the Only Tech Leader Helping Shape the Trump Administration*, Washington Post (Jan. 13, 2025) (www.washingtonpost.com/politics/2025/01/13/andreessen-tech-industry-trump-administration-doge/); Andreessen Horowitz, About: Scott Kupor (Accessed Sept. 8, 2025) (a16z.com/author/scott-kupor/); *Elon Musk's xAI Raises $6 Billion in New Funding,* The New York Times (Dec. 24, 2024) (www.nytimes.com/2024/12/24/technology/elon-musk-xai-funding.html); *DOGE Agent: Marc Andreessen*, Revolving Door Project (Feb. 21, 2025) (therevolvingdoorproject.org/doge-andreessen-marc/); Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[147] A pair of armed security guards accompanied the tour party throughout the visit. When asked, guards said this was not typical but that they needed the additional staff to support the size of the group. Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[148] OPM later clarified that most OCIO employees are in Macon, Georgia and Boyers, Pennsylvania.

Management *Congressional Budget Justification Fiscal Year 2026*, the Office of the Chief Information Office has around 390 full time equivalent staff.[149]

Throughout the visit, OPM was unwilling to share basic information about agency operations and DOGE, and often contradicted information that is public in a class action civil suit, *American Federation of Government Employees, AFL-CIO, et a. v. U.S. Office of Personnel Management, et al.* Only 11 days prior to the Committee site visit, United States District Judge Denise Cote granted a preliminary injunction barring DOGE access to OPM databases and systems based on its finding that OPM had "violated the law and bypassed its established cybersecurity practices" in allowing DOGE access.[150] During the visit, OPM seemed at times unaware of the details of the injunction or unwilling to even concede that OPM has a DOGE team in the first place, raising concerns about their compliance with the court's directives.[151]

In District Judge Cote's June 9 order granting a preliminary injunction in the case, she writes, "the administrative record reflects that, beginning on January 20, OPM gave administrative access to its data systems to seventeen individuals working on the DOGE agenda, as well as to [Chuck] Ezel, [Greg] Hogan, and [Amanda] Scales."[152] Mr. Hogan himself provided at least two official declarations in the case in which he refers repeatedly to "DOGE affiliates" and "DOGE engineers." The administrative record in the case includes a lengthy email chain started on January 27, 2025, by Acting OPM Administrator Ezell titled, "Getting DOGE Engineers access."[153] Mr. Hogan is a participant in that chain. Despite all of this

[149] U.S. Office of Personnel Management, *Congressional Budget Justification Fiscal Year 2026* (Mar. 2025) (www.opm.gov/about-us/fy-2026-congressional-budget-justification/fy-2026-congressional-budget-justification.pdf) (In row 12 of the table found on page 18, the Office of the Chief Information Officer is said to have 389.2 Full Time Equivalent [FTE] employees.).

[150] *American Federation of Government Employees v. U.S. Office of Personnel Management*, No. 25 CV 1237, 3 (S.D.NY June 9, 2025)(order and opinion granting preliminary injunction).

[151] Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[152] *American Federation of Government Employees v. U.S. Office of Personnel Management*, No. 25 CV 1237, 48 (S.D.NY June 9, 2025) (order and opinion granting preliminary injunction).

[153] Appendix - Administrative Record - OPM-000001-OPM-000235 (Apr. 23, 2025), *American Federation of Government Employees v. U.S. Office of Personnel Management,* S.D.N.Y (No. 25 CV 1237) at 28. The court writes that "DOGE affiliates" were "identified by Hogan," in an effort to complete an audit of their data access. That audit consisted of "20 DOGE-affiliated individuals who were granted access to DOGE systems." The court also cites the following: "For example, in his February 19 declaration, Hogan explained that, in addition to himself, the five DOGE Engineers were engaged with implementing the DOGE Executive Order." The court also states: "DOGE obtained broad access to systems containing PII without an adequate showing of need, in contravention of both the Privacy Act and OPM's regular procedures and security standards. It is a fair inference that the DOGE Defendants instructed Ezell to expedite access to OPM systems for DOGE agents, leading to a '911-esque call' with OPM staff. Ezell and others at OPM have described the relevant individuals as 'DOGE Engineers' and 'DOGE employees,' and Hogan has identified them as 'DOGE affiliates.' Many of the DOGE agents have done work on behalf of DOGE at multiple agencies, and at least some of them are likely to be USDS employees, or at least not OPM employees." *American Federation of Government Employees v. U.S. Office of Personnel Management*, No. 25 CV 1237, 40 ,79, 93 (S.D.NY June 9, 2025) (order and opinion granting preliminary injunction).

documentation, Mr. Hogan, Ms. Bonarrigo Villamil, and other OPM officials continued to insist to Senate staff in person that the reports about DOGE are untrue or overblown by the media.[154]

When staff indicated they wanted to better understand data access for these individuals – despite OPM's failure to acknowledge their existence – one OPM official interjected to say that OPM followed all procedures and "made no short cuts" for anyone.[155] He continued that statements that OPM gave expedited access to people without proper vetting are untrue.[156] He said there was no political pressure and no favors or shortcuts given.[157] This directly contradicts statements in Judge Cote's preliminary injunction opinion and order, stating that expedited access was given based on a "911-esque call" requesting that a "political team" composed of six individuals be given access to OPM systems.[158] The court states, "The gravity of the gaps in the onboarding process is amplified by the sweeping access OPM gave to its data systems."[159] OPM failed to take additional actions when news reports indicated that a DOGE employee was "fired from a cybersecurity firm after, according to that firm, 'an internal investigation into the leaking of proprietary information that coincided with his tenure."[160]

When asked about the injunction, Mr. Hogan again responded that there is so much deception in the media and that a lot of these stories are based off of screenshots that were sent to the press.[161] Staff corrected Mr. Hogan that the examples were not media reports but language from OPM itself in the injunction.[162] When staff asked Mr. Hogan if OPM had acted in response to the preliminary injunction he said they had not made any changes, removed access or asked any individuals to delete copies – despite the direct court order.[163] When staff asked if he would know if any of these changes had been made, he said yes.[164]

---

[154] Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *American Federation of Government Employees v. U.S. Office of Personnel Management,* No. 25 CV 1237, 49 (S.D.NY June 9, 2025)(order and opinion granting preliminary injunction)("A chronology of the disclosure of OPM systems to individuals working on the DOGE agenda begins on the evening of January 20, the day of President Trump's inauguration, with a "911-esque call" requesting that a "political team" composed of six individuals be given access to OPM systems. OPM's IT staff did not receive the usual documentation for this request until more than a week later. Internal emails indicate that, pursuant to this emergency request, OPM granted Ezell, Hogan, Scales, OPM-3, OPM-5, and OPM-7 administrative access to USAJOBS, USA Staffing, and USA Performance.").

[159] *American Federation of Government Employees v. U.S. Office of Personnel Management*, No. 25 CV 1237, 61 (S.D.NY June 9, 2025) (order and opinion granting preliminary injunction).

[160] *Id*.

[161] 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).

[162] *Id.*

[163] *Id*.

[164] *Id*.

On this floor, Mr. Hogan explained that staffing at the OCIO was reduced from 1,010 to 400 employees in a matter of months.[165] When asked about this drastic staff cut, Mr. Hogan did not say whether he reviewed all positions they terminated and could not identify the number of terminated employees OPM had to rehire.

Finally, OPM showed staff the director's suite, which was mostly vacant. In the entire director's suite, it appeared that only one of the empty offices was occupied; the office of James Sullivan, OPM's Chief of Staff.[166] When asked whether Mr. Sullivan was part of DOGE, Ms. Bonarrigo Villamil replied "he is a political appointee."[167] Again, Ms. Bonarrigo Villamil's statement contradicted the court's findings that identified Mr. Sullivan as a "DOGE associate."[168]

In this suite, OPM leadership had difficulty answering a series of basic questions about the agency's organization and staffing – again raising concerns whether they did not know how the agency was organized or were unwilling to tell staff. For example, HSGAC Minority asked where the Privacy Office was and neither the Deputy Chief of Staff nor the CIO knew where the Privacy Office was located or the fact that it had been relocated under the Office of the General Counsel.[169] The Privacy Office should be involved in Privacy Impact Assessments (PIAs) for all new technology and training on privacy policies. In fact, the PIA that OPM belatedly completed for the GWES was the first not to be signed by the Chief Privacy Officer; instead it was signed by Mr. Hogan.[170] When asked about the Office of Procurement at OPM, Ms. Bonarrigo said that "of course" there was one – despite public reports indicating that OPM had stated in internal emails that it had conducted a "complete reduction in force" in that office and that "all new procurement actions, contract modifications, and ongoing solicitations are effectively stalled until alternative solutions are identified.[171] OPM has since clarified to staff that "Matt M.", the Deputy Director and Head of Contracting Authority in the Office of Procurement Operations, is the lead on OPM procurement, but that OPM has transferred most of its procurement to GSA.[172]

The final topic discussed was personnel at OPM. Specifically, staff asked whether and how many detailees from other agencies were at OPM, and whether OPM had details out to other agencies. Mr. Hogan responded that he was not aware of any and Ms. Bonarrigo Villamil said she was not sure.[173] HSGAC staff interjected that their responses were confusing and asked the

---

[165] *Id.*

[166] *Id.*

[167] *Id*.

[168] *Id*.

[169] *Id.*

[170] Interview with a former OPM employee by Senate Committee on Homeland Security and Governmental Affairs (Accessed Sept. 8, 2025) (Disclosure, on file with the Committee).

[171] *Sweeping Terminations in OPM's Office of Procurement Operations Have Fully Halted Agency Contracting Business and Are Likely to Increase OPM's Operational Risks, an Internal Email Reads,* Nextgov (Feb. 25, 2025) (www.nextgov.com/people/2025/02/opm-procurement-processing-fully-halted-following-agency-layoffs-internal-email-says/403263/).

[172] Email from Christina Bonarrigo, Deputy Chief of Staff at the Office of Personnel Management, to Senate Committee on Homeland Security and Governmental Affairs Staff (September 23, 2025).

[173] Office of Personnel Management, Site Visit with Senate Committee on Homeland Security and Governmental Affairs and Senate Appropriations Subcommittee on Financial Services and General Government (June 20, 2025).

question again. Ms. Bonarrigo Villamil said that there were "maybe" detailees at OPM.[174] She said that they would have to get back to the Committee with an answer. In a subsequent email to staff, officials claimed to staff that "there is no such thing as DOGE personnel."[175]

V. CONCLUSION

Even as DOGE personnel begin to leave government, it remains unclear what these individuals have done with the sensitive data they have had access to, including whether they have copied it to non-government devices for personal use or whether they have inappropriately manipulated or erroneously removed data. The data these individuals have accessed would be valuable not only to foreign adversaries and bad actors, but also to private companies looking to gain an edge on competitors. DOGE's actions not only put every American's most sensitive information at risk, they also make our government and financial institutions vulnerable to large-scale disruption. Importantly, when DOGE individuals leave government, they can no longer be compelled by federal Inspectors General to comply with oversight investigations. They will still be liable for any legal violations, but this administration is unlikely to pursue accountability. The time for transparency around their roles and actions is now.

The Administration must take the following actions:

1. Immediately shut down the new cloud environment at SSA that contains NUMIDENT data.

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.

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.

4. Release information about the data access privileges of DOGE personnel.

5. Release the identities, titles, and position descriptions for all personnel whose principal mission is implementing Executive Orders 14158, 14210, 14219 and 14222.

6. Ensure all agency personnel are subject to consistent and/or appropriate trainings, policies, and restrictions.

7. Relevant Inspectors General must conduct a comprehensive audit of access to sensitive data systems at these agencies.

---

[174] *Id.*

[175] Email from Christina Bonarrigo, Deputy Chief of Staff at the Office of Personnel Management, to Senate Committee on Homeland Security and Governmental Affairs Staff (September 23, 2025).

APPENDIX A

Production from Whistleblower to Senate Committee on Homeland Security and Governmental Affairs on Sept. 3, 2025

Borges, Chuck

From: Cunningham, Joe
Sent: Monday, June 16, 2025 9:21 AM
To: Moghaddassi, Aram; Peltier, Brian
Subject: AWS Admin access
Attachments: RA-AWS Admin access.pdf

Aram/Brian,

The team in Information Security (IS) has been collaborating with the Systems Operations and Hardware Engineering (SOHE) regarding the access request for administrative access to AWS. After a thorough review, we have determined that this request poses a high risk.

The primary concern stems from the inclusion of a replica copy of NUMI in the development environment. NUMI is classified as a High-Value Asset (HVA), and our standard policy prohibits the use of production data in development environments. Additionally, it is important to note that most security exposures and breaches occur within development environments due to reduced control measures and oversight.

Given the high-risk nature of this request, our current policy requires signoff from the Chief Information Officer (CIO) to accept these risks. I have attached our detailed write-up for your review. If you concur with granting this access, I kindly request that you digitally sign the attached document.

Please feel free to reach out if you have any questions or concerns.

Thanks
Joe

"Success is not final, failure is not fatal: it is the courage to continue that counts."
Winston Churchill

Joe Cunningham
Acting CISO/Acting Associate Commissioner
Office of Information Security (OIS)
Office of Chief Information Officer (OCIO)
Office: 410-965-3098
Cell: 410-818-6440

RISK ACCEPTANCE REQUEST FORM

This form is used to justify a risk acceptance of a known deficiency that does not fit the standard policy/technical waiver processes. The component stakeholder or designee is responsible for writing the justification and completing the form. Depending on risk level, the CIO, CISO, or SRB may approve/deny this request.

Title: AWS – Admin Access **Date:** 06/12/25

1. **Description of the Control Deficiency:**

Title/Description: AWS Admin Access

Scope: Developers are requesting AWS admin access to expedite development timeframes.

The Office of Information Security was requested to provide a security risk assessment for SSA developers to have admin access to their own Virtual Private Cloud (VPC) within the SSA Amazon Web Services – Agency Cloud Infrastructure (AWS-ACI).

The CIO/OSOHE/Division of Infrastructure Services (DIS) manages the AWS-ACI. Each project that works within AWS receives their own VPC and associated AWS accounts. Per agency policy and the ACI System Security Plan (SSP), DIS is required to be admins on the VPC to ensure agency policy and federal regulatory requirements are followed.

2. **Description of Inherent Risk:**

The CIO/OSOHE/Division of Infrastructure Services (DIS) manages the AWS-ACI. Each project that works within AWS receives their own VPC and associated AWS accounts. Per agency policy and the ACI System Security Plan (SSP), DIS is required to be admins on the VPC to ensure agency policy concerning least privilege and federal regulatory requirements are followed.

OIS noted the following risks with bypassing the DIS admin policy:

1. **The VPC/project does not have an Authority To Operate (ATO).** Per Federal Information System Modernization Act (FISMA), and Office of Management and Budget (OMB) Circular A-130, all federal information systems must receive an ATO which ensures NIST security controls are in place and the Authorizing Official (AO) has accepted all residual risks. With the lack of centralized management of security controls that would typically be inherited by the management of the DIS team, we have no documentation on how those controls will be satisfied. Most importantly, NIST Security Controls AC-5 (Separation of Duties) and AC-7 (Least Privilege) which ensure checks and balances are in place.

2. **Production data could be used.** AWS – ACI is an extension of the SSA network, any type of SSA data to include production data and PII could be imported into this VPC. At the time of this assessment, it was noted in some meetings that developers wished to import the SSA NUMIDENT file into this environment. The SSA NUMIDENT is considered a High Value Asset

1

(HVA) and unauthorized access to the NUMIDENT would be considered catastrophic impact to SSA beneficiaries and SSA programs

3. **Sensitive data could be made public.** With admin access, developers will be able to create publicly accessible services (e.g, s3 buckets, internet based APIs, etc.). Currently this is tightly controlled by DIS.

4. **Developers can initiate any AWS service.** Only FedRAMP authorized AWS services are allowed per agency policy and DIS manages what services can be used.

3. Description of Compensating Controls:

While OIS recognizes the developer's request for an uninhibited development environment, we recommend the following based on the risks above:

1. Production data should not be used.

2. Continued participation with DIS to ensure security safeguards and agency policy is followed.

3. Work toward a full Authority To Operate (ATO) to ensure all NIST SP 800-53 controls and risks are documented, per FISMA.

4. Estimated Risk Scoring:

Inherent Risk Score if no Compensating Controls (Section 3) are accepted.

Likelihood	Impact	Estimated Risk Score
3	5	15

Residual Risk Score with acceptance of ALL compensating controls (Section 3).

Likelihood	Impact	Estimated Risk Score
3	2	6

Refer to Appendix A and multiply Likelihood x Impact for the Score.

5. Justification for Risk Acceptance:

Using the methodology established by our Risk Management Framework (RMF) Strategy, we determined the estimated risk score for these condition(s) was >=6, which falls out of the Agency threshold for risk tolerance. If the compensating controls cannot be met, we consider this a **HIGH** risk.

Commented [HS1]: @Harkness, Steven Risk score of 15 is High, not Very High,

2

6. **Additional Remarks:** Provide any other comments or supporting material in support of request:

********** CISO/CIO Decision/Approval **********

3

Due to the HIGH/VERY HIGH risk scenarios to SSA security posture, the Authorizing Official for the ACI environment (the SSA CIO) needs accept this risk as required by FISMA, FedRAMP, SSA Policy and the implementation of the Risk Management Framework process and procedure at SSA.

Approval of this request with **acceptance** of compensating controls (Box 3).

OIS CISO:	**Printed Name:**	**Date:**

AO/CIO:	**Printed Name:**	**Date:**

If Request Denied, include comments below:

Approval of this request with **no acceptance** of compensating controls (Box 3).

OIS CISO:	**Printed Name:**	**Date:**

AO/CIO:	**Printed Name:**	**Date:**

If Request Denied, include comments below:

Appendix A

The Office of Information Security (OIS) scores risk based on 5-point likelihood and impact scales as noted below in Table 1 and 2. Refer to Table 3 for combined risk score.

Table 1: Likelihood and Impact Scales

Likelihood Scale	Likelihood Score	Impact Scale	Impact Score
Very Low: <10% chance of occurrence	1	Very Low: **negligible** adverse effect	1
Low: 10% to 35% chance of occurrence	2	Low: **limited** adverse effect	2
Medium: 35% to 65% chance of occurrence	3	Medium: **serious** adverse effect	3
High: 65% to 90% chance of occurrence	4	High: **severe** adverse effect	4
Very High: >90% chance of occurrence	5	Very High: **catastrophic** adverse effect	5

Table 2: Impact Definitions

Impact Level	Description
Very low	Event could be expected to have a **negligible** adverse effect on organizational operations, agency reputation, organizational assets, individuals, and other organizations. Event can be managed with routine activities. Could lead to immaterial audit findings.
Low	Event could be expected to have a **limited** adverse effect on organization operations, agency reputation, organizational assets, individuals, and other organizations. Event examples include, but not limited to: (i) minor operational impact without business interruption; (ii) minor embarrassment, but no harm to image and reputation; (iii) no instances of PII disclosure or unauthorized systems access; (iv) no damage/ injury to agency facilities, infrastructure or individuals; and (v) compliance or control findings that could escalate to a reportable control deficiency at the Component level (e.g. Notice of Finding and Recommendation (NFR), Management Letter item, and/or OIG/GAO report finding).
Medium	Event could be expected to have a **serious** adverse effect on organization operations, agency reputation, organizational assets, individuals, and other organizations. Event examples include, but not limited to: (i) moderate operational impact with minimal business interruption; (ii) moderate embarrassment with negative customer/media attention (days); (iii) any instances of PII disclosure or unauthorized systems access; (iv) significant damage/injury to agency facilities, infrastructure or individuals; and (v) compliance or control findings that could escalate to a significant deficiency at the agency level.
High	Event could be expected to have a **severe** adverse effect on organization operations, agency reputation, organizational assets, individuals, other organizations, or the Nation. Event examples include, but not limited to: (i) unacceptable operational impact with short-term business interruption; (ii) major embarrassment with significant, negative customer/media attention (weeks); (iii) extensive PII disclosure, unauthorized systems access, or compromised data; (iv) major damage to or loss of agency facilities and infrastructure with fatalities to individuals; and (v) compliance or control findings that are pervasive and could escalate to a material weakness at the agency level.

Very High	Event could be expected to have a **catastrophic** adverse effect on organizational operations, agency reputation organizational assets, individuals, other organizations, or the Nation. Event examples include, but not limited to: (i) large and unacceptable operational impact with long-term business interruption; (ii) very significant harm to agency image with extreme, negative customer/media/congressional attention (months); (iii) widespread PII disclosure or loss of data; (iv) catastrophic damage to or loss of agency facilities and infrastructure with fatalities to individuals; and (v) compliance or control findings that result in a negative audit opinion.

The risk score is the product of the likelihood score multiplied by the impact score.

Table 3 Risk Score (Table pulled from Cyber Risk Management Strategy, June 2022.)

Likelihood	Level of Impact				
	Very Low	Low	Medium	High	Very High
Very High	5	10	15	20	25
High	4	8	12	16	20
Medium	3	6	9	12	15
Low	2	4	6	8	10
Very Low	1	2	3	4	5

Source: Cybersecurity_Risk_Management_Strategy_v2.2_FINAL_06142022ciso.pdf (ssa.gov)

APPENDIX B

Additional details about the sixth floor of GSA from the Committee Staff site visit:

In an office labeled "Chief of Staff," there was a large ping-pong table set up along with a sofa and a whiteboard with cloud computing architecture diagrams scribbled on it.[1] Bedrooms outfitted with IKEA furniture occupied most of the executive suite, including an adjoining room on the Administrator's office that is normally the Administrator's dining room.[2] A kitchen included a dedicated fridge stocked with Celsius energy drinks and Muscle Milk.[3] The windows in one room were crudely covered with black trash bags.[4] Many other conference rooms and offices in the executive suite stood empty.

GSA officials told staff that as far as they were aware, these rooms were not serving as the primary residence of any GSA employee.[5] However, the unstaged bedroom in the Administrator's dining room showed signs of long-term use.[6] The twin beds were unmade. Smartphones, tangles of cables, a hot plate for cooking, and what appeared to be small personal items surrounded them on the floor and nearby ledges. On the floor next to one bed was a large computer console that was covered with a fleece blanket.[7] Mr. Japson was unable to identify whether this computer console was GSA-issued.[8] There was also an adjoining closet full of clothes.[9]

Public reporting indicated that the GSA living quarters also contained a children's playroom and that children had potentially slept there.[10] Mr. Japson confirmed that there had at one time been children's toys and stuffed animals in one of the rooms but that it had since been removed.[11] Mr. Stafford insisted that no children were ever allowed to sleep in the 6th floor executive suite, and that GSA employees are not permitted to escort guests into the suite.[12] GSA told staff that it did not track which individuals were utilizing the sleeping space each day.

GSA told staff that the armed guards and bedroom furnishings are both covered under existing contracts, and that the $25,000 cost figure for the washer-dryer equipment, which was initially reported by Politico, refers to a cost estimate that was never implemented because GSA

[1] 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).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Photos: Here Are the Piles of Used Bedding and Children's Play Sets Left Near DOGE's Old Offices*, WIRED, (July 23, 2025)(www.wired.com/story/photos-bedding-childrens-play-sets-doge-old-offices/).
[11] 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).
[12] *Id.*

was able to utilize a utility room on the sixth floor that already had the necessary water and utility hook-ups.[13] However, GSA claimed to have a spreadsheet detailing all the costs associated with outfitting the sixth floor suite and offered to provide it to HSGAC staff but has yet to do so.[14]

Lack of Concern with Protections for Privacy and Cybersecurity

For over 20 years, federal agencies have been trying to balance the security of their networks, including denial of access to malicious cyber actors and protections of individuals' personally identifiable information (PII), while ensuring systems and information are accessible for legitimate users. The Computer Security Act of 1987, The E-Government Act of 2002, Federal Information Security Management Act of 2002 and 2014, and others have established responsibilities for agencies regarding the security of their systems, limits on data sharing, and access to networks using a risk-based approach. Fundamentally, according to existing statute, each agency's Chief Information Officer (CIO) or Chief Information Security Officer (CISO) is responsible for overseeing and approving access policies, often relying on whether or not the individual has a "need to know" the data. Yet, based on public reporting, court documents, and whistleblower disclosures, the DOGE teams appeared to heavily pressure agency CIO or CISOs for access to networks and data beyond their "need to know," requested and in some cases received access levels higher than normal, and also contrived schemes to ensure they would be able to evade typical oversight of agency devices and move data outside of agency repositories. Some cybersecurity researchers have characterized the activities of DOGE as more akin to malicious cyber actors than federal employees looking for fraud, waste, and abuse.[15]

In addition to potential misuse of agency networks and systems, DOGE staff have also reportedly installed Starlink devices at several federal locations to allegedly enable internet connection "dead zones".[16] SSA and OPM senior officials insisted that no Starlink devices were present. While at GSA, the presence of a Starlink device was confirmed but GSA senior officials did not allow HSGAC staff to view it.[17] To date, GSA officials have not provided documentation demonstrating that the Starlink network at GSA is used by individuals other than the DOGE team, that the network adheres to the agency's own security policies, or that the network is overseen by the agency's security operations center (SOC). GSA officials could not even confirm that the Starlink terminal was configured with basic security settings recommended

[13] *Id.*

[14] *Id.*

[15] House Committee on Oversight and Government Reform, Testimony Submitted for the Record of Bruce Schneier, *Hearing titled "The Federal Government in the Age of Artificial Intelligence",* 119th Cong. (June 5, 2025) (oversight.house.gov/wp-content/uploads/2025/06/Schneier-Written-Testimony.pdf); *Cybersecurity Experts Are Sounding the Alarm on DOGE*, TIME (Mar. 19, 2025) (time.com/7268032/doge-cybersecurity-elon-musk/); *Expert Q&A: DOGE May Be a Cybersecurity Nightmare*, The Cipher Brief (Feb. 26, 2025) (www.thecipherbrief.com/column_article/expert-qa-doge-may-be-a-cybersecurity-nightmare).

[16] *White House Security Staff Warned Musk's Starlink is a Security*, The Washington Post (June 7, 2025) (www.washingtonpost.com/technology/2025/06/07/starlink-white-house-security-doge-musk/); *Elon Musk Installed His Top Lieutenants at a Federal Agency You Probably Haven't Heard of,* Associated Press (Apr. 17, 2025) (apnews.com/article/doge-musk-trump-ai-starlink-gsa-efficiency-d67a41d1be98db11f05ca8e4472f53bd).

[17] 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).

by Starlink itself.[18] Given the lax cybersecurity practices of the DOGE team overall, HSGAC staff are concerned that any data sent or received over the Starlink device at GSA and other locations could be an easy target for foreign adversaries.[19]

In addition to the use of Starlink, another concern is the lack of clarity around the data that DOGE teams had or have access to at federal agencies. With the Privacy Act of 1974, Congress specifically intended to prevent agencies from creating dossiers on citizens by restricting the aggregation of and broad government access to extremely sensitive personal data, requiring purpose-driven needs for data sharing among government agencies.[20] Congress went further with the E-Government Act of 2002, requiring agencies to proactively inform the public about any new program or technology that uses personally identifiable information, and requiring agencies to identify and address privacy concerns before the program or technology is implemented.[21]

Public reporting alleges that DOGE is working to build one or several "master databases" containing data from multiple government agencies without any concern for data quality or any consideration that data collected for a particular purpose should not be used for an unrelated purpose.[22]

For example, this includes a recent report about DHS integrating SSA data into U.S. Citizenship and Immigration Services (USCIS) Systematic Alien Verification for Entitlements (SAVE) database, which was previously used as a tool to help federal, state, local, Tribal and territorial governments look up citizenship status for the purposes of determining eligibility for benefits. DHS reportedly has used the SSA data to turn this system into a "national citizenship list" that would allow these governments to look up any individuals' citizenship status - a highly controversial move that has been avoided in the past. DHS press releases announced DOGE supported this effort, but DHS has thus far failed to go through any of the usual transparency

[18] Starlink, *Gen 2 Router - Setup Guide* (Accessed Sept. 8, 2025) (www.starlink.com/support/article/5d40ff67-9ccd-aa45-ed3f-bcd5ec421174?srsltid=AfmBOoo5ddurtu0wL0-5EAyS45cp9dE9Df2LTF-e7tU6sVwd23OyR0lu); Starlink, *Help Center: Content Filtering* (Accessed Sept. 8, 2025) (www.starlink.com/support/article/1542bce8-8fa4-158f-5880-2dd366dec075).

[19] Letter from Ranking Member Gerald E. Connolly, House Committee on Oversight and Government Reform, to President Donald Trump (Feb. 25, 2025) (oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025-02-25.%20GEC%20Brown%20Stansbury%20to%20President%20Trump%20re.%20DOGE%20Cyber%20Issues.pdf); *A Whistleblower's Disclosure Details How DOGE May Have Taken Sensitive Labor Data,* NPR (Apr. 15, 2025) (www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security); *Russia And China Are Threatening SpaceX's Starlink Satellite Constellation, New Report Finds,* Space.Com (Apr. 8, 2025) (www.space.com/space-exploration/tech/russia-and-china-are-threatening-spacexs-starlink-satellite-constellation-new-report-finds).

[20] *Privacy under siege: DOGE's one big, beautiful database*, Brookings (June 25, 2025) (www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/).

[21] E-Government Act of 2002, Pub. L. No. 107-347.

[22] *DOGE staffer who shared Treasury data now has more access to government systems*, NPR (Mar. 31, 2025) (www.npr.org/2025/03/31/nx-s1-5345708/doge-data-access-labor-cfpb-hhs); *Privacy under siege: DOGE's one big, beautiful database*, Brookings (June 25, 2025) (www.brookings.edu/articles/privacy-under-siege-doges-one-big-beautiful-database/); *DOGE Aims to Pool Federal Data, Putting Personal Information at Risk,* Washington Post (May 7, 2025) (www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/).

requirements that would provide assurance that the data is appropriately used and protected. The quality of the data added into the system is also unknown, raising the specter of American citizens' rights being violated due to bad information in a DHS database. The database will also serve as a tool for citizenship look up for the purpose of assessing voter rolls, but DHS has not clarified whether it will integrate information from the voter rolls into SAVE itself, further growing out the database.

This concern that DOGE teams were actively pulling agency data to combine into a "master database" was further corroborated by court documents and public statements from Coristine himself, staying "it was almost like a competition in the sense to have seven, eight different laptops that they would run around with."[23] When visiting the GSA, staff found stacks of multiple laptops on each desk and GSA staff were unable to confirm that all the equipment seen were GSA issued devices.[24]

GSA officials also confirmed public reporting that Starlink infrastructure was installed at the agency, which could allow DOGE employees to bypass some of the information controls that would ordinarily restrict the flow of data from agency networks without the typical scrutiny.[25]

Based on staff visits, court documents, and whistleblower accounts, GSA appears to be the primary technical hub for the DOGE team given the inhabitation of the sixth-floor wing, installation of Starlink and other technologies, and lack of oversight from GSA officials.

[23] *Big Balls' No Longer Works for the US Government,* Wired (June 24, 2025) (www.wired.com/story/big-balls-coristine-doge-resigned-us-government/).

[24] 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).

[25] *Id*.