UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AFL-CIO, et al., *Plaintiffs*, *vs.* U.S. Department of Labor, et al., *Defendants*.	Case No. 1:25-cv-339-JDB

PLAINTIFFS' MEMORANDUM IN SUPPORT OF THEIR MOTION FOR A PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Other Authorities

INTRODUCTION

Discovery in this case has confirmed just what Plaintiffs have argued. The Department of Labor (DOL) and the Department of Health and Human Services (HHS) have given members of the DOGE Teams working at their agencies unfettered, on-demand access to their most sensitive systems of records. These systems contain deeply personal information, including Social Security numbers, bank account information, and medical diagnosis and procedure codes. The agencies have granted this access without even attempting to identify a particularized need for access to these systems, as required by the Privacy Act, let alone finding that one exists. Requests for access are fast tracked. Normal systems and security training are ignored. And if DOGE Team members seek to access additional systems, DOL and HHS will permit them. HHS, for example, could identify neither an unclassified system of records to which DOGE Team members would be denied access nor a possible reason for a denial.

In lieu of the careful, system-by-system and user-by-user approach contemplated by the Privacy Act, DOL and HHS merely invoke the incantation of "waste, fraud, and abuse" to justify granting access to any system DOGE Team members choose, no matter how sensitive. But "waste, fraud, and abuse" are not magic words, and they cannot conjure up a need to grant DOGE Team members on-demand access to Americans' most sensitive and personal information. In any event, this justification is merely illusory: Both Agencies now claim that Executive Orders required them to grant DOGE Team members access to sensitive systems to review them for waste, fraud, and abuse. But the first relevant Executive Order mentioning waste, fraud, and abuse was issued weeks *after* DOL and HHS granted DOGE Team members access to sensitive systems. Absent this illusion, it becomes clear that the agencies have no other justification for granting access to DOGE Team members. DOGE Team members have no need to access this

information, their access is unlawful, and they have violated the rights of millions of Americans who have relied on the United States government to protect their private information.

For these reason, Plaintiffs American Federation of Government Employees ("AFGE"), American Federation of State, County & Municipal Employees, AFL CIO ("AFSCME"), Service Employees International Union, AFL-CIO ("SEIU"), Communication Workers of America, AFL-CIO ("CWA"), and American Federation of Teacher ("AFT") (collectively, "Plaintiffs") now seek a preliminary injunction to halt DOGE Team members' access to their members private information and prohibit DOL and HHS from granting the DOGE Team access to additional sensitive systems.

FACTUAL BACKGROUND

I. The Department of Government Efficiency

On the day of his inauguration, President Trump issued an executive order establishing the "Department of Government Efficiency," or "DOGE." Ex. 1, Exec. Order No. 14,158, 90 Fed. Reg. 8,441 (Jan. 20, 2025) ("Jan. 20 EO"). DOGE was tasked with "implement[ing] the President's DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity." *Id.* § 1. The Order envisioned the work of "DOGE" being implemented across at least three different entities:

1. the U.S. DOGE Service ("USDS") (formerly the U.S. Digital Service), established within the Executive Office of the President and headed by the USDS Administrator;

2. the U.S. DOGE Service Temporary Organization ("USDS TO"), also headed by the USDS Administrator and established within the Executive Office of the President; and

3. "DOGE Teams," teams of individuals within each federal agency who "coordinate their work with USDS and advise [] Agency Heads on implementing the President's DOGE Agenda."

Id. § 3(a)-3(c).

While the two White House entities are formally led by the USDS Administrator, President Trump "put [] Elon Musk in charge" of the overall DOGE effort.[1] An associate of Mr. Musk's named Steve Davis serves as the "Chief Operating Officer" of DOGE.[2] Mr. Davis is formally a Senior Advisor within the USDS TO, and detailed to the General Services Administration. Ex. 2 (Rule 30(b)(6) Dep. of DOGE) ("DOGE Dep.") at 15:5-23, 87:6-18. Mr. Davis exercised the decision-making authority of the USDS Administrator until February 18, when Amy Gleason was formally appointed as the Acting USDS Administrator. *Id.* at 12:20-15:4. Mr. Davis also provides advice to DOGE Teams on "how he might implement the President's DOGE agenda." *Id.* at 15:20-16:8.

DOGE Teams within federal agencies are themselves made up of at least the following categories of employees:

1. Employees of USDS or the USDS TO, who are either detailed to or concurrently employed by other agencies to serve on their DOGE teams; *see*, *e.g.* Ex. 3 (Defs.' Objections & Responses to Pls. Requests (Apr. 4, 2025)) ("Defs. Responses") at 6, 17, 20 (identifying individuals as USDS employees concurrently employed by federal agencies);

2. Employees of the General Services Administration or Office of Personnel Management, who are either detailed to or concurrently employed by other agencies to serve on their DOGE Teams; some of these employees may also be concurrently detailed to one of the USDS entities; *see*, *e.g.*, Ex. 3 (Defs.' Responses) at 8, 10, 14, 20 (identifying GSA and OPM employees who are detailed to or employed by federal agencies as part of their DOGE teams); Ex. 2, (DOGE Dep.) at 68:2-11.

3. Employees of the federal agencies themselves, although many of these employees may also be detailed to or concurrently employed by other agencies, including to

[1] *See* "Remarks by President Trump at Future Investment Initiative Priority Summit," https://www.whitehouse.gov/remarks/2025/02/press-gaggle-by-president-trump-at-future-investment-initiative-institute-priority-summit/.
[2] *See*, *e.g.*, Fox News, "Elon Musk and DOGE team give behind the scenes look at their mission," YouTube (Mar. 27, 2025). https://www.youtube.com/watch?v=l7kQNwJ4H_w.

USDS; *see*, *e.g.*, Ex. 3, (Defs.' Responses) at 14-15, 17-19 (identifying DOGE Team members who are employees of Defendant Agencies).

Concurrent employment across multiple agencies is typical for DOGE Team members,[3] who could be working for eight or more agencies in their DOGE capacity at any given time. *See* Ex. 2 (DOGE Dep.) at 93:4-16.

When USDS and USDS TO personnel are employed by or detailed to a federal agency, they have "two functions . . . relate[d] to the same agency"—one as an "agency employee" and another as a USDS staffer "consulting with" the agency. *See id.* at 87:19-88:24. So, for example, a USDS or USDS TO employee can recommend that they be onboarded to an agency as a member of the agency's DOGE team. *See* Ex. 4 (Rule 30(b)(6) Dep. of HHS) ("HHS (Rice) Dep.") at 19:23-20:19 (USDS TO employee Brad Smith "recommend[ed] that he be detailed to HHS," which he was).

II. The Three Executive Orders Setting Forth DOGE's Responsibilities

Sections 1 and 4(a) of the January 20 EO identify the purpose of DOGE as focused on the government's computer technology. Section 1, called "Purpose," states in full: "This Executive Order establishes the Department of Government Efficiency to implement the President's DOGE Agenda, by modernizing Federal technology and software to maximize government efficiency and productivity." Section 4(a) is called "Modernizing Federal Technology and Software to Maximize Efficiency and Productivity," and consists of two sentences. The first instructs the Administrator of the United Staes DOGE Service to "commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network

[3] Reflecting an Order issued by the Court with respect to discovery, "DOGE Team members" refers to "individuals that the defendant agencies have onboarded for purposes of carrying out the DOGE Agenda, including those the agencies have directly hired or received as detailees." ECF 75 at 4-5.

infrastructure, and information technology (IT) systems." The second identifies the projects that "DOGE Teams" are to undertake at federal agencies: "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization."

To facilitate these projects, section 4(b) directs Agency Heads "to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems." This directive is qualified by the phrase, "to the maximum extent consistent with law," and adds that "USDS shall adhere to rigorous data protection standards."

The words "waste," "fraud," and "abuse" do not appear in the January 20 EO.

The next Executive Order pertaining to DOGE was issued on February 26, 2025, and is called "Implementing the President's 'Department of Government Efficiency' Cost Efficiency Initiative." Ex. 5("Feb. 26 EO"). It addresses "Federal spending on contracts, grants, and loans," *id.* § 1 (Purpose), but with two substantial exclusions: it only applies to discretionary spending, and it does not apply to "direct assistance to individuals; expenditures related to immigration enforcement, law enforcement, the military, public safety, and the intelligence community; and other critical, acute, or emergency spending, as determined by the relevant Agency Head," *id.* § 2(d). The only section that addresses waste, fraud, and abuse is 3(b), which calls for a review of "covered" contracts. The other directives concern building a system to record payments and justifications; reviewing contracting policies, procedures, and personnel; issuing new contract guidance; creating a system for travel justifications; and the agency's real property, *id.* §§ 3(a), (c)-(g). In many places, these are expressly limited by "applicable law" or equivalent terms.

The third and most recent DOGE Executive Order, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos," was issued on March 20, 2025. Ex. 6 ("March 20 EO"). It

calls for officials designated by the President or agencies to "have full and prompt access to all unclassified agency records, data, software systems, and information technology systems" for "the identification of waste, fraud, and abuse." *Id.* § 3(a). Again, this is limited by "to the maximum extent consistent with law." *Id.*

The March 20 EO also calls for the Secretary of Labor or her designee—"to the maximum extent consistent with law"—to have "unfettered access to all unemployment data and related payment records, including all such data and records currently available to the Department of Labor's Office of Inspector General." *Id.* § 3(d).

By its terms, each executive order ostensibly "shall be implemented consistent with applicable law." Ex. 1 (Jan. 20 EO) at § 5(b); Ex. 5 (Feb. 26 EO) at § 5(b); Ex. 6 (March 20 EO) at § 4(b).

III. DOGE Team Members Have Been Given Broad Access to Sensitive Systems at HHS and DOL

DOGE Team members have been given access to a number of system of records housed at Defendant Agencies containing Personally Identifiable Information (PII) and/or Personal Health Information (PHI) (collectively, "Sensitive Systems"). *See also* ECF No. 48 at 12 (adopting this definition of Sensitive Systems for the purposes of expedited discovery in this matter). In a subsequent Order, the Court explained that the Privacy Act "requires that the employee [to gain access to relevant information] 'have a need for the record in the performance of their duties.'" ECF 71 at 10 n.12 (quoting 5 U.S.C. § 552a(b)(1)). The Court permitted discovery in part because of its relevance "to the question of whether the USDS staffers working at defendant agencies (direct hires or otherwise) have 'a need for the record[s]' they are or were accessing." *Id.*

Discovery has shown that each agency rests its determination that the Privacy Act's "need" requirement is met as to every Sensitive System by virtue of nothing more than the DOGE Executive Orders, and typically the January 20 EO standing alone. The January 20 EO, according to HHS and DOL, alone justifies giving all the DOGE Teams essentially unfettered access to their Sensitive Systems without any further or more particularized demonstration of need.

In other words, discovery has revealed that HHS and DOL have created and applied a new *de facto* policy for DOGE Teams and nobody else: DOGE Teams get access to the all the unclassified systems they want. Team members do not have to explain a particularized need for access and the Agencies do not have to confirm a particularized need. System and security trainings required of everyone else to access these systems are optional for DOGE Teams and frequently have not been completed. Plaintiffs challenge these agency DOGE Data Access Policies as unlawful.

A. Department of Labor

Three DOGE Team members have been given access to, collectively, eight Sensitive Systems. *See* Ex. 3 (Defs.' Responses) at 17-20.[4] Access has only been denied to two systems. One was because of separate litigation involving the Department of the Treasury's access to the same system. The other was due to a software limitation preventing read-only access. *See* Ex. 7 (Rule 30(b)(6) deposition of DOL) ("DOL Dep.") at 87:17-88:20.

[4] The DOL systems are: USAccess; HSPD-12 Enterprise Physical Access Control System; Directory Resource Administrator; Unemployment Insurance Data and Related Records; HR Connect; New Core Financial Management System; Payment Management System; and Office of Job Corps Electronic Information System. *See* Ex. 3 (Defs.' Responses) at 17-19.

One of these Sensitive Systems, for example, is the Unemployment Insurance Data and Related Records. It contains unemployment insurance claims data from state agencies. The PII in this system includes social security numbers, addresses, and bank account information. *See id.* at 59:9-60:16. DOGE Team members have also been granted access to a system called USAccess, which provides Personal Identity Verification to federal agencies for employees, U.S. General Services Administration, "About USAccess," https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/federal-credentialing-services/about-usaccess, and includes names, birthdates, and Social Security numbers, Ex.11 (Request to Access DOL Information System) at 2.

DOL primarily cites the January 20 EO as the basis for providing the DOGE Team members with access to the Department's Sensitive Systems. *See* DOL Dep. at 76:21-77:1, 78:15-20. DOL claims that, standing alone, that Executive Order makes it "apparent" that there is a legitimate need for access. *Id.*; *see also id.* at 72:9-19, 75:11-19; 78:15-79:11. DOL relies on no other information to determine that DOGE Teams must be given access. *See id.* at 79:12-18. This contrasts sharply with the process when other DOL employees seek access. They are asked various questions that DOGE Team members are not asked in what DOL confirmed is a "robust analysis" of an employee's need for access. *See id.* at 59:1-8, 75:20-76:20.

Defendants justify their reliance on the January 20 EO by invoking the mantra of waste, fraud, and abuse. *See id.* at 21:17-22, 34:10-35:1, 41:14-42:5, 42:16-43:3, 126:22-127:18. And, as a factual matter, DOGE Team members at DOL had access to Sensitive Systems when only the January 20 EO existed. Ex. 3 (Defs.' Responses) at 17-20. But the January 20 EO does not mention waste, fraud, or abuse at all. *See* Ex. 1 (Jan. 20 EO).

The February 26 EO, in contrast, does mention waste, fraud, and abuse, *see* Ex. 5 (Feb. 26 EO), but DOL has made no attempt to rely on it. Nor has it given any indication in its written discovery responses, the documents it produced, or its testimony that it ever considers the distinction in the February 26 EO between "covered" contracts and grants and the large category of programs excluded from the Executive Order's reach, a necessary consideration for that EO.

In addition to dispensing with individualized analysis of DOGE Teams' justifications for accessing agency data, DOL also has dispensed with its security requirements in providing access to DOGE Teams, despite assuring the Court that it would "establish confidentiality protocols" for their access to DOL systems. Ex. 10 (Decl. of R. Kryger) (ECF 31-1) at ¶ 9. It has done so in at least three ways:

- *Not requiring User Agreements.* The Office of DOL's Chief Information Officer has a "User Agreement" form that, ostensibly, must be signed by all DOL employees and contractors before accessing Sensitive Systems. Ex. 7 (DOL Dep.) at 109:2-110:12. The form confirms that the user "has completed the standard computer security training for DOL." *Id.* at 109:12-16. Aram Moghaddassi's form is not signed. *See* Ex. 8 (Moghaddassi User Agreement). Elez Marko's form was not signed until March 25, 2025. *See* Ex. 9 (Marko User Agreement). DOL's representative testified that Moghaddassi should not have been given access to Sensitive Systems, and that Elez should not have been prior to March 25. *See* Ex. 7 (DOL Dep.) at 110:13-112:4. Yet Moghaddassi was given access to five Sensitive Systems, and Elez to four—all before March 25. *See* Ex. 3 (Defs.' Responses) at 17-18.

- *Not requiring agreement to Rules of Behavior*. DOL stated in interrogatory responses that Elez and Moghaddassi signed "Rules of Behavior" for each Sensitive System to which they were given access. *See* Responses at 18, 19. But DOL obtained the data in the Unemployment Insurance Data and Related Records system on or about March 20, 2025, pursuant to the March 20 EO and gave Elez and Moghaddassi access on March 21, 2025, without first establishing any Rules of Behavior for them to sign. *See* Ex. 7 (DOL Dep.) at 59:9-62:8, 107:3-107:24; Ex. 3 (Defs.' Responses) at 17, 18.

- *Installing unauthorized software systems*. Elez installed two software systems at DOL. DOL does not permit employees to install either without permission. Elez did not have permission, yet there were no consequences. *See* Ex. 7 (DOL Dep.) at 112:21-115:14, 116:23-117:9; Ex. 3 (Defs.' Responses) at 18.

B. Department of Health and Human Services

The story is effectively the same at HHS. Ten DOGE Team members at HHS have been given access to Sensitive Systems. *See* Ex. 3 (Defs. Responses) at 6-16; Ex. 12 (chart prepared by HHS 30(b)(6) witness J. Wendel used as exhibit 8 in deposition) ("Wendel Chart"); Ex. 13 (Rule 30(b)(6) Dep. of HHS) ("HHS (Wendel) Dep.") at 9:19-10:22. Collectively, they have been given access to 19 of these systems. *See* Ex. 12 (Wendel Chart); Ex. 13 (HHS (Wendel) Dep.) at 28:2-29:10; Ex. 14 (list of systems). HHS has not denied any requests from DOGE Team members for access to a Sensitive System and cannot even identify a reason why a request would be denied. *See* Ex. 13 (HHS (Wendel) Dep.) at 36:21-37:6; Ex. 3 (Defs.' Responses) at 6-17. Rather, the Team members simply choose the systems they want to access. *See* Ex. 13 (HHS (Wendel) Dep.) at 38:2-7. HHS has never before provided such broad access to individual employees. *See id.* at 41:25-42:6.

The Sensitive Systems at issue include, for example, the Centers for Medicare & Medicaid Services' HIGLAS (Healthcare Integrated General Ledger Accounting System) and IDR (Integrated Data Repository) systems. *See* Ex. 12 (Wendel Chart) at 1; Ex. 3 (Defs.' Responses) at 7, 8, 9, 12. 15. These contain PII and PHI, such as names, Social Security numbers, dates of birth, financial account information, health insurance claim numbers, medical record numbers, medical notes, physician identification numbers, diagnosis codes, procedure codes, and more. *See* Ex. 12 (Wendel Chart) at 1.

HHS's representative testified that it granted access to HIGLAS, IDR, and the other 17 Sensitive Systems based solely on the DOGE Executive Orders, without distinguishing among their separate directives. *See* Ex. 13 (HHS (Wendel) Dep.) at 29:11-31:3. The representative asserted that the DOGE Team members' access was justified and necessitated by their search for

"waste, fraud, and abuse" pursuant to the Executive Orders. For example, she stated that Luke Farritor needed access to HHS' Consolidated Acquisition System ("HCAS") "because under the executive order HHS was required to look at systems for waste, fraud and abuse." *Id.* at 27:11-14; *see also* 32:16-20; 33:2-5; 42:19-21; 43: 4-9; 44:3-19; 47: 4-22; 48:1-3. This would seem to rule out the January 20 Executive Order as a basis for access because, as noted, it is narrowly focused on technology, not the search for waste, fraud, and abuse on which DOGE Team members have spent their time. But the timing demonstrates that HHS nevertheless either considers the January 20 Executive Order independently sufficient to grant access or had no basis to grant access. That is apparent because four of the DOGE Team members were given access to Sensitive Systems before the second DOGE Executive Order was issued on February 26, 2025. *See* Ex. 3 (Defs.' Responses) at 6, 7, 12, 16. Farritor had access to nine Sensitive Systems before then, including HCAS as of January 29. *See id.* at 7. Providing further confirmation, the January 20 EO is the only one cited by HHS in its interrogatory responses as justifying the DOGE Team members' access to Sensitive Systems. *See id.* at 6-16.

Of a piece with HHS's sole reliance on the January 20 EO to grant access, it does not review systems individually to determine whether to grant access to a DOGE Team member. *See* Ex. 13 (HHS (Wendel) Dep.) at 31:4-13. And like DOL, there is no indication that HHS considers the February 26 EO's distinction between contracts and grants to which it applies and the many to which it does not apply.[5] This Executive Order, which contains the first mention of waste, fraud, and abuse, has not been relevant to the access granted by HHS.

[5] Medicare and Medicaid, for example, are not covered by the February 26 EO's provision regarding waste, fraud, and abuse because they are mandatory spending, not discretionary. *E.g.*, *compare* Congressional Budget Office, *Mandatory Spending in Fiscal Year 2024: An Infographic*, https://www.cbo.gov/publication/61182 (listing Medicare and Medicaid) *with*

Consistent with the unprecedented broad access to Sensitive Systems given to DOGE Team members, HHS (like DOL) has dispensed with training and security briefing requirements. In the ordinary course, HHS employees must have "higher level training" for access to HIGLAS and IDR because the information in them is especially sensitive. *See* Ex. 4 (HHS (Rice) Dep.) at 31:7-32:16; Ex. 13 (HHS (Wendel) Dep.) at 11:13-12:5. That training is documented. *See* Ex. 4 (HHS (Rice) Dep.) at 32:17-33:1. Four DOGE Team members have been given HIGLAS access—Luke Farritor, Edward Coristine, Marko Elez, and Aram Moghaddassi, *see* Ex. 12 (Wendel Chart) at 1—but only Farritor received the HIGLAS security briefing, *compare* Ex. 3 (Defs.' Responses) at 8 (Farritor) to *id.* at 8-12 (Coristine, Elez, and Moghaddassi). Likewise, five DOGE Team members have been given IDR access—Farritor, Coristine, Elez, Moghaddassi, and Zach Terrell, *see* Ex. 12 (Wendel Chart) at 1—but only Farritor received the IDR computer-based training, *compare* Ex. 3 (Defs.' Responses) at 8 (Farritor) to *id.* at 8-12, 14-16 (Coristine, Elez, Moghaddassi, and Terrell).

ARGUMENT

LEGAL STANDARDS

I. Preliminary Injunctions

Plaintiffs seek a preliminary injunction enjoining Defendants from effectuating the DOGE Access Policies. "The purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be held." *Univ. of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981). *See also Dellinger v. Bessent*, No. 25-5028, 2025 WL 559669, at *3 (D.C. Cir. Feb. 15, 2025), citing *Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) ("The

Congressional Budget Office, *Discretionary Spending in Fiscal Year 2024: An Infographic*, https://www.cbo.gov/publication/61184 (excluding them except for administrative costs).

usual role of a preliminary injunction is to preserve the status quo pending the outcome of litigation.") (cleaned up).

When considering a motion for a preliminary injunction, the Court must consider whether the movant has met its burden of demonstrating that: (1) it "is likely to succeed on the merits," (2) it is "likely to suffer irreparable harm in the absence of preliminary relief," (3) "the balance of equities tips in [its] favor," and (4) an injunction serves the public interest. *Winter v. Nat. Res. Def. Council, Inc.,* 555 U.S. 7, 20 (2008). Where the party against whom the injunction is sought is the government, the final two [] factors—balancing the equities and the public interest—merge. *Pursuing Am.'s Greatness v. Fed. Election Comm'n*, 831 F.3d 500, 511 (D.C. Cir. 2016); *D.A.M. v. Barr*, 474 F. Supp. 3d 45, 67 (D.D.C. 2020).

II. The Administrative Procedure Act

The Administrative Procedure Act ("APA") permits plaintiffs to seek judicial review of "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. To be reviewable under the APA, the challenge must be to an "agency action," which "includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551(13). Such an action is "final" if it is "the consummation of the agency's decisionmaking process . . . by which rights or obligations have been determined or from which legal consequences will flow." *Venetian Casino Resort, LLC v. EEOC.*, 530 F.3d 925, 931 (D.C. Cir. 2008) (alterations in original) (quoting *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997)).

As relevant here, the APA provides that a reviewing court shall "hold unlawful and set aside" agency actions found to be "arbitrary, capricious," or "otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). An "agency action is 'not in accordance with law' if it violates some

extant federal statute or regulation." *Ovintiv USA, Inc. v. Haaland*, 665 F. Supp. 3d 59, 72 (D.D.C. 2023) (quoting *E. Band of Cherokee Indians v. Dep't of the Interior*, 534 F. Supp. 3d 86, 97 (D.D.C. 2021)). An agency action is arbitrary and capricious if the agency failed "to examine all relevant factors and record evidence, and to articulate a reasoned explanation for [its] decision." *Am. Wild Horse Pres. Campaign v. Perdue*, 873 F.3d 914, 923 (D.C. Cir. 2017). This requires that the agency "examine the relevant data and articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'" *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.,* 463 U.S. 29, 43 (1983) (quoting *Burlington Truck Lines v. United States*, 371 U.S. 156, 168 (1962)). Agency action fails to satisfy this standard if the agency "failed to consider an important aspect of the problem," *id.*, or if it "offer[s] an explanation for its decision that runs counter to the evidence before the agency," *Am. Wild Horse Pres. Campaign*, 873 F.3d at 923. In short, the APA's arbitrary and capricious standard "requires agencies to engage in 'reasoned decisionmaking'" *Dep't of Homeland Sec. v. Regents of the Univ. of Cal.*, 591 U.S. 1, 16 (2020) (quoting *Michigan v. EPA*, 576 U.S. 743, 750 (2015)).

III. The Privacy Act of 1974

The Privacy Act of 1974 was passed to "provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies" to, among other things, "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose . . . and that adequate safeguards are provided to prevent misuses of such information." Privacy Act of 1974, 88 Stat. 1896 (1974) at §§ 2(b), 2(b)(4). "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies," Congress decided "to regulate the

collection, maintenance, use, and dissemination of information by such agencies." *Id.* at § 2(a)(5).

The Privacy Act prohibits an agency from "disclos[ing] any record which is contained in a system of records . . . to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a(b). The Privacy Act defines "records" as

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

5 U.S.C. § 552a(a)(4). A "system of records," under the statute, "means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* § 552a(a)(5). As relevant here, an exception to section 552a(b)'s broad prohibition on unconsented disclosure is provided where the records are disclosed "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." *Id.* § 552a(b)(1).

ARGUMENT

I. Plaintiffs are Likely to Establish That They Have Standing

Plaintiffs demonstrate that they are likely to establish standing of Plaintiffs. Indeed, while Plaintiffs establish that *five* Plaintiffs have standing, Plaintiffs only need establish that one Plaintiff has standing with respect to each Defendant in order for each claim to proceed. *Vill. Of Arlington Heights v. Metro. Hous. Dev. Corp.,* 429 U.S. 252, 264 & n. 9 (1977); Mem. Op., ECF 78 at 11. Plaintiffs easily meet this standard.

A. Plaintiffs Have Associational Standing to Challenge Unlawful Data Disclosures at DOL and HHS

The Plaintiffs have associational standing to challenge the data disclosures at DOL and HHS. To establish associational standing, a plaintiff must show that "(1) its members would otherwise have standing to sue in their own right; (2) the interests it seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Int'l Dark-Sky Ass'n, Inc. v. FCC*, 106 F.4th 1206, 1217 (D.C. Cir. 2024) (citation omitted). In evaluating Plaintiffs' standing, the Court must "assume [Plaintiffs] will prevail on the merits." *LaRoque v. Holder*, 650 F.3d 777, 785 (D.C. Cir. 2011).

i. Members of Plaintiffs Have Article III Standing

Here, the Plaintiffs have identified individual members who have Article III standing to sue based on the past and ongoing unlawful disclosures of their private and confidential records to DOGE Team members. To establish Article III standing of a member, a Plaintiff "must show that: (1) [the member] has suffered an injury-in-fact that is concrete and particularized and actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Sierra Club v. FERC*, 827 F.3d 59, 65 (D.C. Cir. 2016) (citation omitted). Injury in fact is "[f]irst and foremost' of standing's three elements." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citation omitted). "[A]n injury in fact" is "an invasion of a legally protected interest which is . . . concrete and particularized and . . .actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citations omitted). An "intangible harm," like the harm from disclosure of private information, is concrete

if the plaintiffs "have identified a close historical or common-law analogue for their asserted injury." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021).

Members of the Plaintiffs have already been injured because their members' data has been unlawfully disclosed to DOGE Team members. As this Court has recognized, intra-agency disclosure of private data is concrete for standing purposes because it has a close analogue in the harms suffered in the torts for intrusion upon seclusion and breach of confidence. ECF 78 at 14-17; *see also All. for Retired Ams. v. Bessent*, Civ. A. No. 25-0313, 2025 WL 740401, at *15–17 (D.D.C. Mar. 7, 2025); *Am. Fed'n of Tchrs. v. Bessent*, Civ. A. No. 25-0430, 2025 WL 895326, at *7–13 (D. Md. Mar. 24, 2025); *Am. Fed'n of State, Cnty. and Mun. Emps., AFL-CIO v. Soc. Sec. Admin.*, Civ. A. No. 25-0596, 2025 WL 868953, at *35–43 (D. Md. Mar. 20, 2025). To the extent there is any difference between the private sphere traditionally recognized by these torts and the sphere of seclusion for an individuals' private data, Congress has both created a reasonable expectation of privacy in that data and "elevate[d]" violations of the Privacy Act "to the status of legally cognizable injuries." *TransUnion*, 594 U.S. at 425; *see* Mem. Op., ECF 78, at 16-17; *see also Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (relevant question is whether disclosure implicates "the same *kind* of harm that common law courts recognize").

The record in this case confirms that union members' private information has been and will continue to be disclosed to DOGE Team members. Individual members of the Plaintiff Unions have PII stored at DOL because they are DOL employees, *see* ECF 29-8 at ¶ 4, or because they have applied for unemployment insurance, *see* Ex. 15 (Decl. of M. Evermore) ¶¶ 4-7; Ex. 16 (Decl. of C. Sullivan) ¶ 6; Ex. 17 (Decl. of T. Fry) ¶¶ 4-5; Ex. 18 (Decl. of J. Reese) ¶¶ 4-7; Ex. _ (Decl. of D. Duckett) ¶¶ 5-8. At DOL, DOGE Team members have been granted access to a variety of systems containing employee data, including of the Plaintiffs' members,

see supra at 8, as well as Unemployment Insurance Data and Related Records, which includes social security numbers, addresses, and bank account information, Ex. 3 (Defs.' Responses) at 17-18; Ex. 7(DOL Dep.) at 59:9-60:16. DOGE Team members have access to most of these systems to this day and can access them at any time. *See* Ex. 3 (Defs.' Responses) at 6-15, 17-20.

Plaintiffs' members' PHI and PII is stored at HHS because the members are Medicare recipients, Ex. 20 (Decl. of P. Welsh) ¶¶ 3-4; Ex. 21 (Decl. of D.M. Smith) ¶¶ 7-8; Ex. 22 (Decl. of W. Wetmore) ¶¶ 3-5; Ex. 23 (Decl. of D. Gray) ¶ 4; ECF 29-18 ¶ 3; ECF 29-20 ¶ 4; ECF 29-2 ¶ 4; ECF 29-22 ¶ 4; Ex. 38 (Decl. of L. Nucci) ¶¶ 4-5. As Defendants admit, DOGE Team members have received ongoing access to and in fact accessed systems containing Plaintiffs' members' sensitive information, often without the requisite training and authorization. See Ex. 3 (Defs.' Responses) at 6-15, 17-20; Ex. 12 (Wendel Chart). At HHS, for example, the 19 systems to which DOGE Team members have been granted access include the HIGLAS and IDR—which DOGE Team members have accessed without a demonstrated need and without going through the training required for users of these systems. *See* Ex. Ex. 4 (HHS (Rice) Dep.) at 31:2-33:1, 35:8-36:21; Ex. 13 (HHS (Wendel) Dep.) at 11:13-13:17; Ex. 12 (Wendel Chart); Ex. 3 (Defs.' Responses) at 7-10, 12, 15. These systems hold extremely sensitive information including Social Security numbers, medical diagnosis codes, medical procedure codes, health insurance claim numbers, employee identification numbers, and medical notes—as well as information sufficient to link these records to specific individuals, such as their names, dates of birth, phone numbers, and physical and email addresses. Ex. 12 (Wendel Chart). They contain, in short, a full medical profile of this country's Medicare recipients.

Moreover, the risk of additional future harm is imminent. Plaintiffs' members face both the risk that the current members of the DOGE Team will access additional Sensitive Systems of

record and the risk that DOL and HHS will provide additional DOGE Team members (either direct hires or detailees) access to Plaintiffs' members' data. And these risks are real: the record shows that DOL and HHS will grant DOGE Team members on-demand access to *any* unclassified system of records at the agencies—the DOGE Team member need only ask. *See supra* at 6-12. The agencies do this even at the expense of their normal security protocols. *See supra* at 9, 11-12. When a new or current DOGE Team member decides to access yet another system containing Plaintiffs' members' highly sensitive data, both DOL and HHS have made clear that they will grant the access, no questions asked.

In addition, union members have standing to challenge the Defendant Agencies' Access Policies because Defendant Agencies have caused Plaintiffs' members' injuries and a favorable decision would redress those harms. Causation requires "a fairly traceable connection between . . . the complained-of conduct" and the claimed injury. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998). Redressability requires "a likelihood that the requested relief will redress the alleged injury." *Id.* The D.C. Circuit has recognized that the two "'are closely related' like 'two sides of a…coin.'" *West v. Lynch*, 845 F.3d 1228, 1235 (D.C. Cir. 2017) (alteration in original) (quoting *Dynalantic Corp. v. Dep't of Def.*, 115 F.3d 1012, 1017 (D.C. Cir. 1997)).

Plaintiffs' members easily check these boxes. Here, the challenged conduct—the Defendant Agencies' adoption and implementation of the Access Policies—has caused and continues to cause the unlawful disclosure of members' private and sensitive information. Redressability follows like the other side of that same coin: Plaintiffs seek an injunction prohibiting Defendant Agencies from giving the DOGE Team access to sensitive systems of records. By its very nature, this requested relief would prevent ongoing illegal disclosures to the DOGE Team. *See All. for Retired Ams.*, 2025 WL 740401, at *18.

ii. Protecting Members Private Data is Germane to Plaintiffs' Purpose

The subject matter of this litigation is also germane to the Plaintiffs' purposes—a fact Defendants have thus far not disputed. All Plaintiffs work to protect their members' interests and have specifically advocated to expand and protect access to Medicare, increase worker access to unemployment insurance, and protect member privacy, including in their data. *See generally* Ex. 24 (Decl. of D. McNeil); Ex. 25 (Decl. of K. Coakley Harrison); Ex. 39 (Decl. of E. Medina Neuman); Ex. 26 (Decl. of A. van Schaick); Ex. 40 (Decl. of W. Weiner); ECF 29-15 ¶¶ 4-10. Indeed, each Plaintiff Union has taken actions unrelated to current litigation to protect and advocate for their members' privacy interests, from offering insurance coverage to members for the unlawful disclosure of their data, Ex. 24 (Decl. of D. McNeil) ¶¶ 7-9, 19, to bargaining over workers' rights not to be monitored in the workplace, Ex. 26 (Decl. of A. van Schaick) ¶ 6; Ex. 25 (Decl. of K. Coakley Harrison) ¶¶ 7-9;); Ex. 39 (Decl. of E. Medina Neuman) ¶ 5. And other courts addressing standing in other cases about DOGE's access to data have specifically recognized that protecting members' private data is germane to the purposes of Plaintiffs AFGE, SEIU, and AFT. *See All. for Retired Americans*, 2025 WL 740401, at *13; *Am. Fed'n of Tchrs. v. Bessent*, 2025 WL 895326, at *7.

iii. This Litigation Will Not Require the Active Participation of Union Members

Finally, neither the claims advanced in this litigation nor the relief requested will require the participation of individual union members. Here, Plaintiffs seek only declaratory and injunctive relief. "'[I]ndividual participation' is not normally necessary when an association seeks prospective or injunctive relief for its members." *United Food & Com. Workers Union Loc. 751 v. Brown Grp., Inc.*, 517 U.S. 544, 546 (1996) (quoting *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977)); *see also Warth v. Seldin*, 422 U.S. 490, 515 (1975).

Courts routinely hold that individual member participation is not necessary when only injunctive and declaratory relief is sought in APA cases. *Powder River Basin Res. Council v. U.S. Dept of Interior*, 749 F. Supp. 3d 151, 162 (D.D.C. 2024), *appeal dismissed sub nom. Powder River Basin Res. Council v. United States Dep't of the Interior*, No. 24-5268, 2025 WL 826502 (D.C. Cir. Mar. 13, 2025); *Nat'l Ass'n for Gun Rts., Inc. v. Garland*, 741 F. Supp. 3d 568, 589 (N.D. Tex. 2024); *Sierra Club v. Perry*, 373 F. Supp. 3d 128, 135 (D.D.C. 2019). In the past few weeks, multiple courts haves specifically recognized plaintiffs can seek injunctive relief pursuant to the APA for agency actions that violate the Privacy Act. *See, e.g.*, *All. For Retired Ams.*, 2025 WL 740401, at *15; *New York v. Trump*, No. 25-CV-01144 (JAV), 2025 WL 573771, at *12 (S.D.N.Y. Feb. 21, 2025), *opinion modified on denial of reconsideration*, No. 25-CV-1144 (JAV), 2025 WL 1095147 (S.D.N.Y. Apr. 11, 2025).

The nature of the claims confirms that individual participation is not necessary. Plaintiffs challenge agency-wide policies to give DOGE Team members unfettered, on-demand access to sensitive systems of records without any showing of individualized need. As a result, the relevant questions address whether the policies exist—and discovery has confirmed that they do—and whether they violate the APA, the Privacy Act, and other laws, not whether any particular disclosure occurred or was lawful. Because "[n]either these claims nor the relief sought" involved consideration of "the individual circumstances" of Plaintiffs' members, member participation is not necessary. *Int'l Union, United Auto., Aerospace & Agr. Implement Workers of Am. v. Brock*, 477 U.S. 274, 287 (1986).

II. Plaintiffs are Likely to Succeed on the Merits of Their Claims

A. The DOGE Data Access Policies Violate the APA

1. The DOGE Data Access Policies are Final Agency Action

The "DOGE Data Access Policies" described above, *see supra* at 6-12—systematically granting DOGE Team members access to Sensitive Systems, without individualized confirmation of DOGE Teams' needs and in violation of normal training and documentation requirements for Sensitive System access—amount to a wholesale rewrite of Defendant Agencies' data access policies. They constitute final agency action and are susceptible to the APA's provisions for judicial review.

Final agency actions are those (1) which "mark the consummation of the agency's decisionmaking process," as opposed to decisions of a "merely tentative or interlocutory nature;" and (2) "by which rights or obligations have been determined, or from which legal consequences will flow." *U.S. Army Corps of Eng'rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (citation omitted).

An action need not take the form of a formal written policy to be "final." Mem. Op., ECF 78 at 26; *see also Her Majesty the Queen in Right of Ontario v. EPA*, 912 F.2d 1525, 1531 (D.C. Cir. 1990) (The "absence of a formal statement of the agency's position . . . is not dispositive."). In *Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008), the D.C. Circuit held that the Equal Employment Opportunity Commission's adoption of a policy allowing disclosure of an employer's confidential information without notice to that employer constituted final agency action reviewable under the APA. The D.C. Circuit viewed this as so self-evident that the sum of its discussion of the issue is that the policy "is surely a 'consummation of the agency's decisionmaking process,' and 'one by which . . . rights [and] obligations have been determined.'" *Id*. (quoting *Bennett*, 520 U.S. at 177-78).

As this Court has held, *Venetian Casino* "is on all fours here." ECF 78 at 26. The factual record demonstrates that HHS and DOL have made final determinations that DOGE Teams are

to be given unfettered, on-demand access to Sensitive Systems without regard to existing agency policies. DOL has entirely dispensed with its usual security requirements for DOGE Team members, *see supra* at 6-8, 10-11, and concedes that the normal questions DOL would answer before granting employees access "don't get asked of" DOGE, *see* Ex. 7 (DOL Dep.) at 76:1-20, 89:7-20. The normal training and certification requirements do not apply to DOGE Team members at DOL. *See* Ex. 7 (DOL Dep.) at 109:2-112:4. HHS admits that it does not undertake any "individualized review" of the DOGE Team's access requests, has granted DOGE Teams access that no other HHS employee has ever received, has not denied access to any system, and would not bar DOGE Teams access to any unclassified system. *See* Ex. 13 (HHS (Wendel) Dep.) at 31:4-33:19, 36:21-24, 39:20-40:21, 41:25-42:6.

And both agencies have concluded that DOGE Team Members' unfettered access is required and justified by the January 20 EO, indicating that the DOGE Data Access Policies will continue to be operative for the foreseeable future. *See supra* 6-8, 10-11.

The record shows sweeping, categorical changes in how each Defendant Agency approaches its obligations to safeguard Sensitive Systems with the entrance of DOGE Team members. These policies are not tentative or interlocutory—they are the policies that determine DOGE's access to Agencies' systems. And they determine the obligations of Agency employees vis a vis access to Sensitive Systems, and alter the rights of every individual whose sensitive data is stored by the agencies.

2. The DOGE Data Access Policies are Arbitrary and Capricious

Defendants' DOGE Data Access Policies are arbitrary and capricious. Agency rules "must examine the relevant data and articulate a satisfactory explanation for its action including a rational connection between the facts found and the choice made." *Motor Vehicle Mfrs. Ass'n*

of U.S., 463 U.S. at 43 (internal quotation marks and citation omitted). "Normally, an agency rule would be arbitrary and capricious if the agency . . . entirely failed to consider an important aspect of the problem . . . or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Id.* In considering an agency's action, the reviewing court "may not supply a reasoned basis for the agency's action that the agency itself has not given." *Id.* (internal quotation marks and citation omitted).

a. The Defendant Agencies Have Not Acknowledged or Justified Their Change in Policy

Defendants' DOGE Data Access Policies have handed over sensitive data on millions of Americans to DOGE with no meaningful acknowledgement or justification from the Defendant Agencies. "[A]n '[u]nexplained inconsistency' in agency policy is 'a reason for holding an interpretation to be an arbitrary and capricious change from agency practice.'" *Encino Motorcars, LLC v. Navarro*, 579 U.S. 211, 222 (2016) (second alteration in original). "An agency may not . . . depart from a prior policy *sub silentio* or simply disregard rules that are still on the books," and it must "show that there are good reasons for the new policy." *Fed. Commc'ns Comm'n v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009). While an agency need not "demonstrate . . . that the reasons for the new policy are *better* than the reasons for the old one" or "provide a more detailed justification than what would suffice for a new policy created on a blank slate," it must at least "display awareness that it *is* changing position." *Id.*

The Defendant Agencies refused to acknowledge that they have made any change in their policies concerning Sensitive System access at all, and in doing so have failed to even attempt to present a reasoned basis for the wholesale changes that the record shows they have in fact made. That is sufficient to find the DOGE Data Access Policies to be arbitrary and capricious.

The Agencies' assertions that no change to their access policies has been made are belied by the record. DOL claims that the policy they use for granting access to DOGE Teams is "the same" as that used for DOL employees, but is simply "treat[ed] with more urgency." Ex. 7 (DOL Dep.) at 89:7-90:10. Yet DOL:

- created a bespoke process for DOGE Team members to access Sensitive Systems, giving DOL just "24 hours notice" in which to address confidentiality, conflicts of interest, and privacy concerns before DOGE enters a System, *see id.* 89:7-20;
- concedes that the normal questions DOL would answer before granting employees access to the Unemployment Database "don't get asked of" DOGE Teams, *id.* 76:1-20;
- acknowledges that the normal training and certification requirements have not applied to DOGE Team members at DOL, *id.* 109:2-112:4;
- acknowledges that the process for granting DOGE Teams access to Sensitive System departed from the "normal practice" of seeking system access from an employee's supervisor, and instead went directly through the Chief Information Officer, *see id.* 33:3-34:8.

HHS insists that there are not "different policies" that apply to DOGE Team's system access versus other HHS employees. Ex. 13 (HHS (Wendel) Dep.) at 38:24-39:19. But this denial is belied by HHS's acknowledgements that:

- HHS grants Sensitive System access to DOGE without any "individualized review" of DOGE's access requests, *id.* 31:4-33:19;
- DOGE Team members "should have" received system-specific training before gaining their access (and did not), *see id.* 11:20-14:3;
- DOGE Teams have been granted access that no other HHS employee has ever received; *id.* 41:25-42:6;
- DOGE Teams have not been denied access to any system, *id.* 36:21-24; and
- HHS would not expect to bar DOGE Teams access to any unclassified system. *See id.* 39:20-40:21.

The APA does not allow Defendants to insist that no reviewable policy change has taken place while fundamentally altering the terms on which a new entity is granted unfettered access to Americans' data.

b. The DOGE Data Access Policies Failed to Consider Key Issues

The hastiness with which the DOGE Data Access Policies were adopted also precluded Defendant Agencies from engaging in any careful consideration of potential drawbacks to their approach. In the scramble to share Americans' data with DOGE, Defendants lost sight of all other considerations—the need to protect Americans' privacy, the potential chilling effects of disclosure, financial or bodily harm that could result from disclosures, conflicts of interest, and the reliance interests of the American people. The APA required that they consider these important factors; because they did not, the resulting policies are arbitrary and capricious.

An agency rule is arbitrary and capricious if it "entirely fail[s] to consider an important aspect of the problem" or is "so implausible that it could not be ascribed to a difference in view or the product of agency expertise." *Motor Vehicle Mfrs. Ass'n of U.S.*, 463 U.S. at 43. Here, HHS and DOL failed to consider numerous important factors, including the factors Congress has established to guide agencies' decisionmaking, the reliance interests of those providing private or confidential information to the government, and the potential for significant conflicts of interest.

First, in considering how to shape DOGE Team members' access, Defendants had ample guidance from statutes and their own regulations about the "important aspects of the problem" it should consider. In addition to strictly regulating sensitive data disclosures to "any person," s*ee* 5 U.S.C. § 552a(b), the Privacy Act also places a variety of affirmative requirements on agencies. It requires, for example, that each agency record access regimes establish clear "rules of conduct" for people with systems access and training on the "rules and the requirements of the

Privacy Act." *See* 5 U.S.C. § 552a(e)(9). It also requires agencies to design "safeguards to [e]nsure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." *Id.* § 552a(e)(10). Defendants also have more detailed regulations implementing the Privacy Act's protections and providing additional agency-or system-specific privacy requirements. *See, e.g.*, 29 C.F.R. § 71 (DOL's implementing regulations); 45 C.F.R. § 5b (HHS's implementing regulations); 45 C.F.R. Part 164 (HIPAA Security and Privacy Regulations). Similarly, the Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to provide information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized access [or] use" of information or information systems maintained by the agency. 44 U.S.C. § 3554(a)(1)(A).

This array of laws and regulations governing the disclosure of sensitive information reflects the considerations that Congress has established to guide agencies' policies and decisionmaking with respect to maintenance and disclosure of private information. Taken together, existing laws emphasize that federal information management should be governed by a cautious, thorough, transparent, system-by-system approach, with a primary focus on responsible stewardship of Americans' information.

That approach cannot be reconciled with the rapid, sweeping, unexplained, and unreasoned changes embodied in the DOGE Data Access Policies. As detailed at length above, the Agencies have abandoned the processes and inquiries they normally follow to justify access to their most sensitive systems—the very "safeguards to insure the security and confidentiality of records" that Agencies are supposed to use to avoid "substantial harm, embarrassment,

inconvenience, or unfairness to . . . individual[s] on whom information is maintained." 5 U.S.C. § 552a(e)(10). And the Agencies regularly ignored the rules of conduct and systems access training that would normally be required for employees to understand and acknowledge the responsibilities they are assuming by gaining access to sensitive records. *See id.* § 552a(e)(9).

Second, Defendants also failed to account for the significant reliance interests that attach to persons who submit personally identifying information to the federal government on the understanding that such information shall be confidential and protected from disclosure, as articulated in the numerous declarations submitted in support of this filing. Ex. 18 (Decl. Of J. Reese) ¶ 8 ("I submitted my information with the trust that I can share information with the government and that that information is going to be kept safe. As a result of the disclosures of information from unemployment insurance records that DOL has made to DOGE, I no longer think that's true"); Ex. 19 (Decl. of D. Duckett) ¶ 9 ("I was never enthusiastic about having to submit all of this personally identifiable information but I understood that it was necessary for the state to provide my benefits…."); Ex. 23 (Decl. of D. Gray) ¶ 8 ("I was told [my medical information] was going to be extremely confidential—the only specific, qualified people would have access to it."); Ex. 17 (Decl. of T. Fry) ¶ 8 ("I believed that my personal information would be stored securely and only used for legitimate purposes"). "When an agency changes course, as [Defendants] did here, it must be cognizant that longstanding policies may have engendered serious reliance interests that must be taken into account." *Regents of the Univ. of Cal.*, 591 U.S. at 30 (internal quotation marks and citations omitted).

Finally, Defendants have not meaningfully considered how the DOGE Data Access Policies implicate conflicts of interest. DOL hosts information that is relevant to the outside

businesses of Mr. Musk and a number of DOGE employees.[6] But there is no indication that the DOL has tailored the DOGE Data Access Policy to ensure confidential and competitively-sensitive information is not extracted from agencies for the benefit of DOGE staff's outside interests, or accounted for the various laws protecting sensitive information from competitive disclosure or conflicts of interest. *See, e.g.*, 18 U.S.C. § 208(a) (prohibiting participation by government employees in in matters or proceedings in which they have a financial interest); 18 U.S.C. § 1832 (prohibiting theft of trade secrets).

While the guidelines for onboarding DOGE Team members to DOL and HHS contemplates the Defendant Agencies "ascertain[ing] and mitigat[ing] any conflicts of interest" that might exist with granting DOGE Teams access to Sensitive Systems, neither Defendant actually assessed any conflicts of interest, instead relying on DOGE Team members to make those assessments for themselves. *See* ECF No. 31-1 ¶ 9; Ex. 7 (DOL Dep.) at 97:6-100:5 (at DOL nobody besides DOGE is "evaluating whether they have a conflict of interest" and it is up to "the individual to disclose potential conflicts of interest and raise that to the solicitor's office for review"); Ex. 4 (HHS (Rice) Dep.) 38:19-40:23 (HHS did not assess conflicts of interest with Amy Gleason or Brad Smith, relying on self-reporting); Ex. 30 at 25CV339_HHS00029.

[6] Mr. Musk's companies have been the subject of (or are currently) the subject of enforcement actions at DOL, including at least investigations at SpaceX, Tesla, and the Boring Company. *See* Marisa Taylor, *At SpaceX, worker injuries soar in Elon Musk's rush to Mars*, Reuters (Nov. 10, 2023), https://www.reuters.com/investigates/special-report/spacex-musk-safety/; Brandon Lingle, *Tesla hit with federal fines for worker safety violations at its Gigafactory Texas in Austin*, San Antonio Express-News (Nov. 26, 2024), https://www.expressnews.com/business/article/tesla-texas-gigafactory-osha-fines-worker-safety-19943647.php; OSHA, *Inspection: 1677194.015 - Tbc The Boring Company*, https://www.osha.gov/ords/imis/establishment.inspection_detail?id=1677194.015 (last accessed Feb. 5, 2025).

Defendant Agencies' decision to rush DOGE through their doors, tossing out the normal rulebook for controlling access to sensitive data, was not "the product of reasoned decisionmaking," and cannot be upheld under the APA. *Motor Vehicle Mfrs. Ass'n of U.S.*, 463 U.S. at 52.

c. The Data Access Policies are Contrary to Law Because They Violate the Privacy Act and Agency Regulations

Under the APA, a reviewing court shall "set aside agency action . . . found to be . . . not in accordance with law" or "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C). An "agency action is 'not in accordance with law' if it violates some extant federal statute or regulation." *Ovintiv*, 665 F. Supp. 3d at 72. The DOGE Data Access Policies violate the Privacy Act, as well as HHS and DOL regulations related to the Privacy Act, and should be set aside.[7]

As this Court has noted, "Congress enacted the Privacy Act to 'protect the privacy of individuals identified in information systems maintained by Federal agencies.'" Mem. Op., ECF 78, (quoting *Doe v. Chao*, 540 U.S. 614, 618 (2004) (quoting The Privacy Act of 1974, Pub. L93-579, § 2(a)(5), 88 Stat. 1896 (1974)). As relevant for this case, the Privacy Act regulates the disclosure of records and imposes requirements on agencies to responsibly maintain their recordkeeping systems. With respect to disclosure, the Act provides that outside of certain enumerated exceptions, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to

[7] As this Court recognized in rejecting Defendants' Motion to Dismiss, Plaintiffs' claim for injunctive relief based on Defendants' violations of the Privacy Act is properly brought under the APA, notwithstanding that the Privacy Act contains its own remedial scheme for certain other types of violations. *See* Mem. Op., ECF 78 at 29-32.

a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a(b).

By granting access to their Sensitive Systems to DOGE Team members, Defendants have disclosed records contained in a system of records without the consent of the individuals to whom those records pertain. This access is allowable under the Privacy Act, then, only if it falls within one of the enumerated exceptions. Defendants have previously argued that DOGE's access to sensitive agency records falls within the "Need to Know" exception. *See* Defs. Mot. To Dismiss, ECF No. 49-1 at 28 (citing 5 U.S.C. § 552a(b)(1)). That exception allows for disclosure 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). But Defendants cannot rely on this exception where, as here, DOGE has neither established the "need for the record" nor that they should be treated as "employees of the agency which maintains the record."

i. Disclosures to DOGE Teams Should Be Considered Disclosures to Outside the Agencies

DOGE affiliates—even those who have been papered as employees of Agency Defendants—continue to answer to DOGE while performing work at Defendant agencies. They are, for the purposes of the Privacy Act analysis, functionally employees of DOGE, however each individual's employment might be papered. Agency Defendants' disclosure of Privacy Act information to DOGE affiliates therefore constitutes disclosure "to another agency" under 5 U.S.C. § 552a(b)—it is a release of protected information outside the agency.

Defendants have attempted to cure the Privacy Act problems caused by unlawful details from DOGE by documenting alternate employment relationships between their affiliates and Defendant agencies. *See* Ex. 2 (DOGE Dep.) at 77:12-19 (USDS traditionally detailed employees to agencies, but "upon the Court's order, changed their practices"). But these

formalistic arrangements cannot change the reality that DOGE affiliates report, first and foremost, to DOGE, and should therefore be treated as DOGE employees. Most of the individuals at issue in this case may not be paid by DOGE—though some are not paid at all, *see, e.g.*, Ex. 32 (Edward Cortistine working under gratuitous services agreement), Ex. 33 (same as to Kyle Schutt), but, in situations where employees have simultaneous employment relationships with multiple government component, they are not, as a "practical matter," *Jud. Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 132 (D.C. Cir. 2005), automatically employees of the agency paying their salary. Although the D.C. Circuit has not articulated a clear test for identifying a true employer in such circumstances, it has adopted a functional approach that "requires an evaluation of all the circumstances." *Id.* at 131 (quoting *Spirides v. Reinhardt*, 613 F.2d 825, 831 (D.C. Cir. 1979)); Mem. Op., ECF 78 at 35. Those considerations can include the matters on which an employee worked, who supervised them, and where the employees physically performed their work. *Jud. Watch*, 412 F.3d at 131-32. These factors, as well as a holistic consideration of the circumstances of DOGE affiliates' work, leave little doubt that they are functionally employees of DOGE, not of their host Defendant agencies.

First, DOGE is choosing to place DOGE affiliates in host agencies; host agencies are not hiring them *sua sponte* and then assigning them to DOGE teams. The January 20 EO explicitly calls for DOGE to direct the placement of its affiliates at agencies, requiring, for example that agency heads "select the DOGE Team members *in consultation with the USDS Administrator*." Ex. 1 (January 20 EO) at § 3(c) (emphasis added). The evidence here shows that DOGE is in fact directing the placement and assignment of DOGE Team members at the agencies. For example, Brad Smith, in his capacity as the lead DOGE official at HHS, "recommended" that HHS bring on certain DOGE affiliates, including Brad Smith himself. *See, e.g.*, Ex. 4 (HHS (Rice) Dep.) at

20:11-16, 40:24-41:21. *See also* Declaration of Thomas H. Krause, Jr., *New York v. Dep't of Treasury*, No. 1:25-cv-01144-JAV, ECF No. 33, ¶ 3 (S.D.N.Y. Feb., 11 2025) ("USDS/DOGE recommended to [DOGE operative already at Treasury] and to incoming Treasury leadership, that [a specific individual] be selected as the Treasury DOGE Team's technical team member," after which Treasury hired that individual).

And the form of those arrangements is unusual: it is possibly unprecedented for the Department of Labor to have employees or detailees with employment arrangements at multiple other federal components, *see* Ex. 7 (DOL Dep.) at 37:4-37:10, *see also* Ex. 2 (DOGE Dep.) at 93:4-16 (at least one DOGE Team member has simultaneous employment relationships at eight agencies).

Second, DOGE affiliates are only present at their respective host agencies to perform DOGE work. *See, e.g.*, Ex. 4 (HHS (Rice) Dep.) at 21:2-8 (DOL brought on board DOGE Team members "to make sure that we met the goals and requirements of the executive order, so we were kind of building our scope and – and team to get the accomplishments that we wanted to meet the requirements of the EO"). As the Court noted, the January 20 EO directs the DOGE Teams at the agencies to work on "core USDS initiatives for USDS purposes." ECF 78 at 35. This is borne out by the actual work DOGE affiliates are performing; there is no difference in Brad Smith's functional responsibilities as a detailee to or employee of HHS and his duties regarding HHS when he was employed only at DOGE. *Id*. at 43:14-24. DOGE also understand those responsibilities to constitute DOGE work. Ex. 2 (DOGE Dep.) at 35:4-7 (DOGE team work "is part of the, like, umbrella of the DOGE mission, right, and the President's DOGE agenda"). That work includes "efforts to cross-reference information across databases from multiple agencies" as part of " a mission and purpose that DOGE teams are generally working

on." *Id.* at 116:4-21. This Court has already recognized that "USDS employees' jobs at the agency defendants entail carrying out the DOGE agenda at those agencies," ECF No. 71, 12; this necessarily muddies the water of reporting relationships.

Third, DOGE affiliates are functionally supervised by DOGE. Interagency agreements make clear that, in some instances, DOGE affiliates expressly and formally report to the Acting Administrator of DOGE even while performing work focused on the Defendant agency which nominally employs them. The agreement between DOGE and HHS on Terms and Conditions for Reimbursable Work and Non-Reimbursable Work, for instance, provides that "USDS employees will . . . report to and be supervised by their USDS supervisor when at USDS facilities and on USDS systems, *even when performing work with the scope of the Agreement*. Ex. 30 (CMS Employment Agreement); Ex. 31 (HHS Employment Agreement) (emphasis added). At a minimum, these agreements govern the work of Amy Gleason and Brad Smith at HHS.[8]

And these clauses may not reflect every situation in which the employees they cover report to DOGE even when conducting agency work; the agreements are silent on employees' reporting obligations when they use DOGE equipment at an agency facility or vice-versa—circumstances which do arise. *See, e.g.*, Ex. 2 (DOGE Dep.) at 99:16-24 (DOGE personnel have used agency systems outside agency facilities), 117:1-118:11 (DOGE personnel have used agency systems at DOGE facilities)

That the DOGE Affiliates are functionally supervised by DOGE is also clear from the Executive Orders themselves. As the Court noted, the January 20 EO tasks DOGE Teams "with 'implementing the President's DOGE Agenda'—in other words, with executing the agenda laid

[8] Defs'. Responses at 6, 17 (Amy Gleason and Brad Smith are both employed at both HHS and detailed to DOGE).

out in the DOGE E.O. and other relevant Executive Orders—as interpreted by the USDS Administrator." ECF 78 at 35, citing the January 20 EO §§ 3(c), 4. The January 20 EO further requires DOGE affiliates to "coordinate their work with" DOGE, but requires only that those teams "advise" the heads of their respective host agencies. To "coordinate" their work with DOGE means that DOGE Teams must "bring into a common action, movement, or condition" or "harmonize" their work with DOGE. "Coordinate," *Merriam-Webster Online*, https://www.merriam-webster.com/dictionary/coordinate. It would be impossible for each agency DOGE Team across the government to make DOGE's work and expectations conform to the work of the individual agency DOGE Teams; coordination therefore can only mean that DOGE Teams are required to work in a way that "harmonizes" with the instructions and expectations of DOGE. That coordination is not merely speculative, it is ongoing: "DOGE . . . certainly coordinates with most, if not all, the DOGE agency teams." Ex. 2 (DOGE Dep.) at 124:19-21.

In contrast, agency DOGE Teams are required only to "advise" host agency heads, a function that requires neither supervision from the agency head nor any form of coordination. And there is little question that the Executive Order is the lone source of guardrails or guidance for DOGE affiliates' work. *See* Ex. 7 (DOL Dep.) at 40:24-41:4 (describing DOGE executive orders as "an instruction or a guide for Department of Labor employees to – to – work with [DOGE] staff. There's no other policies in place"). Even in DOGE's characterization, DOGE affiliates at least sometimes operate as DOGE employees when they are working at agencies—including when advising agency heads. "[A]s an employee of USDS [a DOGE affiliate] can give consultation and advice on how HHS DOGE team could implement . . . the DOGE agenda." Ex. 2 (DOGE Dep.) at 80:5-80:9. When giving such advice to HHS, a DOGE affiliate "reports up to

the [USDS] supervisory chain of command," *id.* 81:9-11, but when "doing work at HHS he is reporting up to HHS agency leadership." *Id.* 81:12-13. This balance of control of DOGE Teams' work weighs heavily in favor of a conclusion that DOGE is their actual employer.

Taken together, it is apparent that DOGE employees, whether detailed to Defendant agencies from DOGE (or elsewhere) or "hired" as SGEs or "experts," are not typical agency employees or detailees. They take direction from a government component besides the agency where they work, operate pursuant to an Executive Order which makes them beholden to that same government component, and use technology equipment from outside their host agencies. This court should resist a formulaic approach requiring it to ignore these considerations to instead identify them as employees of their host agencies solely on the basis of who pays them. Such a result would hypothetically allow an administration to subvert the entire Privacy Act through one well-placed employee at each government component, assigned to report to a single office.

ii. DOGE Does Not Have a Need to Access Agency Systems

In order to establish that their grants of access fall within the "Need to Know" exception, DOL and HHS must show that "the official examined the record in connection with the performance of duties assigned to him and [that] he had to do so in order to perform those duties properly." *Bigelow v. Dep't of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000). As detailed at length, above, the Defendant Agencies did not even attempt to do this before granting access. DOL admitted that the "questions that don't get asked of DOGE" before permitting DOGE to access some highly-sensitive data include "why[] the access is needed" and "what [] the access will be used for." *See* Ex. 7 (DOL Dep.) at 76:1-20. HHS admitted that it does not conduct any "individualized review" to confirm that DOGE has a need to access the Sensitive Systems it has

requested access to. *See* Ex. 13 (HHS (Wendel) Dep.) at 29:11-31:18. DOL and HHS necessarily fail to establish the "Need to Know" exception for this reason alone.

Instead of a particularized analysis, the Defendant Agencies simply treated the January 20 EO as self-executing directives, instantly and comprehensively revealing sensitive data to DOGE. *See, e.g.*, Ex. 7 (DOL Dep.) at 72:1-19 (it is "apparent" that DOGE's access to unemployment data . . . falls within th[e] roles and responsibilities as outlined in the executive orders."); Ex. 13 (HHS (Wendel) Dep.) at 33:2-19 (HHS made an "inference" that DOGE was requesting access to sensitive systems to "look[] for waste, fraud, or abuse" because the official had "read the executive order, so [she] knew that's what they were doing.").

But the EOs do not—and cannot—by themselves establish DOGE Team members' "need" to access dozens of sensitive systems. As an initial matter, at least one circuit has rejected the argument that an executive order, without more, can automatically justify disclosing information protected by the Privacy Act. *See Parks v. U.S. Internal Revenue Serv.*, 618 F.2d 677, 681 (10th Cir. 1980). In this case, the executive orders cited also cannot justify a blanket need to access dozens of Sensitive Systems because this broad access runs directly counter to the purpose of the Privacy Act.

The Privacy Act was "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies," S. Rep. No. 1183, 93d Cong., 2d Sess. (1974), and was motivated by a concern that "every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution." Danielle Keats Citron, A More Perfect Privacy, 104 B.U. L. Rev. 1073, 1078 (2024) (first

quoting 120 Cong. Rec. 36,917 (1974) (statement of Sen. Goldwater) and then quoting 120 Cong. Rec. 36,917 (statement of Sen. Percy)).

The agencies' broad grants of access do just that. Allowing DOGE Team members to access any unclassified system—or all systems—at will, based exclusively on the EOs would "allow the exception to swallow the rule," *Dick v. Holder*, 67 F. Supp. 3d 167, 178 (D.D.C. 2014), and would gut the very protections the Privacy Act is designed to provide. Indeed, there do not appear to be any cases endorsing a "need" to access the sensitive records of millions of Americans. The only courts to address this issue in the context of granting agency-wide records access to DOGE have agreed that the "Need to Know" exception does not apply. *Am. Fed'n of Tchrs.*, 2025 WL 895326 at 24 (D. Md. Mar. 24, 2025); *AFL-CIO*, 2025 WL 868953 at 64 (D. Md. Mar. 20, 2025). "In short, the order[s], which [were] at odds with the stated legislative purpose of the Privacy Act, do[] not license the defendants to violate the Privacy Act." *Parks*, 618 F.2d at 681.

Even if this court were to accept that the executive orders could justify agency-wide system access, the EOs do not, by their own terms, provide the justification on which the agencies now rely. The Agencies now justify the need for widespread DOGE Team system access by repeating the mantra of "waste, fraud and abuse," *see, e.g.*, Ex. 13 (HHS (Wendel) Dep.) at 27:11-14; Ex. 7 (DOL Dep.) at 22:17-23:2. But the January 20 EO establishing DOGE says nothing about waste, fraud, or abuse at all. Instead, it tasked the USDS Administrator with "improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." Ex. 1 (Jan. 20 EO).[9]

[9] It also tasked DOGE Teams with helping "implement[] the President's DOGE Agenda," an undefined term that is not obviously susceptible to understanding any given employee's responsibilities. *Id.* § 3(c)

The February 26 EO at least used the magic words. But this EO applies only "discretionary spending through Federal contracts, grants, loans and related instruments, but *excludes direct assistance to individuals*." *Id.* § 2(d) (emphasis added). By its plain terms, the February 26 EO cannot justify DOGE access to "[u]nemployment claims from states' unemployment insurance agencies," Ex. 7 (DOL Dep). at 59:22-24, or "child support payments," Ex. 13 (HHS (Wendel) Dep.) at 42:17-44:19, or the "basic accounting system" for Medicare and Medicaid payments, Ex. 4 (HHS (Rice) Dep.) 31:2-9. Even if it could, by February 26, 2025, the Agencies had given the DOGE Teams access to numerous Sensitive Systems. *See, e.g.* Ex. 3 (Defs.' Responses) at 6-7 (Luke Farritor had access to sensitive systems as early as January 22, 2025).

The March 20 EO is also insufficient. It orders Agency Heads to grant certain employees "full and prompt access to all unclassified agency records . . . for purposes of pursuing Administration priorities related to . . . waste, fraud, and abuse." Ex. 6 (March 20 EO) at § 3(a). It does not identify what those priorities are, how they are to be undertaken, which records are to be evaluated, or what job functions the people seeking access would be filling, aside from "designees."

In a similar case this week related to DOGE's access to Sensitive Systems at the Social Security Administration, the court found in granting a preliminary injunction that the agency's explanations of employees' need to know (which were more substantial than anything Defendants have offered in this case) had failed to demonstrate "that the DOGE Team members required unlimited access to PII to perform their work." Mem. Op. on Pltfs' Mot. for a Preliminary Injunction, *Am. Fed'n of State, Cnty. and Municipal Emps. v. Social Sec. Admin.*, ELH-25-0596, ECF No. 146 at 126 (D. Md. Apr. 17, 2025). The court noted that seeking

"unprecedented, unfettered access to virtually SSA's entire data systems" could not be justified without "explanation as to why or how the particular records correlated to the performance of job duties," including the detection of fraud, waste, and abuse. See id. at 120-21.

iii. The DOGE Data Access Policies Also Violate Agency Regulations

In addition to violating the Privacy Act, the HHS and DOL DOGE Data Access Policies also violate each agency's own regulations. Specifically, each agency has promulgated, through notice and comment rulemaking, regulations that prohibit disclosure of their records except as permitted by the Privacy Act. DOL, for example, established confidentiality requirements for various sets of sensitive data. *See, e.g.* 20 C.F.R. § 10.10 (FECA) ("All records relating to claims for benefits, including copies of such records maintained by an employer, are considered confidential and may not be released, inspected, copied or otherwise disclosed except as provided in the Freedom of Information Act and the Privacy Act of 1974 or under the routine uses provided by DOL/GOVT-1 if such release is consistent with the purpose for which the record was created."). Similarly, HHS has established regulations likewise protecting records from unauthorized disclosure and implementing the requirements of the Privacy Act. *See* 45 C.F.R. § 5b.9(a). Because Defendants violate the Privacy Act, they also violate these regulations.

III. Plaintiffs Face Irreparable Injury from the Continued Effect of the DOGE Access Policies

For many of the same reasons that Plaintiffs have established standing, *supra* at 15-21, they have also demonstrated that the sharing of information by DOL and HHS with DOGE will cause irreparable harm. "An irreparable harm is an imminent injury that is both great and certain to occur, and for which legal remedies are inadequate." *Beattie v. Barnhart*, 663 F. Supp. 2d 5, 9 (D.D.C. 2009).

DOGE's ongoing unauthorized access to sensitive employment, health, and financial data will cause irreparable harm. *See Hum. Touch DC, Inc. v. Merriweather*, No. 15-CV-00741 (APM), 2015 WL 12564166 (D.D.C. May 26, 2015) (finding irreparable harm and granting injunction where former employee accessed and forwarded emails with confidential patient information without authorization); *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000) ("The harm at issue here—disclosure of confidential information—is the quintessential type of irreparable harm that cannot be compensated or undone by money damages." (citing *Hawai'i Psychiatric Soc'y v. Ariyoshi*, 481 F. Supp. 1028, 1052 (D. Haw. 1979))); *see also Plante v. Gonzalez*, 575 F.2d 1119, 1135 (5th Cir. 1978) ("When a legitimate expectation of privacy exists, violation of privacy is harmful without any concrete consequential damages"; *see also Nat'l Sec. News Serv. v. Dep't of the Navy*, 584 F. Supp. 2d 94, 96 (D.D.C. 2008) (in FOIA context, "[r]ecords . . . indicating that individuals sought medical treatment at a hospital are particularly sensitive").

As described above, the data systems housed at DOL and HHS, including the very data systems that Defendants admit DOGE Teams are accessing, include extremely sensitive information about Plaintiffs' members, including their Social Security numbers, their employment histories, and a breakdown of their wage for the past eight weeks. *See* Ex. 15 (Decl. of M. Evermore); Ex. 18 (Decl. of J. Reese) ¶¶ 5-6. For the hundreds of thousands of members of Plaintiffs enrolled in Medicare, that information includes intimate medical details, including their diagnoses, medical procedures they have undergone, and medical notes. *See* Ex. 12 (Wendel Chart). Disclosure of this information to DOGE is an actual harm to Plaintiffs' members, who did not consent to DOGE accessing their sensitive information and who face injury in the form of a privacy violation every day because unauthorized individuals access their private data.

Members placed their trust in the government to protect their data and unsurprisingly are angry that the Agencies have violated that trust. Ex. 18 (Decl. of J. Reese) ¶ 8; Ex. 19 (Decl. of D. Duckett); *see also* Ex. 16 (Decl. of C. Sullivan) ¶ 8; Ex. 21 (Decl. of D.M. Smith) ¶ 11; Ex. 23 (Decl. of D. Gray) ¶¶ 7, 9; Ex. 17 (Decl. of T. Fry) ¶¶ 9, 11; ECF 29-18 ¶ 6; ECF 29-22 ¶ 7; ECF 29-21 ¶ 7. They are also reasonably worried that their information will be leaked or otherwise misused due to the haphazard and slapdash nature of the Agencies' decisions to hand over their data to untrained members of the DOGE Team. Ex. 18 (Decl. of J. Reese) ¶ 9; Ex. 19 (Decl. of D. Duckett); Ex. 16 (Decl. of C. Sullivan) ¶ 8; Ex. 21 (Decl. of D.M. Smith) ¶ 12; Ex. 24 (Decl. of D. McNeil) ¶¶ 16-18; Ex. 23 (Decl. of D. Gray) ¶¶ 8-9; Ex. 17 (Decl. of T. Fry) ¶¶ 9-11; Ex. 20 (Decl. of P. Welsh) ¶ 6; ECF 29-20

Plaintiffs also have no reason to believe that the pace and scope of DOGE Data Access is slowing down. Since this case was first filed, President Trump has issued a slew of additional executive orders tasking DOGE with additional responsibilities at federal agencies, including:

- Consulting with each Agency Head to "develop a data-driven plan . . . to ensure new career appointment hires are in highest need areas," and identifying career official vacancies "that the DOGE Team Lead assesses should not be filled;" Ex. 34 (Exec. Order No. 14,210 § 3(b), 90 Fed. Reg. 9,669 (Feb. 11, 2025));

- "[I]dentify[ing] all . . . sources of Federal funding for illegal aliens" and "recommend[ing] . . . agency actions to align Federal spending with" the President's immigration policies, Ex. 35 (Exec. Order No. 14,218 § 2(b), 90 Fed. Reg. 10,581 (Feb. 19, 2025));

- Consulting with "agency heads . . . on potential new regulations," Ex. 36 (Exec. Order No. 14,219 § 4, 90 Fed. Reg. 10,583 (Feb. 19, 2025));

- Consulting with "[e]ach Agency Head" to "conduct a comprehensive review of each agency's contracting policies, procedures, and personnel," after each federal agency has "buil[t] a centralized technological system . . . to seamlessly record every payment issued by the agency pursuant to each of the agency's covered contracts and grants." Ex. 5 (Feb. 26 EO);

- Obtaining "full and prompt access to all unclassified agency records, data, software systems, and information technology systems . . . for the purpose of pursuing Administration priorities related to the identification and elimination of waste, fraud, and abuse" including undertaking "both the intra- and inter-agency sharing and consolidation of unclassified agency records," and "receiv[ing] . . . unfettered access to all unemployment data and related payment records, including all such data and records currently available to the Department of Labor's Office of Inspector General," Ex. 6 (March 20 EO); and

- "[C]oordinat[ing]" with the Department of Homeland Security to "review each State's publicly available voter registration list . . . alongside Federal immigration databases and State records," Ex. 37 (Exec. Order No. 14,248 § 2(b)(iii), 90 Fed. Reg. 14,005 (Mar. 25, 2025)).

The record in this case shows that the Defendant Agencies treat executive orders as effectively self-executing when it comes to granting DOGE access to Sensitive Systems, and each additional executive order granting DOGE new authorities creates new plausible claims to sensitive data housed at federal agencies.

III. Balance of the Equities

"It is well established that the Government cannot suffer harm from an injunction that merely ends an unlawful practice." *C.G.B. v. Wolf*, 464 F. Supp. 3d 174, 218 (D.D.C. 2020) (internal quotation marks and citations omitted). Likewise, "[t]here is generally no public interest in the perpetuation of unlawful agency action." *Open Cmtys. All. v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017) (citing *League of Women Voters of United States v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016)). "To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws—such as the APA, as well as regulations . . .—that govern their existence and operations." *Id.* (internal quotation marks and citations omitted). Thus, for the same reasons that Plaintiffs are likely to succeed on the merits, equity requires relief.

But even if this Court were to balance Defendants' interests as if it were a private party, the balance of equities and public interest would still overwhelmingly favor Plaintiffs. Neither

Defendants, nor any non-defendant component of the Government, have any lawful or legitimate need to commandeer the Agency Defendants' information systems or the data within them in this abrupt, unlawful, unreasoned, and chaotic manner.

CONCLUSION

For the reasons set forth above, Plaintiffs respectfully submit that the Court should enter a preliminary injunction bringing to a halt the unlawful access that DOL and HHS have given DOGE Teams to their Sensitive Systems, as set forth in the accompanying proposed order.

Dated: April 18, 2025

Respectfully submitted,

/s/ *Zoila E. Hinson*

Mark B. Samburg (D.C. Bar No. 1018533)
Aman T. George (D.C. Bar No. 1028446)
Rachel F. Homer (D.C. Bar No. 1045077)
Robin F. Thurston (D.C. Bar No. 462679)
Somil B. Trivedi (D.C. Bar No. 1617967)
Skye L. Perryman (D.C. Bar No. 984573)
DEMOCRACY FORWARD FOUNDATION
P.O. Box 34553
Washington, D.C. 20043
Telephone: (202) 448-9090
Fax: (202) 796-4426
msamburg@democracyforward.org
ageorge@democracyforward.org
rhomer@democracyforward.org
rthurston@democracyforward.org
strivedi@democracyforward.org
sperryman@democracyforward.org

Glenn Schlactus (D.C. Bar No. 475950)
Zoila E. Hinson (D.C. Bar No. 1766625)**
Alexa Milton (D.C. Bar No. 155380)**
RELMAN COLFAX PLLC
1225 19th St. NW, Suite 600
Washington, DC 20036

Telephone: (202) 728-1888
gschlactus@relmanlaw.com
zhinson@relmanlaw.com
amilton@relmanlaw.com
Counsel for Plaintiffs

Teague P. Paterson (D.C. Bar No. 144528)
Matthew S. Blumin (D.C. Bar No. 1007008)
AMERICAN FEDERATION OF STATE, COUNTY, AND MUNICIPAL EMPLOYEES, AFL-CIO
1625 L Street N.W.
Washington, DC 20036
Telephone: (202) 775-5900
Facsimile: (202) 452-0556
tpaterson@afscme.org
mblumin@afscme.org
Counsel for American Federation of State, County, and Municipal Employees, AFL-CIO (AFSCME)

Rushab B. Sanghvi (D.C. Bar No. 1012814)
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO
80 F Street N.W.
Washington, DC 20001
Telephone: (202) 639-6426
Facsimile: (202) 329-2928
SanghR@afge.org
Counsel for Plaintiff American Federation of Government Employees, AFL-CIO (AFGE)

Steven K. Ury* (D.C. Bar 1643947)
SERVICE EMPLOYEES INTERNATIONAL UNION
1800 Massachusetts Avenue, NW,
Legal Department, 6th Floor,
Washington, DC 20036
Telephone: (202) 730-7428
steven.ury@seiu.org
Counsel for Plaintiff Service Employees International Union

Matthew Holder**
COMMUNICATION WORKERS OF AMERICA, AFL-CIO
501 Third Street N.W.
Washington, D.C. 20001
Telephone: (202) 215-6788
mholder@cwa-union.org

* Admission pending
** Admitted *pro hac vice*