

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AFL-CIO, *et al.*,

Plaintiffs,

v.

Case No. 1:25-cv-00339

DEPARTMENT OF LABOR, *et al.*,

Defendants.

**MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR A
TEMPORARY RESTRAINING ORDER**

INTRODUCTION

American workers are the backbone of the United States and our economy. Blue collar, white collar, service, tech, manufacturing, education, and in so many other sectors, America's workers have built this nation and make it stronger every day. The US Department of Labor is responsible for the administration of federal laws and protections that keep our nation's workforce strong and growing --- from wage and hour standards, to health, safety, and occupational protections, to unemployment benefits and reemployment services, to maintaining data regarding our nation's economy and the workers who are the backbone of it.

As this motion is being filed, the U.S. DOGE Service—led by Elon Musk, an unappointed, unelected, and temporarily serving official—is threatening to run roughshod over core data at the Department of Labor—data that contains sensitive personal information regarding America's

workers, data regarding our labor statistics, and even health information. As documented in an attached Declaration, in anticipation of DOGE’s arrival, Department of Labor employees have been told to unquestionably give DOGE operatives access to any system or information they request, or else face termination. These systems contain the most private, sensitive employee and medical information on virtually every worker in America—information that this administration, including DOGE, is required by law to protect. They also contain information that comprise our labor force data, the US Bureau of Labor Statistics, that is a backbone data source of the US economy.

DOGE has already endangered the security of vital government systems and violated the privacy and trust of millions of Americans, all in the course of “assuming command” over federal agencies. DOGE operatives have zeroed in on and sought unprecedented access to sensitive information systems at the Department of Treasury, U.S. Agency for International Development, National Oceanic and Atmospheric Administration, the Department of Education, the Office of Personnel Management, and others. The systems and records to which DOGE has sought access are highly sensitive. Indeed, the OPM systems to which DOGE has gained access contain personal information for all federal employees—including some from all three branches—that is so sensitive that a foreign adversary illegally hacked that data system in 2015. This despite President Trump instructing DOGE to adhere to “rigorous data protection standards.” *See* Exec. Order No. 14158, “Establishing and Implementing the President’s ‘Department of Government Efficiency’” (Jan. 20, 2025), § 4(b) (the “E.O.”).

The threats to the Department of Labor that give rise to this action and application for emergency relief represent yet another iteration of what is fast becoming a pattern for DOGE: exceeding its narrow mission and exercising authority it does not (and cannot) possess by exerting

control over agencies through personal attacks and threats of unlawful reprisals, and harming people and the stability of our nation in the process. DOGE's conduct throughout this pattern has been replete with violations of law, and this Court should not permit DOGE to repeat it at the Department of Labor.

LEGAL BACKGROUND

Myriad laws and protections have been violated and implicated by the Defendants' actions here.

I. The Privacy Act of 1974

The Privacy Act of 1974 was passed during the Watergate era 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 § 2(b), 2(b)(4), 88 Stat. 1896 (1974), *codified as amended at* 5 U.S.C. § 552a. “[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.* § 2(a)(5), 88 Stat. 1896, 1896.

To that end, the Privacy Act regulates “records,” defined 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).

Individuals under the Privacy Act are any “citizen of the United States or [] alien lawfully admitted for permanent residence.” *Id.* at § 552a(a)(2).

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, “[n]o 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 a written request by, or with the prior written consent of, the individual to whom the record pertains.” 5 U.S.C. § 552a(b).¹

II. The Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2014 (“FISMA”), 44 U.S.C. §§ 3551-58, 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).

To that end, agencies are responsible for complying with FISMA’s requirements and “related policies, procedures, standards, and guidelines” such as “information security standards promulgated under” 40 U.S.C. § 11331 and “policies and procedures issued by the Director” of the Office of Information and Regulatory Affairs. 44 U.S.C. § 3554(a)(1)(B)(i), (iii).

“[S]enior agency officials” are required to “provide information security for the information and information systems that support the operations and assets under their control,” including understanding the risks of “unauthorized access, use, disclosure, disruption,

¹ This provision contains a number of exceptions, listed at 5 U.S.C. § 552a(b)(1)-(13), none of which Plaintiffs have reason to believe are relevant to the facts of this case.

modification, or destruction” of sensitive agency records, and implementing policies designed to reduce those risks. *See* 44 U.S.C. § 3554(a)(2).

III. The Administrative Procedure Act

The Administrative Procedure Act (“APA”) protects the American public from arbitrary, capricious, and unlawful executive branch action. It allows individuals “suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action” to seek judicial review of the action. 5 U.S.C. § 702. Under the APA, a reviewing court may “compel agency action unlawfully withheld or unreasonably delayed,” *id.* § 706(1), and “hold unlawful and set aside agency action, findings, and conclusions” that are “arbitrary, capricious an abuse of discretion, or otherwise not in accordance with law,” *id.* § 706(2)(A).

FACTUAL BACKGROUND

Many sensitive data sources and processes are housed within the Department of Labor, including some classified information.

IV. Sensitive and Valuable Systems Within the Department of Labor.

The Department lists over 50 different systems containing personally identifiable information across its functions.² Unlawful changes to these systems’ (and others’) access or control could have substantial negative effects, for individual privacy as well as for agency effectiveness. Some examples follow.

A. FECA

² *Privacy Impact Assessments*, U.S. Dep’t of Labor, Office of the Assistance Secretary for Administration and Management, <https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy> (last accessed Feb. 5, 2025) (collecting Privacy Impact Assessments for over 50 systems across various Department functions).

Among DOL's functions, it administers workers compensation programs, including all federal employees' compensation claims through the Federal Employees' Compensation Act ("FECA") Claims Administration. This administration adjudicates new claims for benefits and manages ongoing cases; pays medical expenses and compensation benefits to injured workers and survivors; and helps injured employees return to work when they are medically able to do so.

Because DOL administers all workers' compensation claims for federal employees it is responsible for all of these records.³ FECA records include highly sensitive personal information, including the following information:

Reports of injury by the employee and/or employing agency; claim forms filed by or on behalf of injured Federal employees or their survivors seeking benefits under FECA; forms authorizing medical care and treatment; other medical records and reports; bills and other payment records; compensation payment records; formal orders for or against the payment of benefits; transcripts of hearings conducted; and any other medical, employment, or personal information submitted or gathered in connection with the claim. The system may also contain information relating to dates of birth, marriage, divorce, and death; notes of telephone conversations conducted in connection with the claim; information relating to vocational and/or medical rehabilitation plans and progress reports; records relating to court proceedings, insurance, banking and employment; articles from newspapers and other publications; information relating to other benefits (financial and otherwise) the claimant may be entitled to; and information received from various investigative agencies concerning possible violations of Federal civil or criminal law. The system may also contain information relating to certain claims under the War Hazards Compensation Act (WHCA).

The system may also contain consumer credit reports on individuals indebted to the United States, information relating to the debtor's assets, liabilities, income and expenses, personal financial statements, correspondence to and from the debtor, information relating to the location of the debtor, and other records and reports relating to the implementation of the Federal Claims Collection Act (as amended), including investigative reports or administrative review matters.

³ 20 C.F.R. 10.10; *see also* DOL/GOVT-1, available at <https://www.govinfo.gov/content/pkg/PAI-2023-DOL/xml/PAI-2023-DOL.xml#govt1> (last accessed Feb. 5, 2025).

Individual records listed here are included in a claim file only insofar as they may be pertinent or applicable to the employee or beneficiary.⁴

Given the sensitive nature of these records, regulations require they be treated “considered confidential and may not be released, inspected, copied or otherwise disclosed” except under certain proscribed circumstances, and only if such release is consistent with the purpose for which the record was created.⁵

In FY 2024, over 86,000 new FECA cases were created, implicating the privacy interests of tens of thousands of federal employees.⁶

B. The Wage and Hour Division

The Wage and Hour Division of the Department of Labor enforces federal minimum wage, overtime pay, recordkeeping, and child labor requirements of the Fair Labor Standards Act among other worker protection laws.

The Wage and Hour Division accepts and processes complaints from employees covered by the Fair Labor Standards Act.

The Department promises that all information shared with the Wage and Hour Division is confidential, including the complaints; the name of the complainant and the nature of the complaint.⁷ Complaint information is stored in the Wage & Hour Investigative Support and Reporting Database (“WHISARD”). The Privacy Impact Assessment for WHISARD states that

⁴ DOL/GOVT-1.

⁵ 20 C.F.R. 10.10.

⁶ Office of Workers’ Compensation Programs, *Federal Employees’ Compensation Act (FECA) Claims Administration*, <https://www.dol.gov/agencies/owcp/FECA/about> (last accessed Feb. 5, 2025).

⁷ Wage and Hour Division, *Frequently Asked Questions: Complaints and the Investigation Process*, <https://www.dol.gov/agencies/whd/faq/workers> (last accessed Feb. 5, 2025).

“The WHISARD system does not share PII information with any internal organizations” within the Department, and that “WHISARD does not share PII with any external organization.”⁸

This confidentiality is crucial to protect workers who report wage theft by their employers from retaliation. Workers who report minimum wage violations, for example, are by definition the lowest-wage workers, and are particularly vulnerable to retaliation by employers should those employers become aware that the workers have sought to protect their rights.

C. Occupational Safety and Health Administration

The Occupational Safety and Health Administration’s mission is to ensure that America’s workers have safe and healthful working conditions free from unlawful retaliation. *See* 29 U.S.C. § 651 *et seq.* Through OSHA, workers are able to file complaints about injuries, safety issues, and retaliation. They may do so with their names or as anonymous whistleblowers.

OSHA promises to keep these complaints confidential and maintaining that confidentiality is essential to OSHA mission, which depends on vulnerable workers feeling comfortable coming forward with information about their worksite and employer and on OSHA’s ability to protect those who report violations from retaliation. In the context of this case, disclosure of OSHA records to the leader of multiple companies with ongoing OSHA

⁸ Wage and Hour Division, *Privacy and Impact Assessment – WHD – WHISARD*, <https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy/whd/whisard> (last accessed Feb. 5, 2025).

investigations presents clear risks both to workers and to the integrity of OSHA's enforcement efforts.

OSHA's databases include but are not limited to OSHA's Integrated Management Information Systems,⁹ which houses OSHA complaints both against Tesla and against Tesla's competitors. This database makes some information regarding complaints public.¹⁰ DOGE-affiliated personnel gaining access to the non-public information contained in these complaints would provide confidential information to Mr. Musk, such as regarding a claimant's personal information, or regarding claims against his competitors.

D. The Bureau of Labor Statistics

The Bureau of Labor Statistics ("BLS") was established in 1884, with a goal of collecting and publishing disinterested information about labor markets that "could promote effective, rational, and equitable decisionmaking."¹¹

It describes itself as the "principal fact-finding agency in the broad field of labor economics and statistics" and "collects, calculates, analyzes, and publishes data essential to the public, employers, researchers, and government organizations."¹²

⁹ See OSHA Integrated Management Information System, <https://www.osha.gov/ords/imis/establishment.html> (last accessed Feb. 5, 2025).

¹⁰ See, e.g., 20 partially publicly available complaints against Tesla in 2024, available at https://www.osha.gov/ords/imis/establishment.search?p_logger=1&establishment=TESLA&State=all&officetype=all&Office=all&sitezip=&p_case=all&p_violations_exist=all&startmonth=01&startday=01&startyear=2024&endmonth=12&endday=31&endyear=2024

¹¹ Janet L. Norwood, *One Hundred Years of BLS*, Monthly Labor Review 3, 3 (July 1985), <https://www.bls.gov/opub/mlr/1985/07/art1full.pdf>.

¹² U.S. Bureau of Labor Statistics, *About the U.S. Bureau of Labor Statistics*, <https://www.bls.gov/bls/about-bls.htm> (last accessed Feb. 5, 2025).

BLS is one of the “flagship” sources of statistics published by federal agencies.¹³

The quality of data from statistical agencies is highly dependent on their independence and autonomy.

Autonomy supports data quality directly by allowing leaders and staff to adhere to professional standards. It also supports trust in and use of the products of a statistical agency by reducing suspicions that the products have been manipulated for political purposes. Higher trust and better data quality operate in a positive feedback cycle with survey participation. And data quality and trust are necessary for people to use data products.¹⁴

Indeed, Congress recognized the value of statistical agencies and specifically directed them in the Foundations for Evidence-Based Policymaking Act of 2018 to “(A) produce and disseminate relevant and timely information; (B) conduct credible and accurate statistical activities; (C) conduct objective statistical activities; and (D) protect the trust of information providers by ensuring the confidentiality and exclusive statistical use of their responses.” Pub. L. No. 115-435, § 302, 132 Stat. 5529 (2019), *codified at* 44 U.S.C. § 3563.

Congress also sought to protect the collection of confidential data by statistical agencies in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA). Pub. L. No. 107-347, § 501-526, 116 Stat. 2900 (2002), *codified at* 44 U.S.C. §§ 3572-73. CIPSEA sought to use “[p]ledges of confidentiality by agencies” to “provide assurances to the public that information about individuals or organizations or provided by individuals or organizations for exclusively statistical purposes will be held in confidence and will not be used against such individuals or organizations in any agency action.” 44 U.S.C. § 3571(2). As such CIPSEA

¹³ Constance F. Citro et al., *What Protects the Autonomy of the Federal Statistical Agencies? An Assessment of the Procedures in Place to Protect the Independence and Objectivity of Official U.S. Statistics.*, 10 Stat. & Pub. Policy 1, 1 (2023).

¹⁴ *Id.* at 4.

provides that, among other things, “[d]ata or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.” *Id.* § 3572(c)(1). Further, disclosures may be permitted “only when the head of the agency approves such disclosure and the disclosure is not prohibited by any other law.” *Id.* § 3572(c)(2).

BLS’s independence can be a source of political angst, as it has a long tradition of releasing benchmark data on the state of the U.S. economy with minimal advance notice to political leaders at the White House before the public release.¹⁵ This is because BLS data releases often “move markets” and have other significant effects on the U.S. economy.¹⁶

When President Trump has previously taken issue with economic indicators released by BLS, he has attacked the Bureau’s credibility, accusing them of “fraudulently manipulating job statistics,”¹⁷ and calling their data “phoney.”¹⁸ Political leaders may wish for a BLS that is less independent; one that, for example, is more willing to give the White House longer notice of economic data so that the President can prepare his messaging; or one that alters data to support

¹⁵ Tucker Higgins, *Trump can spin economic numbers – but he likely can’t manipulate them, experts say*, CNBC (Sep. 10, 2019), <https://www.bls.gov/bls/about-bls.htm>.

¹⁶ See Julia Press & Saleha Mohsin, BNN Bloomberg, *Why Key U.S. Economic Data is under Threat* (Dec. 12, 2024), <https://www.bnnbloomberg.ca/business/company-news/2024/12/12/why-key-us-economic-data-is-under-threat/>.

¹⁷ Alicia Wallace, *Trump routinely calls economic data ‘fake.’ Here’s why that’s dangerous*, CNN (Jan. 26, 2025), <https://edition.cnn.com/2025/01/26/economy/us-economic-data-trump/index.html>.

¹⁸ Mona Chalabi, *Statisticians fear Trump White House will manipulate figures to fit narrative*, The Guardian (Jan. 30, 2017), <https://www.theguardian.com/us-news/2017/jan/30/statistics-trump-administration-numbers-manipulation>.

the President's political needs.

V. The "Department of Government Efficiency."

On November 12, 2024, then President-Elect Trump announced his intent to create the "Department of Government Efficiency" ("DOGE") to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget," to help "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.¹⁹

On the day of his inauguration, January 20, 2025, President Trump signed Executive Order 14158, Establishing and Implementing the President's "Department of Government Efficiency," ("the E.O."), reorganizing and renaming the United States Digital Service as the United States DOGE Service, established in the Executive Office of the President.²⁰

The E.O. established the role of U.S. DOGE Service Administrator in the Executive Office of the President, reporting to the White House Chief of Staff.²¹

The E.O. further established within U.S. DOGE Service a temporary organization known as "the U.S. DOGE Service Temporary Organization." The U.S. DOGE Service Temporary Organization is headed by the U.S. DOGE Service Administrator and is tasked with advancing "the President's 18-month DOGE agenda."²²

¹⁹ See Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, 7:46 PM ET), <https://truthsocial.com/@realDonaldTrump/posts/113472884874740859>.

²⁰ Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025).

²¹ *Id.* at § 3(b).

²² *Id.*

The E.O. also requires each Agency Head to establish a “DOGE Team” comprised of at least four employees within their respective agencies. DOGE Teams are required to “coordinate their work with [the U.S. DOGE Service] and advise their respective Agency Heads on implementing the President’s DOGE Agenda.”²³

The E.O. directs Agency Heads to take all necessary steps “to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems,”²⁴ but makes no mention of this directive being subject to applicable law. The E.O. nominally directs the U.S. DOGE Service to adhere to “rigorous data protection standards.”²⁵

The E.O. does not vest any statutory authority in DOGE nor has Congress acted to create statutory authority in DOGE.

VI. DOGE’S Pattern of Rapidly Entering Agencies, Seizing Critical Systems, and Unilaterally Dismantling and Restructuring Them.

Since Inauguration Day, DOGE personnel have sought and obtained unprecedented access to information systems across numerous federal agencies, including the Department of Treasury, U.S. Agency for International Development (“USAID”), National Oceanic and Atmospheric Administration, the Department of Education, the Office of Personnel Management (“OPM”), and others. DOGE personnel also played critical roles in the dismantling of USAID and ongoing concurrent efforts to largely cripple the Department of Education.

DOGE’s behavior repeats itself across virtually every agency it enters: swooping in with new DOGE staff, demanding access to sensitive systems, taking employment action against employees who resist their unlawful commands, and then beginning to re-work the agencies at

²³ *Id.* at § 3(c).

²⁴ *Id.* at 4(b).

²⁵ *Id.*

their will. This process moves incredibly quickly, with agencies established by Congress penetrated roughly overnight; or seemingly fully dismantled within a week.

A. Sensitive data takeovers at Treasury and OPM

Shortly before President Trump’s inauguration, DOGE operatives demanded access to sensitive Treasury systems, including the system used by the Bureau of the Fiscal Service (“BFS”) to control the vast majority of federal payments.²⁶ The career official serving as Acting Secretary of the Treasury prior to Secretary Bessent’s confirmation denied DOGE operatives’ request for access to the BFS payment system, and was subsequently placed on administrative leave.²⁷

Following his confirmation, Secretary Bessent granted DOGE operatives access to BFS, though the precise identities of DOGE-affiliated personnel with access, and their level of access, are not reliably known by the public.²⁸ At a minimum, DOGE-affiliated individuals have access to the wealth of personally identifiable information housed in BFS’ system. According to some

²⁶ Katelyn Polantz et al., *How an arcane Treasury Department office became ground zero in the war over federal spending*, CNN (Feb. 1, 2025), <https://www.cnn.com/2025/01/31/politics/doge-treasury-department-federal-spending/index.html>.

²⁷ Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), <https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/>.

²⁸ Andrew Duehren et al., *Elon Musk’s Team Now Has Access to Treasury’s Payment System*, N.Y. Times (Feb. 1, 2025), <https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html>.

reporting, DOGE-affiliated individuals have the ability to stop individual payments from the BFS system, to change data in the system, or to alter system code.²⁹

DOGE-affiliated individuals followed a similar pattern to seize control of OPM systems, which contain significant personally identifiable information about federal job applicants, employees, and retirees, including information about employees in the Judicial Branch and the Congressional Branch. On January 20, 2025, DOGE affiliates moved into OPM headquarters, eventually setting up sofa beds on the building's fifth floor, which contains the OPM Director's Office.³⁰

DOGE-affiliated individuals directed OPM staff to grant them high-level access to OPM computer systems, and quickly took control of them, including systems containing large troves of personally identifiable information. DOGE-affiliated individuals also locked career civil servants at OPM out of at least some of those systems, giving them completely unchecked control over the systems and the information they contain.³¹ The identities of the DOGE personnel who have access to Treasury and OPM systems and to whom sensitive information has been disclosed are not yet clear, and to the extent there is available information on those individuals, it is only available from public reporting.

B. Agency dismantlement at USAID and the Department of Education

²⁹ Vittoria Elliott et al., *A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System*, Wired (Feb. 4, 2025), <https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/>.

³⁰ *Id.*

³¹ Tim Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, Reuters (Feb. 1, 2025), <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/>.

During the week of January 27th, Elon Musk and his team began joining staff calls at USAID,³² and the DOGE team asked “detailed questions during meetings about organizational charts, contractors and aid programs.”³³ On January 29, USAID’s director of employee and labor relations was placed on leave after he reversed the terminations of dozens of senior USAID staff. DOGE had ordered him to issue “immediate termination notices to a group of employees without due process.”³⁴

On January 31, the DOGE team gained access to and control of several USAID systems at USAID.³⁵ On February 1st, two security officials at USAID were placed on administrative leave after they refused to give members of the DOGE team access to additional systems at the agency, including systems containing classified information.³⁶

As of February 2nd, “[m]ore than 1,000 USAID employees and contractors, including more than 300 people in the Bureau of Global Health and 600 in the Bureau of Humanitarian

³² Will Steakin et al., *Turmoil inside USAID as Musk calls the agency ‘criminal’ and says it ‘has to die.’* ABC News (Feb. 3, 2025), <https://abcnews.go.com/Politics/turmoil-inside-usaid-doge-reps-offices-senior-officials/story?id=118368900>.

³³ *Behind DOGE’s Standoff at USAID: Desk Searches and Elon Musk Calling*, Bloomberg News (Feb. 2, 2025), <https://www.bloomberg.com/news/articles/2025-02-03/behind-doge-s-standoff-at-usaid-desk-searches-and-elon-musk-calling>.

³⁴ Abigail Williams and Vaughn Hillyard, *Senior USAID official ousted after fighting back against removal of career leadership*, NBC News (Jan. 31, 2025), <https://www.nbcnews.com/politics/donald-trump/usaid-labor-director-pushed-fighting-back-removal-career-leadership-rcna190132>.

³⁵ Steakin, *supra* note 32.

³⁶ *Id.*

Assistance, have already been fired or furloughed” from USAID.³⁷ On February 2nd, Elon Musk tweeted: “USAID is a criminal organization. Time for it to die.”³⁸

On February 3rd, staffers at USAID were physically locked out of their headquarters in Washington, D.C. Yellow police tape and federal law enforcement officers blocked the agency’s lobby.³⁹ On February 3, Elon Musk tweeted: “We spent the weekend feeding USAID into the woodchipper. Could [sic] gone to some great parties. Did that instead.”⁴⁰

On February 3, in X Spaces, Elon Musk said about USAID, “It became apparent that its [sic] not an apple with a worm it in What we have is just a ball of worms. You’ve got to basically get rid of the whole thing. It’s beyond repair.” “We’re shutting it down.”⁴¹ On February 4th, USAID sent out an email, placing nearly its entire workforce on administrative leave.⁴²

The same pattern is emerging at the Department of Education where DOGE officials have spent the past few weeks working to unilaterally dismantle the department. According to

³⁷ Abigail Williams et al., *USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems*, NBC News (Feb. 2, 2025), <https://www.nbcnews.com/politics/national-security/usaid-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357>.

³⁸ Elon Musk (@elonmusk), X (Feb. 2, 2025, 12:20 PM ET), <https://x.com/elonmusk/status/1886102414194835755>.

³⁹ <https://abcnews.go.com/US/wireStory/usaid-headquarters-washington-blocked-after-musk-trump-agrees-118391601>.

⁴⁰ Elon Musk (@elonmusk), X (Feb. 3, 2025, 1:54 AM ET), <https://x.com/elonmusk/status/1886307316804263979>.

⁴¹ Ellen Knickmeyer, *Elon Musk says President Donald Trump has ‘agreed’ USAID should be shut down*, AP News (Feb. 3, 2025), <https://apnews.com/article/doge-musk-trump-classified-information-usaid-security-35101dee28a766e0d9705e0d47958611>.

⁴² Alex Marquardt et al., *USAID employees around the world will be placed on leave Friday and ordered to return to US*, CNN (Feb. 4, 2025), <https://www.cnn.com/2025/02/04/politics/usaid-officials-administrative-leave/index.html>.

reporting, about 20 DOGE officials are working inside the department in order to cut spending and agency staff.⁴³ Some officials with DOGE “have gained access to multiple sensitive internal systems...including a financial aid dataset that contains the personal information for millions of students enrolled in the federal student aid program.”⁴⁴ Reportedly, the dataset that DOGE-affiliated personnel infiltrated includes personal information, such as financial ⁴⁵ ⁴⁶ These actions are in anticipation of a White House executive order expected later in February that would “fulfill Trump’s campaign pledge to defund the department” by directing “the Education Department to develop a legislative plan to present to Congress. But it also will instruct the department to come up with a plan to diminish its staff and functions.”⁴⁷

On February 3rd, Musk retweeted a screenshot of a Washington Post article headline on Trump preparation of orders dismantling Education Department as DOGE probes data and responded with “👁️.”⁴⁸

⁴³ Laura Meckler, *Trump preps order to dismantle Education Dept. as DOGE probes data*, Washington Post (Feb. 3, 2025), <https://www.washingtonpost.com/education/2025/02/03/trump-education-department-dismantling-executive-order-draft/>.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *See id.*; *see also* National Student Loan Data System (NSLDS), *Frequently Asked Questions*, <https://nsldsfa.ed.gov/help/faq> (last accessed Feb. 2, 2025).

⁴⁷ Meckler, *supra* note 43.

⁴⁸ Elon Musk (@elonmusk), X (Feb. 3, 2025, 10:50 PM ET), <https://x.com/elonmusk/status/1886623446907400676>.

VII. Imminent Threats of Greater Data Misappropriation at the Department of Labor.

A. Recent threats and DOGE's intent to enter the Department of Labor.

Yesterday evening, a journalist shared on social media that her sources told her that “DOGE is going after the Department of Labor next. DOL workers have been ordered to give DOGE access to anything they want-or risk termination.”⁴⁹

As detailed in the attached affidavit of Rushab Sanghvi, General Counsel of Plaintiff AFGE, this report was substantiated by one of Plaintiff's members. *See generally* Declaration of Rushab Sanghvi, Exhibit A (“Sanghvi Decl. (Ex. A)”). That member was told by Department leadership that when Mr. Musk and his team visit the Department, they are to do whatever they ask, not to push back, not to ask questions. Sangvi Decl. (Ex. A) ¶¶ 5-6. They were told to provide access to any DOL system DOGE requested access to and not to worry about any security protocols; just do it. *Id.* Based on these statements by the Department's leadership, the employee therefore reasonably believes they could face termination if they do not comply. *Id.*

Later today, DOGE staff will enter the Department of Labor and attempt to gain access to sensitive systems to which they do not have access, using threats of employment action to coerce cooperation from the employees tasked with safeguarding the data of millions of Americans and many federal employees. DOGE staff may also attempt to begin an unlawful wholesale dismantling or restructuring of the agency to suit the private business interests or political preferences of DOGE leaders or President Trump.

B. Ongoing Department Enforcement Against Mr. Musk's Companies and Competitors.

⁴⁹ Kim Kelly (@GrimKim), X (Feb. 4, 2025, 5:04 PM ET), <https://x.com/GrimKim/status/1886898588099240401>.

Mr. Musk's companies have been subject to multiple investigations and fines by Department components.

The Occupational Safety and Health Administration ("OSHA") within the Department is responsible for enforcing safety standards at American companies. *See generally* 29 U.S.C. § 651 *et seq.* OSHA has investigated Mr. Musk's space technology company, SpaceX, over multiple safety incidents, and has fined SpaceX in connection with one worker's death and seven other serious safety incidents.⁵⁰ OSHA has also investigated and issued fines to Tesla for unsafe working conditions in its factories.⁵¹

OSHA also has open investigations into the Boring Company, and has issued it multiple fines for serious citations, according to OSHA's website.⁵²

Mr. Musk would ordinarily be unable to access non-public information regarding those investigations. *See* 18 U.S.C. § 1832(a) (Trade Secrets Act); 5 U.S.C. § 552(b)(4) (FOIA exemption for trade secrets); 5 U.S.C. § 552(b)(7)(c) (FOIA exemption for personal information in law enforcement records); 5 U.S.C. § 552(b)(7)(d) (FOIA exemption for records compiled for a law enforcement investigation). Mr. Musk and his personnel do not have legal authorization to access confidential law enforcement information about the investigations of his companies, and

⁵⁰ 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/>.

⁵¹ 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>.

⁵² 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).

those of his competitors. In light of the blanket instruction to provide DOGE employees with “anything they want,” Mr. Musk or his associates will be able to access that information simply by asking DOL employees for it.

LEGAL STANDARD

To obtain a temporary restraining order, “the moving party must show: (1) a substantial likelihood of success on the merits; (2) that it would suffer irreparable injury if the [temporary restraining order] were not granted; (3) that [such an order] would not substantially injure other interested parties; and (4) that the public interest would be furthered” by the order. *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006) (citations omitted); *see also Hall v. Johnson*, 559 F. Supp. 2d 1, 3 n.2 (“[T]he same standard applies to both temporary restraining orders and to preliminary injunctions.” (citation omitted)). “When the movant seeks to enjoin the government, the final two TRO factors—balancing the equities and the public interest—merge.” *D.A.M. v. Barr*, 474 F. Supp. 3d 45, 67 (citing *Pursuing Am.’s Greatness v. FEC*, 831 F.3d 500, 511 (D.C. Cir. 2016)).

Courts in this Circuit continue to apply a “sliding scale” approach, wherein “a strong showing on one factor could make up for a weaker showing on another.” *Changji Esquel Textile Co. v. Raimondo*, 40 F.4th 716, 726 (D.C. Cir. 2022) (internal quotation marks and citation omitted) (noting potential tension in case law but reserving the question of “whether the sliding-scale approach remains valid”); *National Railroad Passenger Corp. (Amtrak) v. Sublease Interest Obtained Pursuant to an Assignment and Assumption of Leasehold Interest Made as of Jan. 25, 2007*, Case. No. 22-1043, 2024 WL 34443596, at *1-2 (D.D.C. July 15, 2024) (recognizing that district courts remain bound by sliding-scale precedent). All four factors favor Plaintiffs here.

ARGUMENT

I. Plaintiffs are Likely to Succeed on the Merits.

As a threshold matter, the Department of Labor’s decision (whether on its own accord or at the direction of DOGE) to grant DOGE employees access to Department of Labor systems, by threatening termination of any employee who does not “give DOGE access to anything they want,” constitutes final agency action subject to judicial review under the Administrative Procedure Act, 5 U.S.C. § 704. 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) (quoting *Bennett v. Spear*, 520 U.S. 154, 177-178 (1997)). DOL’s intended action satisfies both prongs.

D.C. Circuit precedent leaves no doubt on this point: 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 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). If a policy allowing information disclosures constitutes final agency action, a decision *requiring* disclosures must be as well.

Independent analysis of the *Bennett* prongs also makes clear that the Department of Labor’s action constitutes final agency action. In evaluating the first prong, the D.C. Circuit considers “whether the action is ‘informal, or only the ruling of a subordinate official, or tentative.’” *Soundboard Association v. F.T.C.*, 888 F.3d 1261, 1267 (D.C. Cir. 2018) (quoting *Abbott Labs v.*

Gardner, 387 U.S. 136, 151 (1967)). The decision to disclose government information and data to entities outside a government agency, and without a permissible purpose, is not informal; rather, it is a decision of agency policy and practice. Nor is it tentative, reversible, or reviewable by the agency: once information has been disclosed and is no longer within agency control, the agency loses any meaningful ability to retract or control the data. Analysis of the second prong is equally clear: the Department of Labor’s decision has determined Department obligations to disclose data and information within its control, affected the rights of the entities about whom it retains data, and creates significant legal consequences as a result of the Department’s violation of numerous laws.

And should the Court conclude that the Department of Labor’s decision to disclose its information to DOGE employees reflects a violation of policy, rather than a change to policy, that distinction does not change the nature of the decision: it remains a consummation of agency decisionmaking with identical implications for rights and obligations as a corresponding change.

A. DOGE is Operating Without Any Legal Authority and Actions it Takes are *Ultra Vires*.

Under the Constitution, the power to create federal offices is assigned to Congress. *See Nat’l Fed. Of Indep. Bus. v. OSHA*, 595 U.S. 109, 117 (2022); *see also Freytag v. Comm’r*, 501 U.S. 868, 883 (1991) (recognizing “Congress’ authority to create offices[.]”). Accordingly, agencies “possess only the authority that Congress has provided.” *Nat’l Fed. Of Indep. Bus.*, 595 U.S. at 117. The President may not seize legislative power to vest a new White House entity with authorities not granted to it by Congress, or purport to empower the entity to take actions that Congress has entrusted to other agencies. DOGE’s sweeping attempts to claim and exercise power that may only be vested in them by Congress, and have already been entrusted to other agencies, are *ultra vires*.

As described above, DOGE is a government office that was created within the Executive Office of the President by an Executive Order that “publicly renamed” the United States Digital Service “as the United States DOGE Service.” E.O. § 3. DOGE’s work is led by the USDS Administrator, a position newly created by the EO, which is placed within EOP and formally accountable only to the White House Chief of Staff. *See Id.* § 3(b). DOGE also exercises supervisory authority over the U.S. DOGE Service Temporary Organization, which is an inferior component also created by the E.O. and organized under DOGE. *Id.* (citing 5 U.S.C. § 3161). DOGE’s mandate, as defined in the E.O., is “to implement the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.” *Id.* § 1. The E.O. contemplates that employees of DOGE will conduct work at other agencies and, to that end, directs Agency Heads to take all necessary steps “to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems.” *Id.* § 4(b).

The President’s establishment of DOGE is unusual. Indeed, it is unprecedented. Other components within EOP operate on the basis of statutory authority, either their own or that of a supervising component.⁵³ For instance, DOGE’s predecessor entity, the U.S. Digital Service, was established by Presidential directive but organized under OMB’s purview, thereby ensuring that its operation was subject to oversight and control by a statutorily created official within a

⁵³ *See, e.g.*, 15 U.S.C. § 1023 (creating the Council of Economic Advisers); 31 U.S.C. § 501 (creating Office of Management and Budget); 42 U.S.C. § 4342 (Council on Environmental Quality); 42 U.S.C. § 6611 (establishing Office of Science and Technology Policy); 50 U.S.C. § 3021 (establishing the National Security Council).

statutorily created agency.⁵⁴ But DOGE as currently constituted has neither statutory authority, nor oversight from a component of EOP that does. Indeed, the manner in which it is funded—through its own, independent apportionment⁵⁵—confirms that it operates independently within EOP, subject to oversight only by the White House Chief of Staff. DOGE should, accordingly, be able to exercise only the authorities granted to it directly by Congress (none).

In the absence of Congressional authorization to take concrete actions, DOGE may still serve the limited function of advising and assisting the President, but it is not empowered to perform any other functions. Specifically, DOGE has no authority in law to direct operations or decisions at federal agencies, or access or manage sensitive data entrusted to those agencies.

But DOGE has been purporting to exercise much wider authorities during its blitzes into other federal agencies. At the Department of Treasury and OPM, DOGE staff have reportedly forced their way into sensitive information technology systems containing information that is by

⁵⁴ See U.S. Digital Service, Report to Congress (2016), <https://www.usds.gov/report-to-congress/2016/> (explaining that “[a]t its creation, USDS was administratively placed within the Office of the Federal CIO,” but later reorganized within OMB and directly supervised by “the Deputy Director of Management”); see also U.S. Gov’t Accountability Off., GAO-22-104492, Information Technology: Digital Service Programs Need to Consistently Coordinate on Developing Guidance for Agencies (Dec. 10, 2021), <https://www.gao.gov/products/gao-22-104492> (characterizing U.S. Digital Service as a component within OMB); U.S. Gov’t Accountability Off., GAO-16-602, Digital Service Programs (Aug. 15, 2016), (same).

⁵⁵ See Peter Cohn, *White House opens funding spigot for DOGE expenses*, Roll Call (Feb. 4, 2025), <https://rollcall.com/2025/02/04/white-house-opens-funding-spigot-for-doge-expenses/> (noting the nearly \$7 million in funding apportioned directly to DOGE).

law only to be managed and accessed by agency staff.⁵⁶ And when agency staff resisted these unlawful incursions, they were placed on leave from their agency.⁵⁷

At USAID, DOGE similarly took over sensitive agency information systems, placing employees who resisted on administrative leave, and purported to direct the immediate termination of USAID senior staff.⁵⁸ *See also* Compl. at ¶¶ 50-58. As the agency was rapidly wound down and

⁵⁶ Vittoria Elliott et al., *A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System*, *Wired* (Feb. 4, 2025), <https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/>; Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payments System*, *N.Y. Times* (Feb. 1, 2025), <https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html>; Jeff Stein et al., *Senior U.S. official exits after rift with Musk allies over payment system*, *Wash. Post* (Jan. 31, 2025), <https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/>.

⁵⁷ Stein et al., *supra* note 56.

⁵⁸ Will Steakin et al., *Turmoil inside USAID as Musk calls the agency 'criminal' and says it 'has to die.'* *ABC News* (Feb. 3, 2025), <https://abcnews.go.com/Politics/turmoil-inside-usaid-doge-reps-offices-senior-officials/story?id=118368900>; *Behind DOGE's Standoff at USAID: Desk Searches and Elon Musk Calling*, *Bloomberg News* (Feb. 2, 2025), <https://www.bloomberg.com/news/articles/2025-02-03/behind-doge-s-standoff-at-usaid-desk-searches-and-elon-musk-calling>; Abigail Williams and Vaughn Hillyard, *Senior USAID official ousted after fighting back against removal of career leadership*, *NBC News* (Jan. 31, 2025), <https://www.nbcnews.com/politics/donald-trump/usaid-labor-director-pushed-fighting-back-removal-career-leadership-rcna190132>; Abigail Williams et al., *USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems*, *NBC News* (Feb. 2, 2025), <https://www.nbcnews.com/politics/national-security/usaid-security-leaders-removed-refusing-elon-musks-doge-employees-acce-rcna190357>; Will Steakin et al., *Turmoil inside USAID as Musk calls the agency 'criminal' and says it 'has to die.'* *ABC News* (Feb. 3, 2025), <https://abcnews.go.com/Politics/turmoil-inside-usaid-doge-reps-offices-senior-officials/story?id=118368900>; *Behind DOGE's Standoff at USAID: Desk Searches and Elon Musk Calling*, *Bloomberg News* (Feb. 2, 2025), <https://www.bloomberg.com/news/articles/2025-02-03/behind-doge-s-standoff-at-usaid-desk-searches-and-elon-musk-calling>; Abigail Williams and Vaughn Hillyard, *Senior USAID official ousted after fighting back against removal of career leadership*, *NBC News* (Jan. 31, 2025), <https://www.nbcnews.com/politics/donald-trump/usaid-labor-director-pushed-fighting-back-removal-career-leadership-rcna190132>; <https://abcnews.go.com/US/wireStory/usaid-headquarters-washington-blocked-after-musk-trump-agrees-118391601>.

shuttered (despite Congressional authorization and appropriation), the head of DOGE claimed credit for “feeding USAID into the woodchipper” in a matter of days.⁵⁹ DOGE is taking similar actions at the Department of Education.⁶⁰ *See also* Compl. at ¶¶ 59-64.

DOGE does not have any statutory authority to access sensitive information systems, to make personnel decisions for agencies, or to restructure or terminate their operations. But it has been to date freely exercising such *ultra vires* authority at a variety of federal agencies, and absent action from this Court, will seek to do the same at the Department of Labor. Indeed, employees at the Department of Labor have reported that were instructed to “do whatever” the DOGE personnel ask, “not to push back, not to ask questions.” Sanghvi Decl. (Ex. A) ¶¶ 5-6. These employees were specifically instructed to “provide access to any DOL system they [DOGE personnel] requested access to and not to worry about any security protocols; just do it.” *Id.* These employees were given to understand that “they could face termination if they did not comply.” *Id.*

B. DOGE and the Department will violate the Privacy Act

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, § 2(b), 2(b)(4), 88 Stat. 1896 (1974), *codified as amended at* 5 U.S.C. § 552a. “[I]n order to protect the

⁵⁹ Elon Musk (@elonmusk), X (Feb. 3, 2025, 1:54 AM ET), <https://x.com/elonmusk/status/1886307316804263979>.

⁶⁰ Laura Meckler, *Trump preps order to dismantle Education Dept. as DOGE probes data*, Washington Post (Feb. 3, 2025), <https://www.washingtonpost.com/education/2025/02/03/trump-education-department-dismantling-executive-order-draft/>.

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.* § 2(a)(5), 88 Stat. at 1896.

To that end, the Privacy Act regulates “records,” defined 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).

Individuals under the Privacy Act are any “citizen of the United States or [] alien lawfully admitted for permanent residence.” *Id.* at § 552a(a)(2).

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, “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 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 Department houses a number of systems of records subject to the Privacy Act, many of which contain personally identifiable information.⁶¹ Because DOGE is an entity within the White House rather than the Department, any disclosure of records containing PII by the

⁶¹ See, e.g., *Privacy Impact Assessments*, U.S. Dep’t of Labor, Office of the Assistance Secretary for Administration and Management, <https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy> (collecting Privacy Impact Assessments for over 50 systems across various Department functions).

Department to DOGE would fall under the prohibition in § 552a(b). While § 552a(b) contains thirteen exceptions, none of them apply here.

C. DOGE and the Department's Actions Risk Violating Laws Protecting Against Financial Conflicts of Interest and Protecting Competition

Based on the information available to Plaintiffs, it is likely that Defendants are also acting contrary to laws protecting against financial conflicts of interest and protecting market competition. Federal law prohibits any person “participating personally and substantially in an official capacity” in matters where they may have a financial interest from doing so. To the extent DOGE and the Department are being directed by Elon Musk or others on leave from companies he controls, they are compromising federal conflicts of interest and ethics protections. See, 19 USC 208(a) (criminal statute prohibiting employee from participating personally in matters to which they have a financial interest); 5 CFR 2635.402(a) (regulation on “disqualification of financial interest” pursuant to 5 CFR 2635.402(a))).

In addition to the risk of involvement in Department of Labor activities and proceedings from which they are ethically conflicted, DOGE personnel including, but not limited to Mr. Musk, will be able to gain access to trade secrets of entities in direct competition with their own business interests. Such access would ordinarily be impossible, *see* 18 U.S.C. § 1832(a) (Trade Secrets Act); 5 U.S.C. § 552(b)(4) (FOIA exemption for trade secrets), but in light of the blanket instruction to Department of Labor employees to provide DOGE employees “with anything they want,” Mr. Musk or his associates will be able to access that information simply by requesting it.

II. Plaintiffs will suffer immediate, irreparable injury should DOGE be able to assert unlawful authority at the Department.

Should DOGE be permitted to enter the Department today and freely exercise unlawful authority, Plaintiffs and the nation will be irreparably harmed. “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). The D.C. Circuit has confirmed that “‘obstacles’ that ‘unquestionably make it more difficult for [an organization] to accomplish [its] primary mission . . . provide injury for purposes both of standing and irreparable harm.’” *Whitman-Walker Clinic, Inc. v. HHS*, 485 F. Supp. 3d 1, 56 (D.D.C. 2020) (emphasis in original) (quoting *League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 9 (D.C. Cir. 2016)); see also *Open Communities All. v. Carson*, 286 F.Supp. 3d 148, 178 (D.D.C. 2017) (finding irreparable harm and granting injunction where agency action would “perceptibly impair [plaintiff’s] programs and directly conflict with [its] mission” of assisting families receiving housing vouchers “gain access to greater opportunity”); *Council on Am.-Islamic Rels. v. Gaubatz*, 667 F. Supp. 2d 67, 76–77 (D.D.C. 2009) (finding irreparable harm and granting injunction against “any use” of stolen employee documents or electronic information, noting that access to “confidential employee personal information” was “of particular concern”). *Cf. generally FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 395 (2024) (recognizing that organizations suffer injury when government action “perceptibly impair[s]” their ability to carry out their core mission or “directly affect[s] and interfere[s] with [their] core business activities”).

Defendants’ gaining unauthorized access to sensitive employee health and disability 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) (“[w]hen 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”). Among DOL’s functions, it administers workers compensation programs, including the federal employees’ compensation claims through the Federal Employees’ Compensation Act (FECA) Claims Administration. This administration adjudicates new claims for benefits and manages ongoing cases; pays medical expenses and compensation benefits to injured workers and survivors; and helps injured employees return to work when they are medically able to do so. DOL maintains countless pieces of sensitive medical data through this administration and other databases, including interface with systems at other agencies. Unauthorized access to or dissemination of this information will unquestionably and irreparably harm millions of workers and their families.

The plaintiff unions will suffer their own irreparable harm if they cannot ensure worker privacy. In *Human Touch DC*, this court found irreparable harm to a healthcare provider whose former employee inappropriately accessed just a handful of emails containing confidential patient information. The court reasoned that the breach would compromise Human Touch’s reputation, relationship with patients, and ability to provide services if it could not be seen as protecting sensitive patient information. 2015 WL 12564166, at *5. So too here, where federal employees depend on their unions to protect them from these sorts of breaches, and the unions depend on that

trust for continued viability.⁶² For example, Plaintiff AFGE has assisted its members in filing approximately 1,500 workers' compensation claims through FECA for its own federal employee members in 2024 alone. Sanghvi Decl. (Ex. A) ¶¶ 7-9. These claims include detailed personal medical information and financial information, such as about injuries, illness, prognosis, treatment plans, and corresponding financial harm and benefits determinations. *Id.* ¶ 8. These 1,500 claims in 2024 represent only a small fraction of the total claims that AFGE members have submitted. *Id.* ¶ 9. AFGE and these members will be irreparably harmed if their private medical and financial information, submitted through a confidential claims adjudication process, becomes public. *Id.* ¶ 10.

In addition, Plaintiffs will also suffer irreparable harm in the form of chilling their ability to report legal violations by other employers to the Department of Labor. As plaintiffs have declared, their members routinely report legal violations to the Department of Labor. *See* Sanghvi Decl. (Ex. A) ¶¶ 4-8; Declaration of Matthew Ginsburg, Exhibit B ("Ginsburg Decl. (Ex. B)") ¶¶ 4-10; Declaration of Steven K. Ury, Exhibit C ("Ury Decl. (Ex. C)") ¶¶ 4-5. This includes but is not limited to reporting violations on the Fair Labor Standards Act, the Occupational Safety and Health Act, and claims under the Black Lung Benefits Act. Sanghvi Decl. (Ex. A) ¶¶ 4-8; Ginsburg Decl. (Ex. B) ¶¶ 4-10; Ury Decl. (Ex. C) ¶¶ 4-5. The Department of Labor's guarantees of confidentiality are not only required by law, but also essential to these workers' willingness to report these legal violations. These workers reasonably fear retaliation from their reporting, which is why the submissions are confidential. *See* Ury Decl. (Ex. C) ¶ 7 ("The promise of confidentiality

⁶² Indeed, just as in *Human Touch*, America's employers will also suffer harm from their employees losing confidence that their privacy will be protected on the job.

is an essential condition”); Ginsburg Decl. (Ex. A) ¶ 6 (“This assurance [of confidentiality] is vital because fear of employer retaliation is a powerful deterrent[.]”); Mr. Musk and other Defendants’ unlawful access to this information will cause irreparable harm, either by facilitating this retaliation or deterring workers from reporting in the first place.

Courts have recognized that creating a chilling effect from engaging in First Amendment activity, such as reporting violations of the law, constitutes irreparable harm. Indeed, “[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976); *see also Newsom v. Norris*, 888 F.2d 371, 378 (6th Cir. 1989) (“[E]ven minimal infringement upon First Amendment values constitutes irreparable injury sufficient to justify injunctive relief.”). The chilling effect due to “fear of employer retaliation” is well recognized as “irreparable harm.” *See Pye ex rel. N.L.R.B. v. Excel Case Ready*, 238 F.3d 69, 75 (1st Cir. 2001); *see also NLRB v. Electro-Voice, Inc.*, 83 F.3d 1559, 1572 (7th Cir. 1996) (noting the “chilling effect” on organization that often follows the illegal discharge of key union members).

Finally, Plaintiffs will suffer irreparable harm if DOGE is permitted to take sweeping, unilateral, and unauthorized control over the Department’s personnel and organization. The types of actions that DOGE has taken at other agencies, including terminating programs, restructuring agencies, and taking adverse employment actions against personnel that DOGE leaders view as an impediment to their agenda, will irreparably impair the Department’s ability to execute its mission. Plaintiffs rely on the Department and its programs to ensure fair treatment of American workers. Ury Decl. (Ex. C) ¶¶ 3-9; Ginsburg Decl. (Ex. A) ¶¶ 3-7. Rapid, arbitrary, and ill-considered fundamental changes to the Department’s work and responsibilities will wreak havoc for Plaintiffs, their members, and the communities they serve. *Cf., e.g., Dep’t of Homeland Sec.*

v. Regents of the Univ. of Calif., 591 U.S. 1, 30-33 (2020) (beneficiaries of federal programs have reliance interests in the programs’ ongoing operation, and the termination of such programs should not be carried out in arbitrary or capricious ways). Given DOGE’s repeated pattern of doing this at other agencies, this court need not wait until it happens at DOL to enjoin it.

III. The balance of equities and the public interest favor Plaintiffs.

“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 Communities Alliance v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017) (citing *League of Women Voters of U.S.*, 838 F.3d at 12). “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 the Government’s interests as if it were a private party, the balance of equities and public interest would still overwhelmingly favor Plaintiffs. Neither Defendants nor any of their associates have any lawful or legitimate need to commandeer Department of Labor information systems or the data within them in this abrupt, unlawful, unreasoned, and chaotic manner.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court grant their motion and enter a temporary restraining order enjoining Defendants from providing any person with non-public Department of Labor information or access to such information regarding his or her

business interests or direct competitors to his or her business interests, enjoining the Department from granting DOGE access to any systems of records that DOGE lacks statutory authority to access, and enjoining DOGE from exercising *ultra vires* authority by purporting to require access those systems, take adverse actions against Department employees for preserving the integrity of those systems, or effectuate restructuring or reorganizing of the Department or any of its components. In the alternative, Plaintiffs ask this Court to enter a brief stay of Defendants' actions pursuant to 5 U.S.C. § 705.

Dated: February 5, 2025

Respectfully submitted,

/s/ Mark B. Samburg

Mark B. Samburg (D.C. Bar No. 1018533)
 Aman T. George (D.C. Bar No. 1028446)
 Benjamin Seel (D.C. Bar No. 1035286)
 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
 bseel@democracyforward.org
 rhomer@democracyforward.org
 rthurston@democracyforward.org
 strivedi@democracyforward.org
 sperryman@democracyforward.org
Counsel for Plaintiffs

Teague P. Paterson (D.C. Bar No. 144528)
 Matthew S. Blumin (D.C. Bar No. 144528)
 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)
and Local 3707*

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*

* Motion for admission *pro hac vice*
forthcoming