Written Expert Testimony to the House Committee on Oversight and Government Reform

Hearing titled "The Federal Government in the Age of Artificial Intelligence"

Bruce Schneier
Fellow and Adjunct Lecturer
Harvard Kennedy School

June 4, 2025

Data security breaches present significant dangers to everyone in the United States, from private citizens to corporations to government agencies to elected officials. Over the past four months, DOGE's approach to data access has massively exacerbated the risk. DOGE employees have accessed and exfiltrated data from a variety of government agencies in order to, in part, train AI systems. Their actions have weakened security within the federal government by bypassing and disabling critical security measures, exporting sensitive data to environments with less security, and consolidating disparate data streams to create a massively attractive target for any adversary.

Data consolidation might seem harmless or even positive, but we have to understand what's at stake when our data gets consolidated. Data is power. Any entity, whether public or private, that holds data about individuals has some ability to understand, predict, and manipulate their behavior. For example, major tech companies use people's individual data to deliver advertising that shapes what we buy and even what we believe.

Our government collects much broader and more intimate data about Americans. The power of that data depends not just on the amount and sensitivity of the data, but also on how it is organized. The separation of government data into many separate stores across many agencies limits what the government--and potential malicious actors--can do with it. Accordingly,

significant security, privacy, and liberty interests are built into that separation. Connecting disconnected data stores represents a massive increase in the power of whoever holds that data.

Whether you fear government tyranny, attacks from foreign adversaries, or attacks from domestic malicious actors, the AI-fueled consolidation of citizen data should make your fears grow. If the consolidation is carried out recklessly and in secret, as DOGE affiliates are largely doing, this new and unchecked power presents serious risks to every American.

What DOGE and its affiliates are doing with government systems and data

Starting in late January, DOGE personnel gained extensive access to government systems containing Americans' sensitive personal data [1]. For example, at the Treasury Department they obtained access to payment systems that process trillions of dollars in government transactions. DOGE employees gained both "read" and, in at least one case, temporary "edit" access as well [2]. This means that they were able to both see and alter the data. At the Consumer Financial Protection Bureau, DOGE employees gained "read access" to sensitive financial data [3]. DOGE also gained access to health information, social security numbers, military records, and more from the Center for Medicare and Medicaid Services and from Veterans Affairs. DOGE accessed data [4] at many other major agencies including the Office of Personnel Management and Departments of Commerce, Education, Energy, Labor, Health and Human Services, and Transportation. (This period is discussed in more detail in Appendix A, "Understanding DOGE and Your Data.")

Since January, DOGE has transformed from an agency to a more integrated program across agencies as many DOGE personnel and affiliates have moved into official roles within the government. In this new capacity, DOGE affiliates (who are no longer constrained in their data access by court orders or inter-agency agreements) have become widely embedded across agencies including Office of Personnel Management, the General Services Administration, Treasury, Health and Human Services, and many more.

At these organizations, they are overseeing a transformation of data practices that follows a common **"DOGE approach" with 4 distinguishing features**:

1. **Data consolidation**: Exfiltrating and connecting the massive US databases to create a single pool of data that covers all people in the United States. This has long been a goal among some tech leaders: in fact, Oracle started as a CIA project, and aimed to create a database covering everyone in the US. Toward this end, DOGE affiliates are working to connect databases across many agencies, including highly sensitive data sets like IRS taxpayer returns which have been kept separate to encourage trust and tax compliance among the public.
2. **Reduced security protocols:** DOGE affiliates have consistently removed access controls and audit logs, created unmonitored copies of data, exposed highly sensitive data to

cloud-hosted tools, sought maximally permissive data access waivers, and omitted previously required security protocols for vetting staff.

3. **AI training and processing**: Processing this data with AI tools, which exposes data outside carefully monitored environments.
4. **Outsourcing**: Transferring control over data access to private companies, especially Palantir.

For example, at IRS, DOGE is attempting to create a single tool that would allow access to all data from IRS systems (consolidation) [5]. Public reporting indicates that Palantir employees were working on the projects without a signed contract that would stipulate security measures (reduced security protocols). The plan for the project involved using AI tools (AI) controlled by a private entity to manage access to all IRS data (outsourcing).

The data consolidation, removal of controls, AI use, and outsourcing to private sector actors may seem to enhance efficiency, but it actually amplifies known dangers of data in the hands of our adversaries.

The known dangers of data in the hands of our adversaries

Americans may disagree about who counts as an adversary, but everyone agrees we have them. And the more powerful someone is -- whether they be an individual, a corporation, or the government itself -- the more powerful the adversaries they attract.

We already know that America's geopolitical adversaries are attempting to access the consolidated DOGE data. When DOGE staff gained access to sensitive NLRB data, a user with a Russian IP address immediately tried to log in with the staffers' (correct) usernames and passwords [6]. These efforts happened "in near real-time", with no lag between issuing log-in credentials and the log-in attempts. While these specific log-in attempts were blocked, they are likely the tip of a much larger iceberg.

What can our adversaries do with data?

Adversarial Use Case 1: Coercion

First, data can be used to ruin reputations, target people for harassment or financial ruin because of their political ties under a future administration, or undercut people's businesses by leaking secrets to competitors.

Data can be used to coerce people for a variety of purposes: into revealing information, providing access, disavowing or changing their political positions, or otherwise cooperating with an adversary. The more powerful the person, the more valuable the coercion. Some of the basic techniques for using data for coercion include the following:

- **Blackmail and threats.** Adversaries use government data profiles to find people to blackmail and threaten into giving up information, access, or decision-making power. These threats can leverage the most innocuous data. Something as simple as a home address or the name of a child's school, which can easily be found on a tax return, can be weaponized. Threatening to leak sensitive data on social media and whip up an outraged mob (sometimes called doxxing) puts public figures and their families in immediate danger. Of course, stigmatized or secret behavior can also be identified from government data, including married public figures treated for STDs under Medicare or VA benefits, people who were treated for mental illness or drug use, people with unusual financial transactions indicating gambling problems or hidden investments, or people with family members facing these issues.
- **Bribery.** It's much easier to identify possible bribery targets when the adversary has access to financial data, like tax returns from the IRS.
- **Using sensitive corporate information.** The data systems DOGE can access aren't limited to individuals. There are reports of DOGE access at the Consumer Financial Protection Bureau, the National Labor Relations Board, the Federal Aviation Administration, the Food and Drug Administration, and more. All this data provides incredible leverage over companies: the ability to leak information about vulnerabilities to a competitor, identify We know that corporations are targets for nation-state actors, as in the SolarWinds attack from 2020, which gave the Russian government access to over 14,000 government and corporate systems.

Coercion doesn't have to target the elected official or other public figure directly. Anyone with a relationship can be a target: the public figure, their staff, their family, their friends. In fact, access to broad data simplifies the process of mapping those relationships: an adversary can use this data to identify potential targets based on employment, residence, school similarities, etc.

Adversarial Use Case 2: Preparing the Battlefield for Cyberwar

The true risks of cybersecurity issues often aren't seen right away. It may take months or years to maneuver into position to coerce critical public figures. But coercion isn't the only risk.

In any future armed conflict with China or another nation-state-level actor, it's highly likely that a first step would be to cause massive economic disruption, including targeting elite actors so they are distracted by personal concerns during the crisis. Data is a crucial resource in such a conflict: if the attacker wants to target bank accounts associated with members of Congress or military leadership, for example, data from OPM, IRS, and the Treasury Payments System (all of which have been accessed by DOGE affiliates) would be invaluable.

Adversaries can also use data and systems access -- even if it is read only -- to learn more about how to access systems in the future. It's similar to allowing a thief to walk around your house

and take pictures without touching anything. The thief can note vulnerabilities, the locations of valuables, and other useful information for future attacks.

Finally, we know that American adversaries have installed back doors in our critical infrastructure systems, like the power grid [7, 8]. This is a major ongoing threat to the public. Given the many security breaches and decreases in compartmentalization observed as DOGE has worked to centralize data and access, it is a certainty that American adversaries are looking to exploit those breaches to provide themselves with access going forward. Back doors into the Treasury Payments System or other crucial infrastructure could be immensely valuable in a cyberconflict.

How DOGE has created unprecedented cybersecurity risks for the American people and government

DOGE's approach is making the risks of weaponization more real and the potential impacts more devastating.

Pooled sensitive data with weak cybersecurity protections creates significant risks to elected officials, national security, and the public as a whole. Some of the most serious risks come from the potential for access to this data because it can be more easily attained by both criminals and nation states. By combining vast amounts of data, and bypassing or disabling industry standard security protocols, DOGE affiliates have started to amass an irresistibly tempting honeypot for adversaries who want leverage over them.

In 2015 as part of a hack of the Office of Personal Management, China gained access to all data on the SF-86, the form used by government employees who are applying for security clearances, and possibly to a broader set of data on federal employees. This one time breach was widely regarded as a massive security threat, because it exposed extremely personal data about people in sensitive positions to an American adversary. China suddenly knew who had been hired for intelligence agencies, and had detailed dossiers. This breach pales in comparison to the potential magnitude of data exposure from the combined DOGE datasets, but many of the security risks are similar.

Bypassing security practices creates a risk of back doors and security breaches

DOGE's lax security practices have been widely described in the media, and I have discussed them in my sworn declaration in AFL-CIO vs OPM (attached as Appendix B). DOGE and its affiliates have hired young, inexperienced staffers with minimal relevant background to work on critical infrastructure with major security risks. Worse, they have simply skipped the universal background checks required for people with sensitive access, leading to situations where staff with foreign ties and connections to criminal enterprises have been given broad access to critical data and infrastructure.

We know about some major breaches already: DOGE affiliates have posted classified information online, configured web and email servers in ways that allowed public attacks, and had their usernames and passwords used by actors with Russian IP addresses immediately after those credentials were issued.

Given the security breaches we know about, it is likely that there are many more we are not aware of. Once such access is revoked, it is possible to begin the work of identifying any back installed due to these lax practices. However, the process will take years of massive audits costing hundreds of millions of dollars. Claims that access has been "read only" cannot be trusted, meaning that identifying and eliminating vulnerabilities will take years and hundreds of millions of dollars in auditing and rewriting software to address. Until that audit process happens, there is no knowing who -- inside or outside of government -- controls what.

Consolidating data makes the risks of cybersecurity breaches worse

In a castle or an office building, one way to prevent access by thieves is to include multiple layers of access controls: key cards, keys, pass codes, a security guard, and more. This is known as defense in depth. As discussed above, DOGE and its affiliates have avoided many components of access control.

But another key component of cybersecurity is compartmentalization: once inside the metaphorical building, each person's key only opens their own office. This limits the downside risk of any given breach. DOGE has been focused on combining data sets to create individual level profiles of each person in the United States. Instead of stocking each person's metaphorical office with only the data they need, they propose to combine all the data rooms into a single large space which many government agencies can access. After consolidation, stealing credentials (an office key) doesn't merely give access to one person's office, but to the entire stash.

This creates an incredibly tempting target with many access points for any adversary. Any leaked or compromised data accessed by American adversaries can help adversarial actors identify people who may be able to offer them increased access. As the government increases its engagement with companies like Palantir, both federal agencies and those companies in turn become targets. In the meantime, opportunities for control and harassment by this administration or by future administrations are unprecedented, especially since the increase in AI capabilities allows vast amounts of data to be processed in real time.

Because DOGE and its affiliates have bypassed standard security practices, there is almost no way to do an audit on what data was copied or who has it. That ship has sailed. It's quite possible we will see government data on US citizens and classified topics gradually emerge on dark networks in the years ahead. In the meantime, this administration, future administrations, and any adversaries who gain access to the consolidated data will have nearly unprecedented access to data they can use for coercion and hacking. While significant damage has already been done, ongoing access makes it much worse. Until the data pipeline is shut down, there is the risk that

adversaries will have not only a single moment's snapshot, but a constantly updated source of information on where to focus their efforts at blackmail, threats, and bribery on people based on current data.

Finally, any pooled data source will inevitably be prone to errors, as duplicate records, similar records, and data artifacts propagate through the connection. We have already seen major errors of interpretation, as when DOGE affiliates claimed there were people over 150 years old receiving SSA benefits. Those erroneous dates were an artifact of issues with date-handling in COBOL, a software language used in the mid-20th century to create many of SSA's data systems. As data systems are pooled and centralized, errors will propagate and combine. AI tools are unlikely to reduce this issue, since they are not likely to have appropriate contextual information to assess how to manage errors.

Additionally, our adversaries could deliberately introduce errors into the data in an attempt to poison the AI systems. This is a known method of attack, and has been extensively researched within the AI security community.

Whether accidentally or deliberately, errors in the AI training data or input puts people at risk of having benefits cut off, or being targeted for fraud, across multiple systems rather than just one. It also results in an untrustworthy AI system. Unless the data inputs to the AI are known to be accurate and complete, the AI's outputs cannot be trusted as accurate and complete. This is known as the integrity problem.

AI amplifies the dangers of data consolidation and shoddy security practices

Historically, one of the major limits on using data is the difficulty of searching through large volumes of data. As AI capabilities and deployment increase, that limitation decreases.

- Using government data sources to train AI creates a permanent, untraceable record of the data. AI tools can access and return their training data, and can also use it to comb for vulnerabilities in either the system or the data.
- This administration or a future administration could use AI tools combined with data access to create massive surveillance systems that target all Americans.
- AI tools are not ready to take over for humans. No responsible company in the world is turning over its corporate decision-making or customer interactions to AI agents at scale. Using AI agents for higher-level systems creates exponential risks. There have been numerous stories recently of AI interfering with their being shut down, sending secret emails on its own, and so on. Giving AI agents the opportunity to do this on government services puts national security and public well-being at risk.

DOGE's approach has already done irreparable damage to American security. However, the situation can get even worse. We must stanch the flow of data so that at least what our adversaries have taken will soon be outdated. By following the DOGE approach, the current

administration has increased both the likelihood and the potential scale of attacks against us and endangered our safety, both individually and collectively. A decisive shift in the administration's approach to data security can begin to right the ship.

Appendices

A. Alexander Pascal, Allison Stanger, Bruce Schneier, Kinney Zalesne, Nick Pyati, Sarah Hubbard, and Vivian Graubard. "Understanding DOGE and Your Data". March 31, 2025. https://ash.harvard.edu/resources/understanding-doge-and-your-data/

B. Bruce Schneier: Declaration from AFL-CIO vs OPM, United States District Court, Southern District of New York, Case No. 1:25-cv-01237-DLC, April 21, 2025.

References

[1] The New York Times. "The People Carrying Out Musk's Plans at DOGE." Published in *The New York Times*, February 27, 2025. https://www.nytimes.com/interactive/2025/02/27/us/politics/doge-staff-list.html

[2] Jeff Stien. "Treasury revoked editing access 'mistakenly' given to DOGE staffer." Published in *The Washington Post*, February 11, 2025. https://www.washingtonpost.com/business/2025/02/11/doge-treasury-access-marko-elez/

[3] Makena Kelly. "DOGE Is Now Inside the Consumer Financial Protection Bureau." Published in *Wired*, February 7, 2025. https://www.wired.com/story/doge-access-consumer-financial-protection-bureau-data/

[4] Tanya S. Chutkan. *State of New Mexico vs. Elon Musk. Memorandum Opinion and Order*. February 18, 2025. https://storage.courtlistener.com/recap/gov.uscourts.dcd.277463/gov.uscourts.dcd.277463.29.0.pdf

[5] Makena Kelly. "Palantir Is Helping DOGE With a Massive IRS Data Project." *Wired*, April 11, 2025. https://www.wired.com/story/palantir-doge-irs-mega-api-data/

[6] Jenna McLaughlin. "A whistleblower's disclosure details how DOGE may have taken sensitive labor data." *NPR*, April 15, 2025. https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security

[7] Ryan Lucas. "Wray warns Chinese hackers are aiming to 'wreak havoc' on U.S. critical infrastructure." *NPR*, January 31, 2024. https://www.npr.org/2024/01/31/1228153857/wray-chinese-hackers-national-security

[8] Andy Greenberg. “China-Linked Hackers Breached a Power Grid—Again.” *Wired*, September 12, 2023. https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/

ADDITIONAL RESOURCE MAR 31, 2025

Understanding DOGE and Your Data

By:
Alexander Pascal, Allison Stanger, Bruce Schneier, Kinney Zalesne, Nick Pyati, Sarah Hubbard, Vivian Graubard

Over the past several weeks, the Department of Government Efficiency (DOGE) within the Trump Administration has been embedding staff in a range of United States federal agencies. These staff have gained access to data maintained by the federal government. This guide explains what is in the data, what DOGE is doing with it, and why it matters to all Americans.

PROGRAMS
Allen Lab for Democracy Renovation, GETTING-Plurality

ISSUES
Civic Engagement, Democracy and AI, Democratic Reform

What are those federal datasets and what do they have to do with me?

What data does the federal government have about me?

The federal government maintains comprehensive records of Americans' interactions with government services. Government records include not only basic information like your name, address, birthday, and Social Security number, but a much broader range of data. Any time you submit a government form, file an application or your taxes with the government, register a complaint, or receive a service, these interactions become data in

a government database. For example, the government maintains detailed records of:

- **Financial information:** Your tax returns, federal benefits, and any government payments.
- **Health information:** Your Medicare, Medicaid, or Veterans Administration (VA) records.
- **Social Services and Public Benefits information:** Information regarding any social services you may have applied for, including food assistance (WIC, SNAP), social security and disability income, and housing assistance
- **Education information:** Your educational history in federal student aid records and any government-funded research.
- **Immigration information:** Any visa or immigration benefits for which you applied, or information on applications for individuals you have sponsored.

You may have other sensitive data stored by the government as well. For example, if you've ever held a security clearance or government job, there are extensive background check records, including what your former colleagues and neighbors said about you. If you've ever served in the armed forces, your service records, including your mental health records, are held by the federal government. Data like employment records, fingerprints and facial recognition data, immigration status may also be included. Some private records (for example, private health data) may have been accessed by the government if needed for national security or law enforcement purposes.

What does the government normally use this data for?

The data maintained by the federal government is essential to running the government and providing public services. For example, tax records enable fair collection of revenue and distribution of benefits; healthcare data allow the United States Department of Veterans Affairs, Medicare, and Medicaid to provide care and track outcomes; and education records allow the government to manage student aid and measure program effectiveness. Every function of the federal government, from law enforcement to border protection to managing the economy, depends on robust, accurate data.

Because this data is so valuable and sensitive, the federal government has guardrails in place to ensure it is used appropriately. By law, federal agencies are required to:

- Use the data only for authorized purposes
- Protect it from unauthorized access
- Maintain accurate records of who accesses which data
- Keep data separated between agencies, unless those agencies are specifically authorized to share

Who normally has access to this data? What qualifications and safeguards are there?

Access to government data is traditionally strictly controlled through multiple layers of protection. Historically, all federal employees have been required to undergo some form of background check to ensure they are reliable, trustworthy, and suitable for the job, and they must obtain appropriate "clearances" before accessing sensitive data. Higher-level clearances and access to more sensitive data and information require more extensive and rigorous background checks that examine criminal records, financial history, foreign contacts, and other potential security risks, among other things.

In addition to security clearances, access to government data follows "need-to-know" principles. Even employees with security clearances can only access data necessary for their specific roles. Systems maintain detailed logs of who accesses what information and when, and regular audits ensure

compliance with these restrictions. Most importantly, access to data is subject to strict privacy protections.

What is DOGE doing with my data?

What is DOGE?

The Department of Government Efficiency (DOGE), formerly the United States Digital Service (USDS), was established by executive order in 2025 under Elon Musk's leadership, with the goal of modernizing government operations.

Since its formation, DOGE has been granted or has sought unprecedented access to government systems and data across agencies. DOGE claims that it needs this access in order to identify and target areas of waste, fraud, and abuse within government spending. It's unclear if DOGE employees have met security clearance requirements even as they gain broad access to sensitive systems.

Who from DOGE has access to my data?

Multiple DOGE employees have gained extensive access to government systems containing Americans' sensitive personal data. At the Treasury Department, DOGE personnel have obtained access to payment systems that process trillions of dollars in government transactions. DOGE employees have "read" access, and at least one employee temporarily had "edit" access as well, meaning that they would be able to both see and alter the data. At the Consumer Financial Protection Bureau, DOGE employees have "read access" to sensitive financial data. DOGE has also gained access to health information, social security numbers, military records, and more from the Center for Medicare and Medicaid Services, as well as Veterans Affairs. DOGE is also seeking to give team members access to IRS systems containing hundreds of millions of tax returns and other sensitive tax information.

This access extends across multiple agencies. While the Treasury Department recently prohibited access to personal taxpayer data, DOGE was not blocked from accessing data at seven other major agencies including the Office of Personnel Management and Departments of Commerce, Education, Energy, Labor, Health and Human Services, and Transportation. Additionally, the recent executive order "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos" aims to make inter-agency data easier for federal employees to access.

What are the risks of DOGE accessing my data?

Why does "read-access" to Americans' data matter?

DOGE team members have "read-access" to Americans' data across numerous federal agencies, ranging across the Social Security Administration, Health and Human Services, the Department of Education, the Veterans Administration, and more.

Read-access carries risk, and could enable individuals to do the following:

- Copy data to use for unauthorized purposes
- Deny access to public services, benefits, and opportunities such as: medical care, housing, food or student financial assistance, veteran or military benefits, public contracts, and more.
- "Doxx" (share personal information online)
- Provide or sell data to foreign governments, data brokers, and/or private companies

Could my data be altered, manipulated, or deleted?

Yes, and this represents one of the most serious risks. Unlike traditional government employees who have read-only access to most systems, some DOGE personnel have been granted "edit-access" to critical databases at USAID and are requesting this access at other federal agencies. The risk of "edit-access" means records could be altered or erased.

These risks are particularly concerning for government payment systems. With both read and edit-access to Treasury systems, DOGE personnel could modify payment records, redirect funds, or interfere with benefits distribution.

Will my data be leaked?

The risk of data leaks is substantial. DOGE recently shared sensitive information on their public-facing website, including data on budget and staffing at the National Reconnaissance Office spy agency, which was not intended for public release and raises national security risks.

The Electronic Privacy Information Center has already filed suit against OPM, Treasury, and DOGE over data breach concerns.

Could my data be used against me?

Yes, and the risks are both immediate and long-term. In the short term, unauthorized access has already enabled targeting of individuals for harassment. For example, some employees of the United States Agency for International Development (USAID) have been "doxxed," i.e., had their personal information released publicly, after DOGE accessed personnel files. Federal workers are reporting fear of political retaliation, with FBI officials particularly concerned about the targeting of those perceived as disloyal to the administration. While these examples involve federal employees, the data DOGE is accessing could enable similar attacks against many Americans who do not work for the federal government. Leaked data could enable identity theft, financial fraud, or targeted harassment.

What else could my data be used for?

The quality of AI systems depends on the data used to train them. Much of that data is information scraped from the internet that can be messy, biased, or unreliable, and leading AI companies now spend enormous sums of money to buy higher-quality data. Government databases offer something fundamentally different: comprehensive, verified records about the most critical areas of Americans' lives. At least one prominent technology executive has suggested that the United States and other countries consolidate all of their national data into a single dataset that could be used to train AI models, though the American public has not consented to personal data being used for these purposes. Recently, DOGE has begun deploying AI tools for government agencies to leverage, such as GSAi.

Access to Americans' data could give private companies significant advantages in training AI systems and in setting business strategy. Without proper oversight, this access could lead to private companies profiting from sensitive information or foreign governments exploiting vulnerabilities.

The safeguards protecting government data were built over years to protect Americans, but these protections are already eroding. The consequences could be immediate or unfold over time, leading to loss of services, harassment, discrimination, or manipulation by the government, private entities, or foreign powers.

As these events are rapid and ongoing, this guide has only been updated to March 2025.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, *et al*., Plaintiffs, v. U.S. OFFICE OF PERSONNEL MANAGEMENT, *et al*., Defendants.	Case No. 1:25-cv-01237-DLC

DECLARATION OF BRUCE SCHNEIER IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

I, Bruce Schneier, declare as follows:

1. I am over eighteen years of age and competent to give this declaration. This declaration is based on my personal knowledge, information, and belief.

2. I have been a security technologist for more than thirty years, focusing on all aspects of cybersecurity. I am currently an adjunct lecturer at the Harvard Kennedy School, where I teach cybersecurity policy. I am a fellow at the Belfer Center for Science and International Affairs, the Ash Center for Democratic Governance in and Innovation, and the Berkman Klein Center for Internet and Society—all at Harvard University. I am the author of more than a dozen books and hundreds of articles, essays, and papers on digital security and cybersecurity. I have testified before Congress, served on government committees, and am a frequent commentator about security and privacy issues. I am a Board Member of the Electronic Frontier Foundation and AccessNow, and an Advisory Board Member of the Electronic Privacy

Information Center and VerifiedVoting.org. I am also the Chief of Security Architecture at Inrupt, Inc., and a partner at Alchemist Associates LLC.

3. More information about me and links to my many publications about computer and digital security are available at www.schneier.com. My curriculum vitae is attached as Exhibit A.

4. From long experience in this field, I know that engineers and programmers who are skilled in one area of technology are often not skilled at cybersecurity. It requires a different kind of expertise, mindset, and experience to understand and take the appropriate steps to protect computer systems from attack than it does to build or maintain those systems.

5. Based on my experience and the information available on the public record, and as I explain further below, my professional opinion is that imminent risks of significant harm exist for the millions of Americans whose sensitive data is held by the US Office of Personnel Management (OPM), including plaintiffs, as a result of the access to OPM systems given to personnel of the newly created Department of Government Efficiency (DOGE). Additionally, this access has created an imminent risk of harm to America's national security.

6. The longer that people affiliated with DOGE have access to, or copies of, the personnel information in the OPM databases, the more imminent the risk of harm and the greater harm that can occur due to that risk.

7. As I detail further below, the most alarming aspect of the reported activities is that defendants have systematically circumvented security measures that would detect and prevent misuse—including standard incident response protocols, auditing, and change-tracking

mechanisms—in large part by sidelining the career officials in charge of those security measures and replacing them with inexperienced operators.[1]

8. The defendants also appear to be operating without proper and experienced oversight, especially with regard to the specific security measures of the many complex systems that OPM operates. The approach and execution of DOGE personnel's access to OPM systems creates significant security risks and violates longstanding OPM policy.

9. For instance, Declarant Greg Hogan has been at OPM less than four months and was not previously in governmental service. Given that limited experience, his familiarity with OPM systems is likely not deep. Mr. Hogan's previous experience is with a company owned by Elon Musk that was developing technology to make cars semiautonomous.

10. Additionally, other DOGE engineers obtained access to OPM's records before the agency confirmed that they had government-issued computers and before they had been vetted in accordance with longstanding agency practices.[2]

11. In one instance, records were disclosed to an inexperienced engineer who called himself "Big Balls" online, who had previously been fired from a cybersecurity firm following

[1] Letter from Rep. Gerald Connolly, Ranking Member, House Committee on Oversight and Government Reform & Rep. Shontel Brown Ranking Member, House Committee on Oversight and Government Reform, Subcommittee on Cybersecurity, Information Technology, and Government Innovation to Charles Ezell, Acting Director, Office of Personnel Management (Feb. 4, 2025), https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.02.04.%20GEC%20and%20Brown%20to%20OPM-Ezell-%20DOGE%20Emails.pdf (Connelly & Brown letter). *See also Tim Reid, Musk aides lock workers out of OPM computer systems, Reuters, Feb. 2, 2025,* https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.

[2] Nick Schwellenbach, Elon Musk's DOGE Team Raise Vetting, Ethics Concerns, Project on Government Oversight, Feb. 6, 2025, https://www.pogo.org/investigations/elon-musks-doge-teams-raise-vetting-ethics-concerns; Anthony Kimery, Internal feud rages over unvetting DOGE access to federal IT systems, Biometric Update, Feb. 19, 2025, https://www.biometricupdate.com/202502/internal-feud-rages-over-unvetted-doge-access-to-federal-it-systems; Charles Rollet, Federal workers sue Elon Musk and DOGE to cut off data access, TechCrunch, Feb. 11, 2025, https://techcrunch.com/2025/02/11/federal-workers-sue-elon-musk-and-doge-to-cut-off-data-access/?guccounter=1.

(according to a recent firm statement) "an internal investigation into the leaking of proprietary information that coincided with his tenure."[3]

12. Reports also indicate that individuals associated with DOGE connected an unauthorized server into the OPM network.[4]

13. As a result of these and other "urgent concerns related to potential unauthorized access of government networks and sensitive information at certain federal agencies, including at the U.S. Office of Personnel Management (OPM)" raised by several members of Congress in a letter dated February 6, 2025, the Office of Inspector General of the OPM initiated an investigation on March 7, 2025.[5]

Types of Security Risks

14. Poor security of OPM's network creates three distinct kinds of security risks, all of which appear to be present here:

15. D**ata exposure**. This is the risk that OPM's data—both personal information and transaction records—could be accessed or copied.

16. **System manipulation**. This is the risk that, because of poor security, external threat actors could break into OPM's network. They would be able to manipulate OPM's systems while also altering audit trails that would provide evidence of their changes. This could include adding and deleting data or installing "backdoors" to facilitate later access.

17. **System control.** This is the risk that external threat actors could fully take control of OPM's systems. Going beyond mere manipulation, they would be able alter core systems and

[3] https://www.nytimes.com/2025/02/07/us/politics/musk-doge-aides.html.

[4] Connolly & Brown Letter.

[5] https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/hogr-minority-final.pdf

authentication mechanisms, while at the same time disabling the very tools designed to detect such changes. This is more than modifying operations; it is modifying the infrastructure that those operations use.

18. These three risks can result in three different types of security breaches: confidentiality, integrity, and availability.

19. **Confidentiality breaches.** These occur when a person's data is exposed. The data OPM has about millions of people is highly personal, and there are many ways to exploit it. External actors who want this data include adversarial foreign state actors like China—who I will discuss further below—and include criminals who want to use the data for identity theft and other forms of fraud.

20. In the case of OPM data, beyond simple exposure of personally identifying information, which is bad enough, the breaches involve unauthorized access to even more sensitive data. This includes personnel security clearance data revealing intelligence connections, background investigation information exposing personal vulnerabilities, financial disclosure forms containing detailed asset information, and medical information revealing conditions that could be exploited.

21. Many of the plaintiffs are at higher risk if their identities and locations are disclosed. This includes those who work undercover or in clandestine government services, as well as the Administrative Law Judges who often face threats of retaliation from litigants.

22. A particular risk for plaintiffs who are targets of foreign intelligence services is that a breach that allows those services to identify intelligence officers can allow these adversaries to build targeting profiles and conduct human intelligence operations against those federal employees.

23. **Integrity breaches** occur when the data is modified, either accidentally or deliberately. Depending on the nature of the modification, this can have catastrophic consequences for plaintiffs, most of whom rely on OPM to receive their proper paychecks, benefits, retirement support, and more.

24. Specifically, unauthorized modifications can allow others to alter security clearance statuses to grant access to unauthorized individuals, modify payroll or benefits information to deny or change benefits in ways that create financial distress, modify employment history in ways that deny or delay promotions or salary increases, insert false disciplinary actions to create grounds for blackmail, or change contact information to intercept communications. These attacks are used by both foreign adversaries and criminals.

25. **Availability breaches** occur when data is deleted or otherwise made unavailable. Any sort of availability breach can be as catastrophic as integrity breaches for people who depend on OPM for their salaries, benefits, and retirement and medical care payments.

26. This kind of breach includes the possibility of ransomware, when an external threat actor encrypts the data and demands payment to unlock it. The criminal ransomware industry is extensive and robust**,** and countries like North Korea engage in ransomware as a means of funding their government.

27. Unavailable data can result in denial of service, impacting retirement and health benefits and disruption or harm to background investigations.

28. All three of these types of breaches are more likely now that OPM's security is reduced. Indeed, those breaches could already be in process.

Violating Separation of Duties Increases Security Risks

29. Because computer systems like OPMs have such high security requirements, they were designed with the same two-person control principle that guides nuclear launch protocols:

No single person should have the ability to make critical changes to the system. Just as launching a nuclear missile requires two separate officers turning their keys simultaneously, making changes to critical systems that house sensitive personal records traditionally requires multiple authorized personnel working in concert.

30. This approach, known as "two-person control" or "separation of duties," isn't just bureaucratic red tape; it's a fundamental security principle as old as security itself. It is used for many situations, far beyond the nuclear example. When your local bank processes a large transfer, for instance, it requires two different employees to verify the transaction. When a company issues a major financial report, separate teams must review and approve it. These are essential, time-tested safeguards against corruption and error.

31. This principle has been codified in NIST 800-53 AC-5 (Separation of Duties).

32. People associated with DOGE have been granted full administrative access to DOGE systems, which allows them to make changes without the protection provided by a separation of duties protocol.

33. Worse, these same people have been granted and have in fact accessed a wide range of *different* government computer systems across different government agencies, including those of the Defendant Office of Personnel Management,[6] along with the US Treasury,[7] the US

[6] *Elon Musk seizes computer system, locks out senior government officials*, Yahoo, Feb. 2, 2025, https://www.yahoo.com/tech/elon-musk-seizes-computer-system-171738117.html.

[7] *Wyden Demands Answers Following Report of Musk Personnel Seeking Access to Highly Sensitive U.S. Treasury Payments System*, U.S. Senate Committee on Finance, Jan. 31, 2025, https://www.finance.senate.gov/chairmans-news/wyden-demands-answers-following-report-of-musk-personnel-seeking-access-to-highly-sensitive-us-treasury-payments-system.

Agency for International Development,[8] US Citizen and Immigration Services,[9] and reportedly others. This also violates the security principle of separation of duties.

34. In other words, the same individuals with access to Treasury systems now have access to OPM's personnel database, creating a unified attack surface across multiple critical government functions that can be exploited by adversaries, both foreign and domestic.

35. These reports confirm my fears about a lack of experience and understanding about the security needed for these systems. Both inside and outside of OPM, this kind of broad, uncontrolled access by the same people to multiple systems violates the fundamental separation of duty principles.

Violation of the Principle of Least Privilege Creates Risks.

36. A second principle is known as the Principle of Least Privilege, which holds that a person using a system should only have access to the minimum portion of a system and data necessary to do their jobs and only for as long as they need it.

37. This has been captured in NIST 800-53 AC-6, which lists The Principle of Least Privilege as a key security control.[10]

38. In sharp contrast to this Principle, many of the newly hired DOGE personnel, and all of them initially, were granted maximum access to OPM's systems.

39. Federal systems, including OPM, typically implement time-limited, audited privileged access through secure mechanisms like CyberArk/Venafi or BeyondTrust. Reports

[8] Abigail Williams, et al., *USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems*, NBC News, Feb. 2, 2025, https://www.nbcnews.com/politics/national-security/usaid-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357.

[9] (https://www.theverge.com/policy/643807/doge-uscis-data-naturalization-elon-musk); https://www.washingtonpost.com/business/2025/02/10/musk-doge-state-department-surrogate/

[10] https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

indicate DOGE personnel have obtained persistent administrative access, bypassing these controls. Without proper personnel access management controls, detecting malicious activity becomes nearly impossible, as administrative users can modify audit logs to conceal their actions.

Risks from Hardware or Software Modification

40. Every hardware or software modification to complex systems like OPM's systems normally goes through a complex planning process and includes sophisticated access control mechanisms. The way DOGE has accessed and manipulated the OPM systems has made them much more vulnerable to attack. Making matters worse, as noted above, the experienced, legitimate system administrators trained to protect them have been sidelined, locked out, or driven out.

41. For instance, the Federal Information Security Modernization Act (44 U.S.C. § 3554) requires formal security assessment and authorization before substantive system changes are made.

42. DOGE's reported activities bypass this process, creating unassessed and unauthorized modifications to federal information systems.

Leaving the Door Propped Open

43. Foreign adversaries typically spend years attempting to penetrate government systems such as OPM, using stealth to avoid being seen and carefully hiding any tells or tracks. As the Congressional report on the breach confirms, the Chinese government's 2015 breach of OPM started in 2012, and included the installation of backdoors that were later exploited. The breach was a significant US security failure, and it illustrated how personnel data could be used to identify intelligence officers and compromise national security.

44. By modifying core systems, the DOGE agents have not only compromised current operations but have also likely left behind vulnerabilities that could be exploited in future attacks, giving adversaries such as Russia and China an unprecedented opportunity.[11] Those countries have long targeted these government systems, not only to gather intelligence, but to understand how to disrupt these systems in a crisis and to plant backdoors that could be triggered at a later date.[12]

45. This risk, and the irreparable harm that occurred due to the 2015 OPM breach, was identified and discussed in more detail by the House Oversight Committee in its 2016 report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,"[13] attached as Exhibit B. It includes an explanation of how the government focused on a first intruder and missed a second one, who later exfiltrated the fingerprints of 5.6 million people.

46. Even more recently, an employee of the National Labor Relations Board provided information to the Senate Select Committee on Intelligence that demonstrated significant

[11] Suzanne Smalley, As DOGE teams plug into federal networks, cybersecurity risks could be huge, experts say, The Record, Feb. 3, 2025, https://therecord.media/doge-opm-treasury-cybersecurity.

[12] PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Intrastructure, Cybersecurity Advisory, Feb. 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a; Gintaras Radauskas, China secretly acknowledges Volt Typhoon attacks on US infrastructure: why?, cybernews, April 14, 2025, https://cybernews.com/cybercrime/china-volt-typhoon-infrastructure-taiwan-warning/; Laila Kerney, US electric grid growing more vulnerable to cyberattacks, regulator says, Reuters, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/ ("Geopolitical conflict, including Russia's invasion of Ukraine and the war in Gaza, have dramatically increased the number of cyber threats to North American power grids, NERC said. Threats also commonly come from China").

[13] https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

security problems arising after DOGE was granted access to its systems, including over twenty attempts to access the systems from a Russian IP address.[14]

47. The technical details of how these systems operate now, their security protocols, and their vulnerabilities are now potentially exposed to unknown parties without any of the usual safeguards. Instead of having to breach heavily fortified digital walls, these parties can simply walk through doors that are being propped open—and then erase evidence of their actions.

Imminent Harm from DOGE Access

48. If the OPM database has been or will be breached, either due to external attacks made easier through DOGE's activities or mistakes or security failures by the new DOGE team, the consequences would be significant and irreparable.

49. For the plaintiffs, privacy (confidentiality breaches) consequences can include identity theft, fraud, misidentification, harm to credit ratings, stalking, risk of retaliation from foreign adversaries, risk of loss of assets, and vulnerability to blackmail and other forms of exploitation, just to name a few. Any of these can result in substantial harm, loss of money or property, embarrassment, inconvenience, or unfairness. In most data breach situations, people suffer not just one, but many of these harms.

50. For the plaintiffs, integrity consequences can include miscategorization, which can result in a loss of pay, medical care, and other benefits, depending on the data that has been impacted. It can also impact potential promotions, job security, and more.

51. For the plaintiffs, availability consequences can include the same sorts of harms as integrity risks, as well as risks from ransomware and other attacks.

[14] Declaration of Daniel J Berulis, submitted to the Senate Select Committee on Intelligence and the U.S. Office of Special Counsel (April 14, 2025), available at https://whistlebloweraid.org/wp-content/uploads/2025/04/2025_0414_Berulis-Disclosure-with-Exhibits.s.pdf at ¶21.

52. Additionally, as I noted above, OPM's databases contain information about plaintiffs who face particular risks, including two specific kinds.

53. First, it creates more acute risks for current or former government employees who are or have operated under cover or who reasonably fear targeting by a foreign adversary or domestic criminal gang. This category includes many who operate publicly under various pseudonyms for protection of both themselves, their families, and their work.

54. Second, it creates acute risks for government employees in politically charged areas who could receive threats of violence, and face actual violence. For example, Administrative Law Judges often face violence and threats of violence from unhappy litigants. The same is true of employees who interact with the public at various agencies ranging from Social Security to Veterans Affairs to the Internal Revenue Service.

55. There is no indication that defendants have taken any steps to recognize these increased security needs, much less that they have taken any precautions in response of them.

Significance of the 2015 Office of Personnel Management Breach by China

56. As the House Oversight Report (*supra,* note 13) confirms, the 2015 breach exposed 21.5 million records containing SF-86 security clearance forms, which provided detailed information about millions of Americans and their families. Intelligence community sources have confirmed these records were used by Chinese intelligence to identify US intelligence officers operating under nonofficial cover.

57. The direct federal costs exceeded $500 million for remediation and identity protection services. Individual victims reported spending an average of over 200 hours resolving identity theft issues.

58. The 2015 breach began when attackers obtained legitimate credentials and escalated privileges, which is precisely the vulnerability being recreated by granting DOGE personnel unrestricted access without proper security controls.

59. The American intelligence community continues to deal with the fallout, as the compromised identity/profile data has, in the words of prominent privacy law scholar, Professor Daniel Solove of George Washington University Law School, a harm with "no end."[15]

The Ongoing Risk of Access

60. While any access to OPM's systems increases the security risks, ongoing access creates ongoing risks. That is because the longer that insecure access of the DOGE actors continues, the greater the chances of any of the breaches discussed above, and therefore any of the harms discussed above, occurring.

61. The risks are immediate, severe, and easily foreseeable, and may have already started happening, even if the consequences are not yet manifest. Quite often, the victims of identity theft and other injuries are not immediately aware of them—the knowledge comes when they receive an incorrect paycheck or benefits payment or are denied benefits entirely. It comes when they are informed of credit problems, billed for services that they did not seek or, worse, arrested or detained based upon incorrect or modified information about them.

62. The consequences for plaintiffs, whose data is now put at increased risk due to DOGE access to the entirety of the data that OPM holds about them, will be difficult if not impossible to fully remedy through money damages. The better option is to curtail any further sharing, and mitigate against the potential for breach by enjoining Defendants from accessing the

[15] https://www.linkedin.com/pulse/opm-data-breach-harm-without-end-daniel-solove

data entirely, and taking the other steps I outline below to at least try to block further harms from past access.

63. This is because once the data is taken by others—whether thieves or foreign adversaries—it becomes impossible in any meaningful sense to get it back in a way that entirely prevents or remedies ongoing harm. For instance, if a person suffers one identity theft as a result of the theft of personal data stored in the OPM database, some financial recovery can help but will never fully compensate them for the ongoing loss of the compromised credentials.

64. Additionally, the harm can be ongoing and can be repeated. Once released, the data can be reused multiple times. Similarly, access by one foreign adversary does not mean that another foreign adversary won't gain access via the same or a future breach.

65. This also means that even if the data has not been breached to date, future breaches or attacks are an ongoing risk. This is due to to ongoing access by people without sufficient training, experience, oversight, and limitations on use.

66. This also means that even if the data has already been taken by one set of thieves or spies, ongoing access by DOGE risks further attacks and breaches. Put another way, just because plaintiffs may already have been injured by the access and use of their data by Defendants, that does not mean that future, additional harm cannot occur due to continued access and use.

67. In sum, the more people who gain access to their data, and the longer that they have that access, the greater harms plaintiffs face. Preliminary injunctive relief will reduce the future harms plaintiffs may suffer due to DOGE access, even if some harm has already occurred.

DOGE Does Not Need Immediate, Full, and Uncontrolled Access to Personnel Data held by OPM to Fulfill Its Mandate

68. There is a vast difference between actual efforts to carefully and thoughtfully modernize OPM systems, which can be done in a way consistent with the Privacy Act, and what Defendants have done and continue to do.

69. The clearest evidence of this is in the resignation letter of February 25, 2025, from twenty-one members of the former US Digital Service (renamed DOGE) to White House Chief of Staff Susie Wiles.[16]

70. These civil servants, who were actually working to modernize many government systems when DOGE took over their renamed agency, noted that the new DOGE agents were "firing technical experts, mishandling sensitive data and breaking critical systems," in direct contradiction to their stated mission. These civil servants stated, "We will not use our skills as technologists to compromise core government systems, jeopardize Americans' sensitive data or dismantle critical public services."

Mitigation Steps

71. As a result of this reckless course of conduct, the Defendants are endangering the very systems they claim to be modernizing, as well as the people who rely on the security and privacy of those systems.

72. To address these vulnerabilities, five immediate steps are essential.

73. **Revoke Access.** DOGE access must be revoked and proper authentication protocols restored. Only after complete vetting and training, and only on an individual basis with

[16] https://www.documentcloud.org/documents/25544180-usds-resignation-letter/

a truly justified need, should access be restored, and only based upon the principle of least privilege access.

74. **Full Forensic Analysis.** A comprehensive forensic investigation should be conducted to identify all system modifications, data accesses, and potential persistence mechanisms established during the DOGE access period.

75. **Compromise Recovery.** OPM should treat all affected systems as potentially compromised, consistent with a Cyber Incident Response Plan in accordance with NIST SP 800-61r2.

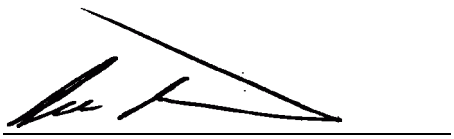
76. **Clean System Rebuild.** Critical authentication and authorization systems should be rebuilt from trusted media on clean hardware.

77. **Independent Security Assessment.** An independent security assessment should be conducted by qualified third-party experts (not affiliated with DOGE) to validate the effectiveness of remediation efforts.

78. Each day of continued unrestricted access makes the eventual recovery more difficult and increases the risk of irreversible damage to these critical systems and to the people whose data is stored in them. While the full impact may take time to assess, these steps represent the minimum necessary actions to begin restoring system integrity and security protocols.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on April 23, 2025.



Bruce Schneier

EXHIBIT A

EXHIBIT B