**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | |
|---|---|
| AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, *et al*.,<br><br>Plaintiffs,<br><br>v.<br><br>U.S. OFFICE OF PERSONNEL MANAGEMENT, *et al*.,<br><br>Defendants. | Case No. 25-cv-1237-DLC |

**MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION**

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Regulations**



**Other Authorities**

## INTRODUCTION

Congress passed the Privacy Act of 1974 following Watergate and the Counterintelligence Program (COINTELPRO) scandal "to restore trust in government and to address what at the time was seen as an existential threat to American democracy."[1] Trust had eroded after revelations about "White House enemies' lists," misuse of existing government personality profiles, and snooping on government employees.[2] In response to these legitimate concerns, Congress recognized that the federal government's increasing use of databases full of personal records "greatly magnified the harm to individual privacy" and sought to tightly limit their use by agencies. PL 93–579, 88 Stat 1896 (1974).

In passing the Privacy Act, Congress chose to protect the privacy of Americans, including government workers. It did so by sharply limiting the power of executive branch agencies to disclose information they collect. Congress also required the government to adopt high levels of security and protection against both internal and external threats.

Defendants' disclosures of personal records are violating the Privacy Act, irreparably harming Plaintiffs, and creating an imminent risk of more harm to Plaintiffs sufficient to justify a preliminary injunction. These are concrete injuries that satisfy Article III standing by analogy to longstanding common-law prohibition against intrusions on seclusion, among other privacy protections. Under cover of purported "efficiency" and "modernization," and despite language of the relevant executive orders requiring them to act consistent with existing law and "rigorous data protection standards," Defendants are inflicting the very harms that Congress passed the Privacy

---

[1] U.S. DOJ Overview of the Privacy Act of 1974, 1 (2020 Ed.), https://www.justice.gov/Overview_2020/dl?inline.

[2] Legislative History of the Privacy Act, 301 (1976), https://tile.loc.gov/storage-services/service/ll/llmlp/LH_privacy_act-1974/LH_privacy_act-1974.pdf.

Act to prevent. Specifically, the Office of Personnel Management ("OPM") is disclosing databases full of Plaintiffs' sensitive personal data to the so-called Department of Government Efficiency ("DOGE") and its agents.

Moreover, the paltry Administrative Record ("AR") produced so far in response to this Court's order demonstrates that Defendants granted high-level administrative access with power to modify OPM's critical systems and data to inexperienced new hires, while sidelining the civil servants with long experience protecting those systems against external breach or internal misuse—in flagrant disregard of the careful security protections and access limitations required by the Privacy Act. Evidence shows that some DOGE agents obtained OPM records without vetting or oversight, and many are employees of other agencies. Moreover, the AR gives no reason why DOGE agents need access and the ability to alter such a massive number of sensitive personal records and systems to fulfill any legitimate governmental duty.

These actions violate longstanding, bedrock security practices that protect both the systems and the information stored in them from intentional harms and unintentional breaches. For instance, DOGE's actions violate the principle of separation of duties, which prevents any single person from having the ability to access and modify critical parts of a system or set of systems. DOGE's actions separately violate the principle of least privilege, which provides that a user should have only those minimum rights, roles, and permissions required to perform their roles and responsibilities.

Thus, Plaintiffs have a likelihood of success on the merits of their claims that Defendants have violated the Administrative Procedures Act ("APA") because their actions are not in accordance with the Privacy Act's non-disclosure and cybersecurity rules. Plaintiffs also are likely to prove that Defendants violated the APA's ban on arbitrary and capricious actions, and that

DOGE Defendants acted ultra vires.

A preliminary injunction is further warranted here because the longer Defendants are allowed to violate the law, the greater the actual harms suffered by Plaintiffs from disclosure of their data by OPM to DOGE Defendants, who have shown a willingness to retaliate against federal workers. Even without malicious behavior by DOGE, Plaintiffs also are at imminent risk of harm from hacking, leaks, and breaches because of the lack of proper cybersecurity safeguards. A preliminary injunction is needed to stop any current misuse of the data and prevent further damage and risk to Plaintiffs.

## FACTS

### The Executive Order

On January 20, 2025, President Trump signed an executive order establishing DOGE for the purpose of "modernizing federal technology and software." Exec. Order No. 14,158, 90 C.F.R. 8441 (2025) ("E.O."). The E.O. creates three sets of DOGE actors: (1) it renames the existing "U.S. Digital Service" to the "U.S. DOGE Service" ("USDS"); (2) within USDS, it creates "the U.S. DOGE Service Temporary Organization" ("Temporary Organization") for 18 months; and (3) it directs other agencies to establish internal "DOGE Teams" to implement "the President's DOGE Agenda." § 3(a)-(c).[3]

Individuals working for USDS and the Temporary Organization are employees of USDS. § 3(a)-(b). Individuals who make up "DOGE Teams" established within OPM are primarily "Special Government Employees" who can be "hired or assigned" from other agencies, including USDS. § 3(c). DOGE Teams must "coordinate their work" with USDS. *Id.* The E.O. instructs

[3] "DOGE Defendants" are USDS, its Acting Director, the Temporary Organization, and Elon Musk.

agencies to grant USDS "full and prompt access to" records. § 4(b). But disclosure must be "consistent with law" and must be done with "rigorous data protection standards"—meaning that agencies must follow the Privacy Act. *Id.*

**DOGE Agents**

Starting in January 2025, at least seven DOGE agents (OPM-2 through OPM-8) were appointed to OPM. OPM-000006; OPM-000010; OPM-000014; OPM-000016; OPM-000022; OPM-000112; OPM-000116.[4] They are variously described as DOGE engineers, DOGE employees, or political tech staff. Ten other DOGE agents (OPM-9 through OPM-18) have access to OPM records, but the AR contains no evidence of their appointment to OPM. OPM-000089–90, OPM-000098, OPM-000103.

At least four DOGE agents (OPM-2, OPM-3, OPM-4, and OPM-7) receive no paycheck from OPM. OPM-000008–9, OPM-000012, OPM-000015, OPM-000113.

At least six DOGE agents (OPM-3, OPM-4, OPM-5, OPM-6, OPM-14, and OPM-16) each perform work at two or more agencies, in addition to OPM.[5] OPM-3 performs work for the Social Security Administration (SSA) and U.S. Department of Education. OPM-000013. While not disclosed in the AR, OPM-4, OPM-6, and OPM-14 are detailed to DOGE.[6] OPM-4 also is an

[4] This brief refers to DOGE agents by anonymized monikers (such as "OPM-2") and to AR pages by bates numbers (such as "OPM-000008"), which were assigned by Defendants in the public-facing AR. *See* Dkt. 66 (protective order) ¶ 4; ECF No. 78 (AR).

[5] OPM-000013; *AFL-CIO v. Dep't of Labor*, No. 1:25-cv-00339, ECF No. 73-2 at 10, 14 (D.D.C. Mar. 29, 2025) (Declaration of Victoria Noble ("Noble Decl."), Ex. A); *Brehm v. Marocco*, No. 1:25-cv-00660, ECF No. 7-3, at 2–3 (D.D.C. Mar. 6, 2025) (Noble Decl., Ex. B); *New York v. Trump*, No. 1:25-cv-01144, ECF No. 98-1, at 3–4 (S.D.N.Y. Mar. 5, 2025), *sub nom. New York v. U.S. Dep't of the Treasury* (Noble Decl., Ex. C); *Does 1-26 v. Musk*, --- F.Supp.3d ---, 2025 WL 840574, at *6 (D. Md. Mar. 18, 2025); *Nat'l Treasury Emps. Union v. Vought*, --- F.Supp.3d ----, 2025 WL 942772, at *5 (D.D.C. Mar. 28, 2025).

[6] Noble Decl., Ex. A at 10, 14.

employee of the General Services Administration and is detailed to the Department of Health and Human Services.[7] OPM-6 also works for the Consumer Financial Protection Bureau (CFPB).[8] OPM-14 also works for two other agencies.[9] OPM-5 worked for at least four other federal agencies.[10] OPM-16 works for at least two other agencies, including USADF, which terminated his detail assignment after, among other things, OPM-16 demanded same-day access to agency systems and threatened to fire agency officials if they failed to grant it.[11] The AR contains no agreement or memorandum of understanding limiting DOGE agents' disclosure of OPM data to DOGE Defendants. *Cf.* OPM-000013.

**Disclosures to DOGE Agents**

Starting on January 20, 2025, OPM gave DOGE agents access to its computer systems and disclosed the highly sensitive records of millions of Americans. Cybersecurity experts agree that the level of unrestricted access given to DOGE was not needed to accomplish its purported mission. Declaration of Ann Lewis ("Lewis Decl.") ¶ 7; Declaration of David Nesting ("Nesting Decl.") ¶¶ 11–31.

On January 20, 2025, OPM gave DOGE agents "administrator accounts with super user permissions" to access the USAJOBS records systems. OPM-000104. OPM gave access to

[7] Noble Decl., Ex. A at 10.
[8] Noble Decl., Ex. A at 14.
[9] *Brehm v. Marocco*, No. 1:25-cv-00660, ECF No. 7-4, at 3–4 (D.D.C. Mar. 6, 2025) (Noble Decl., Ex. D); *Nat'l Treasury Emps. Union*, 2025 WL 942772, at *5.
[10] *Musk*, 2025 WL 840574 at *6, *11 (U.S. Agency for International Development); *Nat'l Treasury Emps. Union v. Vought*, --- F.Supp.3d ----, 2025 WL 1144646, at *3 (D.D.C. Apr. 18, 2025) (Consumer Financial Protection Bureau); *Sustainability Institute, et al. v. Trump*, 2:25-cv-02152, ECF No. 67-2, at 5–6, 12, (D.S.C. Apr. 17, 2025) (Noble Decl., Ex. E) (U.S. Department of Agriculture); Noble Decl., Ex. C at 3–4 (Internal Revenue Service); *New York v. Trump*, No. 1:25-cv-01144, ECF No. 98, at 9 (Mar. 5, 2025) (Noble Decl., Ex. F) (same).
[11] Noble Decl., Ex. B at 3–4 (White House Personnel Office and USADF).

Amanda Scales, Greg Hogan, OPM Acting Director Charles Ezell, OPM-3, OPM-5, and OPM-7. *Id.* This access came in response to a "911-esque call," according to one OPM IT staff member. OPM-000107. There are no details of that call in the AR.

On January 27, 2025, other DOGE agents began receiving access to OPM systems, including USA Staffing, USAJOBS, and the Enterprise Human Resources Integration Data Warehouse ("EHRI"). That day, Defendant Ezell sent an urgent email to OPM's IT staff titled "Getting DoGE [sic] Engineers access." OPM-000028–29. Those engineers included OPM-2, OPM-4, and OPM-6. OPM-000028. Ezell said DOGE Engineers "don't have immediate plans to change anything but if we need to we might need to move quickly." *Id.* Ezell wanted a shortlist of "all the systems" at OPM. *Id.* For "each computer system," he said DOGE engineers needed "Code read and write permissions" and "regular user" and "admin user" permissions. OPM-000029.

In Defendants' haste, security protocols were cast aside for DOGE agents. In an email among OPM's existing IT staff, an employee noted that DOGE engineers "need to have access today," describing it as an "urgent request from political tech staff." OPM-000108. Before granting access, OPM's IT staff did not verify that the DOGE engineers had government-furnished equipment or personal identity verification ("GFE/PIVs"). OPM-000028. And DOGE agents—including one associated with past data mismanagement—were not vetted.[12] At the same time, career staff in OPM's Office of the Chief Information Officer were stripped of their own access permissions, preventing them from seeing what DOGE engineers were doing. OPM-000026. Ezell dismissed the need to follow standard security training, writing that DOGE engineers "won't have

[12] Jason Leopold, et al., "Musk's DOGE Teen Was Fired by Cybersecurity Firm for Leaking Company Secrets," *Bloomberg* (Feb. 7, 2025), https://www.bloomberg.com/news/articles/2025-02-07/musk-s-doge-teen-was-fired-by-cybersecurity-firm-for-leaking-company-secrets (Noble Decl., Ex. G).

a lot of time to go through a lot of presentations on what the systems are and what the program officers feel about the programs, etc." OPM-000027. Defendants' supplement to the AR confirms that in the rush to onboard DOGE employees, not everyone completed even the cursory training that was required prior to accessing protected systems. *See, e.g.*, OPM-000190, OPM-000193.

On February 3, 2025, Amanda Scales requested that another DOGE engineer, OPM-8, receive "admin access" to USA Staffing. OPM-000110. Scales appeared to make this request in an instant-message conversation. *Id.* Defendants did not provide the full conversation in the AR.

On February 6, 2025, *The Washington Post* reported that OPM's disclosures "alarmed security officials."[13] That same day, CIO Greg Hogan told OPM's IT staff, "I want to start unwinding peoples access if it is currently unnecessary." OPM-000027. Hogan noted that "we have never needed access to ERHI/eOPF." OPM-000026. OPM-2, OPM-4, and OPM-6 were removed from those two systems. OPM-000090-91. Still, at any time, DOGE agents could be reissued credentials to those systems, and those agents continue to access other systems. OPM-000089–91.

On Feb. 11, 2025, Plaintiffs filed this lawsuit. A day later, OPM's Acting Chief Information Security Officer began conducting an audit of "all internal OPM user accounts" created from January 20 to February 12, 2025. OPM-000054. *See also* OPM-000089–102 (Account Creation Audit).

Between January 24 and February 7, 2025, ten DOGE agents (OPM-9 through OPM-18) obtained access to USA Performance – Office of the Director. *See* OPM-0000103.

---

[13] Isaac Stanley-Becker, et al., *Washington Post*, "Musk's DOGE Agents Access Sensitive Personnel Data, Alarming Security Officials" (Feb. 6, 2025), https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/ (Noble Decl., Ex. H).

**OPM's Records Systems**

OPM acts as the "chief human resources agency and personnel policy manager for the Federal Government."[14] OPM's logs show that DOGE agents created accounts for at least 14 OPM systems. OPM-000089-091. Many of these systems contain sensitive personal information on millions of Americans. As current and former federal employees, Plaintiffs' and their members' records are in those systems. Kelley Decl. ¶ 4; Ramrup Decl. ¶ 3; Toussant Decl. ¶ 3.[15]

The Electronic Official Personnel Folder System ("eOPF") maintains information on current and former federal employees, including Social Security numbers, bank-account numbers, names and addresses, dates of birth, health and life-insurance-policy numbers, civil and criminal-history information, personnel actions like promotions and suspensions, race, national origin, and labor organization activities.[16] From January 28 to February 6, 2025, three DOGE agents (OPM-2, OPM-4, and OPM-6) had access to the eOPF. OPM-000089–91.

The Enterprise Human Resources Integration Data Warehouse ("EHRI") contains current and former federal employees' names, social security numbers, employment and appraisal histories, compensation and benefits, and personal contact information.[17] From January 28 to February 6, 2025, the same three DOGE agents that had access to the eOPF also had access to EHRI. OPM-000089–91. Among other things, eOPF and EHRI were used to populate a newly created government-wide email system. OPM-000119.

---

[14] "About Us," OPM, https://www.opm.gov/about-us.
[15] Plaintiffs' declarations were previously filed at ECF Nos. 29-31.
[16] OPM, "Privacy Impact Assessment for Electronic Official Personnel Folder System," (April 9, 2025), https://www.opm.gov/information-management/privacy-policy/privacy-policy/eopf-pia.pdf (Noble Decl., Ex. I). *See also* OPM-000058–59.
[17] OPM, "Privacy Impact Assessment for Enterprise Human Resources Integration Data Warehouse," (July 11, 2019), https://www.opm.gov/information-management/privacy-policy/privacy-policy/ehridw.pdf (Noble Decl., Ex. J).

USA Performance maintains information on federal employees, including names, social security numbers, work locations, positions, work plans, and self-assessments.[18] At least 17 DOGE agents continue to have access to that system. OPM-000089-91, OPM-000103.

USA Staffing maintains information from job applicants including names, addresses, citizenship statuses, and veterans' information. It can also include information like social security number, age, gender, work experience, and education.[19] Numerous DOGE agents continue to have access to USA Staffing's Admin Portal—and have used that access. OPM-000089–91, 103.

**Plaintiffs' Harm**

Plaintiffs claim ongoing harm to their fundamental right to privacy, as well as imminent harm from hacking by outsiders and improper retaliatory use by the government itself. Kelley Decl. ¶¶ 9–11; Ramrup Decl. ¶¶ 6–11; Toussant Decl. ¶¶ 4–6.

Cybersecurity experts agree that continued DOGE access creates an imminent risk of a future breach, including by foreign nations. Declaration of Bruce Schneier ("Schneier Decl.") ¶¶ 5, 28, 32–35, 42–54; Lewis Decl. ¶ 17; Nesting Decl. ¶¶ 42–43. The harm from another OPM breach would be substantial and devastating. Schneier Decl. ¶¶ 56–59; Nesting Decl. ¶ 42. The cybersecurity risks increase by the day. Schneier Decl. ¶¶ 63–67, 78.

Harm resulting from improper use of Plaintiffs' sensitive records by the government itself is also imminent and substantial. The administration already has discriminated against current

[18] OPM, "Privacy Impact Assessment for USA Performance," https://www.opm.gov/information-management/privacy-policy/privacy-policy/usap-pia.pdf (May 13, 2020) (Noble Decl., Ex. K).
[19] OPM, "Privacy Impact Assessment for USA Staffing," https://www.fhfa.gov/sites/default/files/2023-12/OPM%20USA%20Staffing_pia.pdf (July 28, 2021) (Noble Decl., Ex. L).

employees based on their demographic information[20] and retaliated against former employees.[21]

**ARGUMENT**

A "'plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.'" *New York v. U.S. Dep't of Homeland Security*, 969 F.3d 42, 58 (2d Cir. 2020) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)).

## I. PLAINTIFFS HAVE STANDING

The record before the Court establishes that Plaintiffs[22] have standing for the reasons explained in the Court's April 3, 2025, Opinion and Order denying in substance Defendants' motion to dismiss ("Order"). --- F.Supp.3d ----, 2025 WL 996542, at *4–9.

### A. Plaintiffs Have Been and Continue to Be Injured in Fact

The record shows that Plaintiffs have suffered and continue to suffer "harms analogous to intrusion upon seclusion." *Id*. at *6. The personnel "records at issue contain information about the deeply private affairs of the plaintiffs. *Id.* The records include, for example, social security numbers, health information, financial information, demographic information, and union activity. *Supra* at 8–9. For some Plaintiffs, "disclosure of the simple fact that they are included in the records could compromise their highly sensitive government roles." Order, 2025 WL 996542 at

[20] 90 Fed. Reg. 8757, E.O. 14183, "Prioritizing Military Excellence and Readiness," (Jan. 27, 2025) (discriminating against transgender military personnel).

[21] Presidential Memoranda, "Addressing Risks from Chris Krebs and Government Censorship," (April 9, 2025), available at https://www.whitehouse.gov/presidential-actions/2025/04/addressing-risks-from-chris-krebs-and-government-censorship/.

[22] The term "Plaintiffs" used herein encompasses both the individually named Plaintiffs and the union Plaintiffs' members on whose behalf the unions have associational standing. *Id*. at *4. The unions have each identified such a member, and the members' interests in this case are germane to the unions' purposes. Kelley Decl. ¶¶ 3, 6, 8–11; Ramrup ¶¶ 3, 5-6, 8–11.

*6; *see*, *e.g.*, Ramrup Decl. ¶¶ 6–7 (describing threats to judges); Schneier Decl. ¶¶ 21–22. Plaintiffs had every reason to expect that their OPM records would be carefully guarded and kept private and secure. Kelley Decl. ¶ 9; Ramrup Decl. ¶ 9–10; Toussant Decl. ¶ 4. "That is in fact what the Privacy Act requires." Order, 2025 WL 996542 at *6.

The record shows "that the DOGE agents demanded immediate access to OPM records" and "were given that access" as to at least 14 OPM systems. *Id*. at *7; OPM-000028–29; OPM-000104; OPM-000110; OPM-000089–102; *supra* at 5–7. As a legal matter, this is injury enough: "exposure of the plaintiff's personally identifiable information to unauthorized third parties, without further use or disclosure, is analogous to harm cognizable under the common law right of privacy." Order, 2025 WL 996542 at *7 (cleaned up). As a factual matter, there is more injury: evidence shows DOGE agents actually accessed those systems. Section II(A), *infra*. For instance, DOGE agents used the EHRI and eOPF databases to create a government-wide email system. OPM-000119. This confirms congressional letters and news reports, which also found that DOGE agents set up an outside server to control the personnel databases and DOGE agents searched through employee position descriptions. Section II(A), *infra*.

Moreover, Plaintiffs' records "were disclosed to DOGE agents in a rushed and insecure manner that departed substantially from OPM's normal practices." Order, 2025 WL 996542 at *6; Section II(B), *infra*. The "DOGE agents were not vetted, were not required to obtain security clearances, and were not trained about OPM security protocols and duties before the records were disclosed to them." Order, 2025 WL 996542 at *6; II(B), *infra*. DOGE agents "were even granted 'administrative' access, enabling them to alter OPM records and obscure their own access to those records." Order, 2025 WL 996542 at *6; OPM-000029; Lewis Decl. ¶¶ 7–8, 17. This intrusion upon Plaintiffs' "private affairs and confidential information was a substantial invasion of their

privacy and would be highly offensive to a reasonable person." Order, 2025 WL 996542 at *6. The record also shows that DOGE agents continue to possess Plaintiffs' confidential information. Order, 2025 WL 996542 at *7; OPM-000089–102.

Like the district court for the District of Columbia, this Court need not defer to the two-to-one decision of a Fourth Circuit panel to stay pending appeal a preliminary injunction in a related DOGE lawsuit on standing grounds, or the full court's eight-to-seven vote not to consider the matter en banc. *Am. Fed'n of Teachers v. Bessent*, No. 25-1282, 2025 WL 1023638, *1 (4th Cir. Apr. 7, 2025). Judge King, joined by five other judges, opined in a dissent that the district court had correctly found standing by analogy to intrusion upon seclusion. *Id.* at *9. Only two judges joined contrary opinions, meaning six judges who voted against en banc consideration have expressed no view on standing. As Judge Bates of the D.C. federal district court recently explained, in declining to defer to these two Fourth Circuit judges, one of their concurring opinions "dealt with Fourth Circuit precedent not binding on this Court," and the other misapplied the tort of intrusion on seclusion. *AFL-CIO v. Dep't of Labor*, --- F.Supp.3d ----, 2025 WL 1129227, at *7–8 (D.D.C. Apr. 16, 2025) ("*AFL-CIO*").

While the ongoing illegal disclosure of Plaintiffs' protected information to DOGE Defendants is enough to establish standing, Order, 2025 WL 996542 at *8, the current record also shows "that a risk of future harm exists and that the risk is substantial." *Id*. Record evidence shows that Defendant OPM gave:

> sweeping and uncontrolled access to DOGE agents who were not properly vetted or trained. That access included the ability to install and modify software and to alter internal documentation of access to the data. It identifies one of the DOGE agents as a 19-year-old who is known online as "Big Balls" and had been fired by a cybersecurity firm following an internal investigation into the leaking of proprietary information that coincided with his tenure. It explains as well that OPM is a target of cyberattacks, and that in 2015 OPM publicly disclosed that it had been subject to a data breach affecting over 20 million people. Because of the

> extraordinary access given to DOGE agents, U.S. security experts have already raised concerns that "Russia, China, Iran and other adversaries could seek to exploit the chaos by launching new cyber intrusions."

Order, 2025 WL 996542 at *8; sections II(B), III, *infra*; Schnier Decl. ¶¶ 5, 28, 32–35, 42–54; Lewis Decl. ¶ 17; Nesting Decl. ¶¶ 42–43. In addition to risk of data theft by third parties, there is also risk of data misuse by Defendants themselves. Kelley Decl. ¶ 11; Toussant Decl. ¶ 6; Ramrup ¶ 11; nn. 20–21, *supra*. The record evidence thus "amply [shows] the existence of risk necessary to support a finding of standing." Order, 2025 WL 996542 at *9.

Finally, Plaintiffs' injuries here also are analogous to claims for "disclosure of private information" and "harms specified by the Constitution." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021); Plaintiffs' Memorandum in Opposition to Motion to Dismiss, ECF No. 67 at 19–22. A fourth analogy is to the common law tort of "breach of confidence." *AFL-CIO*, 2025 WL 1129227 at *9.

**B. Causation and Redressability**

The record shows that Defendants caused and are causing Plaintiffs' injuries. The "OPM Defendants, who are responsible for the safekeeping of [P]laintiffs' records, disclosed them to DOGE agents without requiring those agents to be appropriately vetted or trained, and without limiting their access in the ways required by the Privacy Act." *Id*.; sections II(A), (B), *infra*.

"This harm is redressable through an injunction, which may prohibit improper disclosure from continuing and, to the extent that any information from OPM records has been copied, order that the information be impounded and destroyed." Order, 2025 WL 996542 at *9.

The AR and other record evidence thus show an injury in fact to Plaintiffs "caused by the defendants' illegal behavior, which may be redressed through a declaration and injunction." *Id*.

## II. PLAINTIFFS ARE LIKELY TO SUCCEED ON THEIR CLAIMS

### A. Defendants' Disclosures Violate Section (b) of the Privacy Act

Defendants "disclosed" OPM records in violation of 5 U.S.C. § 552a(b). OPM Defendants admit that they gave DOGE agents comprehensive access to at least 14 systems, including eOPF, EHRI, and several other OPM systems that contain Plaintiffs' sensitive records. OPM-000023, OPM-000028–29; OPM-000104; OPM-000089–110; Kelley Decl. ¶ 4; Ramrup Decl. ¶ 3; Toussant Decl. ¶ 3. "'[P]roviding' access to another person for their review of a record is a disclosure." Order, 2025 WL 996542 at *12.

But in addition, there is evidence of actual use in further violation of the statute. In a February 28, 2025, Privacy Impact Assessment, OPM described using the EHRI and eOPF databases to create a government-wide email system. OPM-000119. This confirms congressional letters and news reports, which also found that DOGE agents set up an outside server to control the personnel databases.[23] These reports also detail DOGE agents searching through employee position descriptions.[24] Further, DOGE agents were given "administrative access" (or "God Mode"), which would allow them to disable audit trails. Lewis Decl. ¶¶ 7–8; *Musk*, 2025 WL 840574 at *3. At other agencies, DOGE agents have been accused of using these permissions to hide the full extent of their access and use.[25]

---

[23] Letter from Rep. Gerald Connolly & Rep. Shontel Brown to Charles Ezell (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 (Noble Decl., Ex. M).

[24] Caleb Ecarma and Jedd Legum, "Musk associates given unfettered access to private data of government employees," *Musk Watch* (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered (Noble Decl., Ex. N).

[25] Declaration of Daniel J. Berulis (April 14, 2025), at ¶¶ 16, 19, 23, 27, available at https://whistlebloweraid.org/wp-content/uploads/2025/04/2025_0414_Berulis-Disclosure-with-Exhibits.s.pdf (describing "missing logs and disabled tooling" at the National Labor Relations Board) (Noble Decl., Ex. O).

Defendants cannot show that their unlawful disclosures fit within exception (b)(1), which allows disclosure only "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Many DOGE agents are not "of the" OPM, and no DOGE agent "needs" the records for any legitimate "duty." Nor does any other exception apply. Defendants bear the burden of proof here: "It is well settled that exceptions in the Privacy Act are affirmative defenses …" *Lombrano v. Air Force*, No. 21-cv-872 (DLF), 2022 WL 392308, at *5 (D.D.C. Feb. 9, 2022); *Doe v. FBI*, 936 F.2d 1346, 1353 (D.C. Cir. 1991) (government "bears the burden of demonstrating" an applicable exception to the Privacy Act).

**1. Many DOGE agents are not "of the" OPM.**

Many DOGE agents are functionally controlled and supervised by agencies other than OPM, including DOGE itself. Moreover, their federal onboarding paperwork is deficient. These are two independent reasons they are not "of the" OPM.

First, DOGE agents are functionally employees of DOGE or other agencies when they access OPM's records. To be employed by an agency, an employee must be "subject to the supervision" of that agency. 5 U.S.C. §2105(a)(3) (defining "employee"). When an employee is detailed to multiple agencies, courts can take a "functional approach that includes an evaluation of all the circumstances of the relationship, such as what work they do, where they work, and who supervises them." Order, 2025 WL 996542, at *13 (quoting *Jud. Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 131–32 (D.C. Cir. 2005)); *see also AFL-CIO*, 2025 WL 1129227 at *17 (describing initiatives, purposes, and supervision as relevant).

Here, when DOGE agents access OPM's records, they are functionally employees of DOGE or other agencies—not OPM. They are supervised by DOGE because they were hired in

"consultation with" DOGE and must "coordinate their work" with DOGE. E.O. § 3(c). Their work focuses on the "DOGE agenda," not OPM's agenda. *Id.* The DOGE agents do not answer to OPM officials. At other agencies, OPM-5 and OPM-16 directed the activities of agency officials based upon DOGE priorities.[26] OPM-16 threatened to fire high-ranking agency officials who refused his demands.[27] Moreover, at least six DOGE agents are simultaneously employed by multiple other federal agencies, including DOGE itself. *Supra*, n.5. And at least four DOGE agents receive no paycheck from OPM. OPM-000008–009, OPM-000012, OPM-000015, OPM-000113. Finally, the AR contains no agreement or memorandum of understanding that limits DOGE agents' disclosure of OPM data to DOGE. *Cf.* OPM-000013.[28] In the words of OPM Acting Director Ezell, these are "DoGE Engineers," OPM-000023–29, and "DOGE employees." OPM-000194.

Second, some DOGE agents did not finalize their employee paperwork with OPM before obtaining the agency's records, and the AR does not contain employee onboarding information for many others.[29] Government employees must generally complete a standard government form called a "Notification of Personnel Action" (SF 50), which details a person's position and is signed by an authorized official at the agency. *Horner v. Acosta*, 803 F.2d 687, 693–94 (Fed. Cir. 1986) (describing need to execute the form). Here, OPM-4 did not complete this form. Moreover, OPM-

[26] Noble Decl., Ex. E at 5–6, 12 (emails showing that OPM-5 directed USDA officials' "review" of climate change-related funding OPM-5 sought to "reallocate" and planned to introduce AI data analysis tools that DOGE was developing for use at "other agencies"); Ex. B, at 3–4 (stating that OPM-16 threatened to dismiss agency's entire board unless they gave DOGE same-day access to sensitive systems and approved DOGE team's plan to fire all agency staff, pursuant to "DOGE's interpretation" of agency's authorizing statute).

[27] Noble Decl., Ex. B at 3–4.

[28] Nor does any Memorandum of Understanding in the AR require DOGE agents to adhere to OPM polices, work at OPM facilities, use OPM devices, or report to OPM supervisors. *Cf.* OPM-000013. *Contra* Hogan Decl., ECF No. 40, ¶ 14.

[29] The AR is devoid of any evidence that ten DOGE agents (OPM-9 through OPM-18) were appointed or detailed to OPM.

6 and OPM-7 obtained OPM records on January 28, 2025, and January 20, 2025, respectively, but OPM did not finalize their employment documents until January 30, 2025. OPM-000021, OPM-000089–90, OPM-000111. *Cf. AFSCME v. Soc. Sec. Admin.*, --- F.Supp.3d ----, 2025 WL 868953, at *60 (D. Md. Mar. 20, 2025) (DOGE agents were not "employees" of agency until detail agreements were "finalized").

**2. No DOGE agent "needs" the records.**

Even if DOGE agents are OPM "employees" (and many are not), no DOGE agent has a "need" to know all the sensitive personal data they received from OPM to perform any legitimate governmental "duty." "In determining whether an official has a 'need' for a record within the meaning of § 552a(b)(1), courts consider 'whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly.'" Order, 2025 WL 996542 at *13 (quoting *Bigelow v. Dep't of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000)). The "unauthorized disclosure of millions of records" is "unlawful" absent a "showing of why each employee needed to receive the information." *Bessent*, 2025 WL 582063 at *11. No such showing appears in the AR.

Further, OPM officials' remarks demonstrate the absence of "need." *See Henson v. NASA*, 14 F.3d 1143, 1149 (6th Cir. 1994), *opinion corrected on reh'g*, 23 F.3d 990 (6th Cir. 1994) (evidence of officials' beliefs that some recipients of information did not need to know indicated absence of "need"). Hogan admitted that the DOGE agents "have never needed" the access they were given to highly sensitive systems. OPM-000026. Ezell requested—and obtained—comprehensive access that DOGE agents "don't have immediate plans" to use. OPM-000028. Hogan later suggested unwinding "currently unnecessary" access. OPM-000029.

The lack of "need" is also demonstrated by the mass resignation of the very government employees who had been tasked with IT modernization before Defendants' takeover. In a letter to the White House Chief of Staff, twenty-one civil servants employed by USDS (before its renaming) complained that DOGE agents were "firing technical experts, mishandling sensitive data and breaking critical systems."[30] These civil servants further stated, "We will not use our skills as technologists to compromise core government systems, jeopardize Americans' sensitive data or dismantle critical public services." *Id.*; *see also* Schneier Decl. ¶¶ 68–70.

Experts Nesting and Lewis also agree about the lack of need. They have deep experience in government and industry practices for building or modernizing IT systems that operate on private information. Nesting has direct experience at OPM as Deputy Chief Information Officer and Deputy Chief Data Officer. He stated that in his long experience with government systems, "it is not only possible, but vastly preferable to modernize IT systems without access to the data." Nesting Decl. ¶ 21. Nesting describes several government IT modernization projects across various government agencies in which he personally participated where there was no need for access to data, even for projects that required substantial code changes. ¶¶ 20–31 (Affordable Care Act system, Consular Consolidated Database, visa process systems, U.S. Refugee Admissions Program's (USRAP) case management system). He notes, "a team trying to modernize bank vaults doesn't need to have access to the contents of everyone's vaults." ¶ 15.

Similarly, Lewis, who most recently served as the Director of Technology Transformation Services at the U.S. General Services Administration, said it is her opinion that "DOGE's access

[30] Letter from USDS employees to White House Chief of Staff Susan Wiles (Feb. 25, 2025), available at https://www.politico.com/f/?id=00000195-3e8d-d4a2-afbf-fffd5d810000 (Noble Decl., Ex. P).

to sensitive OPM information is unnecessary for the purposes expressed by DOGE—and ignores vital security protocols." Lewis Decl. ¶ 7. Government IT modernization is not new, and DOGE's actions are "inconsistent with both the need to successfully modernize these systems and to do so securely." Lewis Decl. ¶ 23.

Likewise, the crafting of a federal hiring plan does not create a "need" for irrelevant records or information that cannot lawfully inform personnel decisions. Highly detailed records about millions of people who aren't even currently employed by federal agencies—like former employees and rejected job applicants—cannot reasonably inform a "data-driven plan" for staffing decisions. Nor can DOGE "need" access to data it cannot lawfully consider in making employment decisions, like an individual's union activity, race, disability, medical condition, or other protected characteristics. Further, OPM appointees do not "need" *any* of the information to direct terminations of other agencies' employees, given that OPM lacks the authority—let alone "duty"—to do this. *AFGE v. OPM*, --- F.Supp.3d ----, 2025 WL 820782 at *5 (N.D. Cal. Mar. 14, 2025).

**B. Defendants' Cybersecurity Failures Violate Section (e)(10) of the Privacy Act**

OPM and DOGE failed to "establish appropriate administrative, technical, and physical safeguards" to "insure the security and confidentiality of records" and "protect against any anticipated threats or hazards." § 552a(e)(10). This security provision is a simple, nondiscretionary mandate that OPM should know from litigation arising from its previous security breach. It requires agencies to "take basic, known, and available steps" to protect personal records. *In re OPM Breach Litig.*, 928 F.3d 42, 63 (D.C. Cir. 2019) (finding eight specific safeguards like

training, logging, and oversight that OPM previously neglected).[31]

Here, Defendants failed to establish vetting, access controls, oversight, policies, and training for DOGE agents. For example, inexperienced DOGE agents obtained "super user" and "admin" permissions with no use limitations almost immediately after the inauguration—before confirmation that they were using government-issued equipment and while experienced OPM staff were stripped of their access and oversight. OPM-000026, OPM-000029, OPM-000104. Despite working for multiple agencies, most DOGE agents were not required to sign agreements that limited their sharing with most other agencies, including DOGE itself. *Cf.* OPM-000013. DOGE itself does not have published security policies. And one DOGE agent, OPM-4, obtained records despite being fired from cybersecurity firm Path Network in 2022 following (according to a recent firm statement) "an internal investigation into the leaking of proprietary information that coincided with his tenure."[32] Another DOGE agent (OPM-5) obtained access to sensitive systems prior to completing a pre-appointment background investigation. OPM-000218.

From the start, officials emphasized that DOGE agents "won't have a lot of time" for training presentations to understand the records systems and security. OPM-000027. Defendants have only recently tried to paper over these deficiencies by supplementing the AR. But the supplement merely shows that some—but not all—DOGE agents self-certified that they had read a training document, which does not detail any of the specific records systems for which DOGE

[31] Defendants' compliance with § 552a(e)(10) is not "discretionary." 5 U.S.C. § 701(a)(2). Instead, the provision, previously enforced against OPM, provides a "meaningful standard" for agencies. *Weyerhaeuser Co. v. U.S. Fish & Wildlife Serv.*, 586 U.S. 9, 23 (2018). The evidence shows Defendants failed to establish safeguards—and radically departed from existing safeguards—regarding disclosures to DOGE agents.

[32] Noble Decl., Ex. G. This should have been flagged on Question 12 of the "Declaration of Federal Employment" (Form 306), which is not part of the AR. *Cf.* OPM-000193.

agents gained access.[33] Even if this constituted appropriate training for those systems (which it does not), that would not make up for Defendants' failure to establish other safeguards related to vetting, access, oversight, and policies. *See* Schneier Decl. ¶¶ 8, 29–39; Lewis Decl. ¶¶ 7–16; Nesting Decl. ¶¶ 36–37.

### C. Defendants Violated the APA

#### 1. Defendants' actions are not in accordance with law and are arbitrary and capricious.

Under the APA, courts can set aside agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706.

Since Defendants violated the Privacy Act, their actions are "not in accordance with law" under 5 U.S.C. § 706(2)(A). *See also AFSCME*, 2025 WL 868953 at *53 (describing Social Security Administration disclosures to DOGE).

Additionally, an agency decision is "arbitrary and capricious" in violation of the APA, 5 U.S.C. § 706(2)(A), if the agency failed to "consider an important aspect of the problem" or "articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Motor Vehicle Mfrs. Ass'n v. State Farm Ins. Co.*, 463 U.S. 29, 43 (1983) (quotation marks and citation omitted). Defendants failed to do either. Defendants disclosed "sensitive, confidential data of millions of Americans who entrusted their government with their personal and private information" articulating no "reasonable explanation for why the DOGE Team needs access to the wide swath of data." *AFSCME*, 2025 WL 868953 at *65; Section

[33] There is no evidence that OPM-3, OPM-4, OPM-6, or OPM-8 through OPM-18 completed this cursory training before gaining access to sensitive systems. Moreover, the training document purports to require employees to take a "final quiz which will rate your understanding of the information provided." OPM-000130. There is no evidence in the AR that any DOGE agent completed this quiz.

II(A), *supra*. Defendants also created serious cybersecurity risks by not establish vetting, access controls, oversight, policies, and training for DOGE agents. Section II(B), *supra*; Schneier Decl. ¶¶ 8, 58; Nesting Decl. ¶¶ 36–41; Lucas Decl. ¶¶ 7, 16–18. At the time of these decisions, OPM offered a wholly implausible explanation for why DOGE agents needed "urgent" access to systems they had no "immediate plans" to use: DOGE agents might "need to move quickly" if they later decided to make unspecified "changes." OPM-000028–29, OPM-000108. This "inexplicable urgency" does not justify "the serious risks that access entailed," nor does the E.O. itself. *New York v. Trump*, --- F.Supp.3d ----, 2025 WL 573771, at *21–22 (S.D.N.Y. Feb. 21, 2025).

Defendants' other attempts to justify their conduct are "impermissible *post hoc* rationalizations" not properly before this Court. *Dep't of Homeland Sec. v. Regents of the Univ. of California*, 591 U.S. 1, 22 (2020). The record contains no evidence that Defendants even considered the cybersecurity, national security, or privacy risks inherent in allowing unrestricted access to repositories of protected personal information. These failures render Defendants' actions arbitrary and capricious. *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43.

**2. There is final agency action.**

The APA provides for judicial review of "final agency action." 5 U.S.C. § 704. For an agency action to be "final," two conditions must be met: it "must mark the consummation of the agency's decisionmaking process," and it "must be one by which rights or obligations have been determined, or from which legal consequences will flow." *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997) (citation omitted). Courts take a "pragmatic approach" in analyzing finality. *U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 599 (2016). There is no requirement that there be a writing to memorialize a final agency action. *See Brotherhood of Locomotive Eng'rs & Trainmen*

*v. Fed. R.R. Admin.*, 972 F.3d 83, 100 (D.C. Cir. 2020); *Amadei v. Nielsen*, 348 F. Supp. 3d 145, 165 (E.D.N.Y. 2018).

Final agency action is shown here. In sharp contrast to normal cybersecurity procedures, Defendants decided to unlawfully disclose the sensitive OPM records of tens of millions of Americans to DOGE agents with no legal right or duty to access those records. Section II(A), (B), *supra*; Order, 2025 WL 996542 at *16–18. While done in a "911-esque" fashion, OPM-000107, the decision was neither tentative nor interlocutory. *Bennett*, 520 U.S. at 177–78. Finally, the disclosures have legal consequences for Plaintiffs by depriving them of their privacy rights under both the Privacy Act and the APA. Section II(A), C(1), *supra*; *see also Bennett*, 520 U.S. at 177–78*; Chrysler Corp. v. Brown*, 441 U.S. 281, 318–19 (1979); *Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 930–31 (D.C. Cir. 2008).

**3. There is no adequate alternative remedy.**

This Court already ruled that the Privacy Act does not provide the injunctive relief Plaintiffs seek. Order, 2025 WL 996542 at *18. Therefore, if that remains so, Plaintiffs have no adequate recourse to remedy the ongoing harm other than injunctive relief under the APA. *Id.*

**D. The DOGE Defendants Have Acted Ultra Vires**

Plaintiffs are likely to prevail on their ultra vires claim, which is pleaded against the DOGE Defendants alone and asserts that no law permitted them to access and administer OPM systems. An ultra vires claim is available where a governmental official or entity's action "plainly" exceeds its lawful authority, is "contrary to a specific prohibition in the statute that is clear and mandatory," a statutory claim is unavailable because a provision implicitly precludes the claim from review, and there is not an alternative procedure to review it. *Yale New Haven Hosp. v. Becerra*, 56 F.4th 9, 26–27 (2d Cir. 2022) (quotation omitted). "When an executive acts ultra vires, courts are

normally available to reestablish the limits on his authority." *Open Society Justice Initiative v. Trump*, 510 F. Supp. 3d 198, 214 (S.D.N.Y. 2021).

The DOGE Defendants' actions are "plainly beyond the bounds" and "clearly in defiance" of any authority DOGE Defendants possess and thus are ultra vires. *See Fed. Express Corp. v. U.S. Dep't of Com.*, 39 F.4th 756, 764 (D.C. Cir. 2022). Specifically, in directing and controlling the use and administration of Defendant OPM's systems, DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of Americans to DOGE agents that had not yet been fully vetted or trained, and in ways grossly inconsistent with settled security requirements in violation of the Privacy Act. Sections II(A), (B), *supra*. The DOGE Defendants directed and induced the violations of Sections (b) and (e)(10) of the Privacy Act, and there is no Privacy Act exception that applies, as explained above. Sections II(A), (B), *supra*.

The DOGE Defendants' "blatantly lawless" direction of mass disclosures violate the Privacy Act, far exceed their legitimate authority, and are thus ultra vires. Order, 2025 WL 996542 at *20; *Fed. Express Corp.*, 39 F.4th at 764; *see also Nat'l Ass'n of Letter Carriers*, 604 F. Supp. 2d at 673 (entertaining claim for injunction for ultra vires conduct for Privacy Act violations). Thus, Plaintiffs are likely to prevail on their ultra vires claim.

## III. ONGOING DISCLOSURE OF PLAINTIFFS' SENSITIVE RECORDS CONSTITUTES IRREPARABLE HARM

Plaintiffs continue to suffer irreparable harm in the form of unlawful disclosure and security of their records, which the Court already has found cannot be fully remedied by future money damages. "Each day of continued unrestricted access makes the eventual recovery more difficult and increases the risk of irreversible damage[.]" Schneier Decl. ¶ 78; *see also* Nesting Decl. ¶ 41 (in legacy systems, "sensitive information stored in them can be lost, altered or

compromised in ways that cannot be remedied.").

"To satisfy the irreparable harm requirement, plaintiffs must demonstrate that absent a preliminary injunction they will suffer an injury that is neither remote nor speculative, but actual and imminent, and one that cannot be remedied if a court waits until the end of trial to resolve the harm." *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quoting *Grand River Enter. Six Nations, Ltd. v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007)). Plaintiffs need only show a "threat of irreparable harm, not that irreparable harm already have occurred." *Mullins v. City of New York*, 626 F.3d 47, 55 (2d Cir. 2010); *see also Arias v. Decker*, 459 F. Supp. 3d 561, 571 (S.D.N.Y. 2020) (increased risk of severe infection in immigration detention constitutes irreparable harm).

"The disclosure of private, confidential information 'is the quintessential type of irreparable harm that cannot be compensated or undone by money damages.'" *Airbnb, Inc. v. City of New York,* 373 F. Supp. 3d 467, 499 (S.D.N.Y. 2019) (quoting *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000)); *see also Trump v. Deutsche Bank AG*, 943 F.3d 627, 637 (2d Cir. 2019), v*acated and remanded on other grounds sub nom. Trump v. Mazars USA, LLP*, 591 U.S. 848 (2020) (citation omitted) ("compliance with the subpoenas" seeking plaintiffs' personal information "would cause irreparable harm because 'plaintiffs have an interest in keeping their records private from everyone, including congresspersons'"); *Microsoft Corp. v. Does 1-2*, No. 23-CV-02447-LDH-JRC, 2023 WL 11984986, at *2 (E.D.N.Y. Apr. 19, 2023) ("immediate and irreparable harm will result from Defendants' ongoing violations of . . . the Electronic Communications Privacy Act…"); *Bessent*, 2025 WL 895326 at *31 ("In line with courts in the Second, Fifth, and Ninth Circuits, this Court finds that the ongoing disclosure of the plaintiffs' [personally identifiable information] to government employees not authorized to access it

constitutes irreparable harm.").

And courts "in the Second Circuit have repeatedly found that the future risks of disclosure of PII can amount to irreparable harm satisfying the injunctive relief standard, as long as the expectation of privacy is reasonable." *Trump*, 2025 WL 573771 at *25; *id*. at *26 (ruling that plaintiffs "sufficiently allege[d] irreparable harm from the risk of 'expanded access' to the BFS payment systems that will possibly compromise the systems to become 'far more vulnerable to hacking or activities that render the information corrupted or compromised.'").

Absent a preliminary injunction, Plaintiffs will continue to suffer irreparable harm because their sensitive records are being unlawfully disclosed to government agents who do not need them. Section II(A), *supra*. Moreover, an injunction is needed to prevent DOGE agents from receiving expanded access to Plaintiffs' records, given Defendants' incorrect position that DOGE agents need the records. Plaintiffs have an interest in maintaining the confidentiality of their sensitive records that they gave to the government, and the Privacy Act gives "forceful recognition" to that right. *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 156 (2011).

In addition to the ongoing harm of disclosure itself, Plaintiffs reasonably fear that Defendants will use the information against them by, *e.g.*, terminating Plaintiffs' employment based on information DOGE agents have no right to access in the first place or cutting off their benefits. Kelley Decl. ¶ 11; Toussant Decl. ¶ 6; Ramrup Decl. ¶ 11. Given this administration's unlawful actions directed at current and former government workers, these fears are not speculative.[34]

Finally, Plaintiffs will be irreparably harmed without a preliminary injunction because the DOGE Defendants' ongoing access significantly compromises the security of OPM's systems that

[34] *See, e.g.*, Presidential Memoranda, n.21, *supra*; E.O. 14183, n.20, *supra*.

contain Plaintiffs' personal information. *See Trump*, 2025 WL 573771 at *26. DOGE's access has compromised the cybersecurity of Plaintiffs' personnel records, significantly heightening the risk that their information will be far more vulnerable to hacking, or that their personnel files will be compromised. Schneier Decl. ¶¶ 14–28, 43–47; Lewis Decl. ¶ 17; Nesting Decl. ¶¶ 42–43. Foreign adversaries typically spend years attempting to penetrate U.S. government systems. Schneier Decl. ¶ 43. DOGE agents have likely "left behind vulnerabilities that could be exploited in future attacks." *Id.* ¶ 44. Moreover, "every hacker in the world" now knows inexperienced DOGE agents "hold the keys" to these sensitive systems. Lewis Decl. ¶ 17. Defendants are "fully aware of the risks" of granting DOGE agents "broad access" to agency systems, which on at least one occasion led to errors in which a separate federal agency's system was misconfigured and unauthorized external disclosures of PII that violated security protocols.[35]

## IV. THE BALANCE OF EQUITIES FAVORS PLAINTIFFS

To obtain preliminary injunctive relief, Plaintiffs must also show that the balance of equities tips in their favor, and that the injunction is in the public interest. *Homeland Security*, 969 F.3d at 58. When the federal government is a party, these factors merge. *Nken v. Holder*, 556 U.S. 418, 435 (2009).

Plaintiffs' "extremely high likelihood of success on the merits is a strong indicator that a preliminary injunction would serve the public interest." *League of Women Voters of U. S. v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016); *see also Saget v. Trump*, 375 F. Supp. 3d 280, 377 (E.D.N.Y. 2019) (citing *Issa v. Sch. Dist. of Lancaster*, 847 F.3d 121, 143 (3d Cir. 2017)) ("Because Plaintiffs have shown both a likelihood of success on the merits and irreparable harm, it is also likely the

[35] *Trump*, No. 1:25-cv-01144, ECF No. 34, ¶¶ 11, 15, 20 (S.D.N.Y. Feb. 11, 2025) (Noble Decl., Ex. Q); *id.*, ECF No. 116-1, ¶¶ 9, 12 (S.D.N.Y. Mar. 14, 2025) (Noble Decl., Ex. R).

public interest supports preliminary relief.").

Moreover, "'[t]here is generally no public interest in the perpetuation of unlawful agency action. To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations.'" *New York v. Trump*, 490 F. Supp. 3d 736, 747 (S.D.N.Y. 2020) (quoting *League of Women Voters*, 838 F.3d at 12); *see also Planned Parenthood of N.Y.C. v. U.S. Dep't of Health and Hum. Servs.*, 337 F. Supp. 3d 308, 343 (S.D.N.Y. 2018) (collecting cases). Individual privacy is an important public interest. *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994). The public also has a strong interest in protecting federal workers' data, including against foreign nations. *TikTok Inc. v. Garland*, 145 S. Ct. 57, 69 (2025). Defendants' actions threaten national security by making OPM's systems more vulnerable to cyberattacks by foreign adversaries and intelligence services. Schneier Decl. ¶¶ 43–47. All these concerns strongly weigh in favor of granting a preliminary injunction. *See Trump*, 2025 WL 573771 at *26; *Bessent*, 2025 WL 895326 at *31–32.

## CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court grant their motion for a preliminary injunction.

Dated: April 25, 2025

Respectfully submitted,

*/s/ Rhett O. Millsaps II*
Rhett O. Millsaps II
Mark A. Lemley (admitted pro hac vice)
Mark P. McKenna (admitted pro hac vice)
Christopher J. Sprigman
LEX LUMINA LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
(646) 898-2055

F. Mario Trujillo (admitted pro hac vice)
Victoria Noble
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Norman L. Eisen (admitted pro hac vice)
STATE DEMOCRACY DEFENDERS FUND
600 Pennsylvania Avenue SE #15180
Washington, DC 20003

Subodh Chandra (admitted pro hac vice)
THE CHANDRA LAW FIRM LLC
The Chandra Law Building
1265 W. 6th Street, Suite 400
Cleveland, OH 44113

*Counsel for Plaintiffs*

**CERTIFICATE OF COMPLIANCE**

I certify that, excluding the caption, table of contents, table of authorities, signature block, and this certification, the foregoing Memorandum of Law in Support of Plaintiffs' Motion for Preliminary Injunction contains 8,500 words, calculated using Microsoft Word for Mac, which complies with Rule 7.1(c) if the Local Rules of the United States District Courts for the Southern and Eastern Districts of New York.

Dated: April 25, 2025

/s/ *Rhett O. Millsaps II*
Rhett O. Millsaps II