UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AFL-CIO, *et al.*, *Plaintiffs*, v. DEPARTMENT OF LABOR, *et al.*, *Defendants*.	Case No. 1:25-cv-00339

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

TABLE OF CONTENTS

INTRODUCTION 1

Factual Background 2

I. The Establishment of DOGE 2

II. Threats to DOL, HHS, and CFPB 4

A. DOL establishes the DOL DOGE Access Policy and authorizes DOGE to access DOL systems. 4

B. HHS establishes the HHS DOGE Access Policy. 8

C. CFPB establishes the CFPB DOGE Access Policy. 12

Statutory and Legal Framework 15

III. The Privacy Act of 1974 15

IV. The Administrative Procedure Act 16

LEGAL STANDARD 16

ARGUMENT 17

I. Plaintiffs are Likely to Succeed on the Merits. 17

A. Plaintiffs have standing. 17

1. Plaintiffs AFL, AFGE, CWA, and SEIU have demonstrated standing to challenge the unlawful disclosure of Department of Labor data. 18

2. Plaintiffs CWA, AFSCME, and SEIU have demonstrated standing to challenge the unlawful disclosure of HHS data. 21

3. Plaintiffs EAMF and VPLC have demonstrated standing to challenge the unlawful disclosure of CFPB data. 22

B. Plaintiffs are likely to succeed on their APA claims. 23

1. Defendants' sharing of data and information systems with DOGE constitutes final agency action. 23

2. Defendants' DOGE Access Policies Are Contrary to Law. 24

3. Defendants' DOGE Access Policies Are Arbitrary and Capricious. 30

4. Defendants' DOGE Access Policies Are Procedurally Infirm. 33

C. DOGE is Operating Without Any Legal Authority and Actions it Takes are *Ultra Vires*. 34

II. Continuing to Allow DOGE to Unlawfully Access Systems and Records Will Cause Plaintiffs to Suffer Immediate, Irreparable Injury. 37

III. The balance of equities and the public interest favor Plaintiffs. 41

CONCLUSION 42

TABLE OF AUTHORITIES

Cases **Page(s)**

Abbott Labs v. Gardner, 387 U.S. 136 (1967) 23

Action All. of Senior Citizens of Greater Philadelphia v. Heckler, 789 F.2d 931 (D.C. Cir. 1986) 19

Am. Ass'n of Cosmetology Schools v. Devos, 258 F. Supp. 50 (D.D.C. 2017) 17

Armstrong v. Exec. Off. of the President, Off. of Admin., 1 F.3d 1274 (D.C. Cir. 1993) 36

Barton v. District of Columbia, 131 F. Supp. 2d 236 (D.D.C. 2001) 16

Bennett v. Spear, 520 U.S. 154 (1997) 22

C.G.B. v. Wolf, 464 F. Supp. 3d 174 (D.D.C. 2020) 40

Capital Area Immigrants' Rights Coalition ("CAIR") v. Trump, 471 F. Supp. 3d 25 (D.D.C. 2020) 19, 21

Changji Esquel Textile Co. v. Raimondo, 40 F.4th 716 (D.C. Cir. 2022) 16

Chaplaincy of Full Gospel Churches v. England, 454 F.3d 290 (D.C. Cir. 2006) 15

Clean Air Council v. Pruitt, 862 F.3d 1 (D.C. Cir. 2017) 32

Conservative Baptist Ass'n of Am., Inc. v. Shinseki, 42 F. Supp. 3d 125 (D.D.C. 2014) 19

Council on Am.-Islamic Rels. v. Gaubatz, 667 F. Supp. 2d 67 (D.D.C. 2009) 37

D.A.M. v. Barr, 474 F. Supp. 3d 45 (D.D.C. 2020) 16

Dep't of Homeland Sec. v. Regents of the Univ. of Cal., 591 U.S. 1 (2020) 32

Dickson v. Sec'y of Def., 68 F.3d 1396 (D.C. Cir. 1995) 29

Elrod v. Burns, 427 U.S. 347 (1976) 39

Food & Drug Admin. v. All. for Hippocratic Med., 602 U.S. 367 (2024) 17, 18

Freytag v. Comm'r, 501 U.S. 868 (1991) 34

Haddon v. Walters, 43 F.3d 1488 (D.C. Cir. 1995) 36

Hall v. Johnson, 599 F. Supp. 2d 1 (D.D.C. 2009) 15

Hawai'i Psychiatric Soc'y v. Ariyoshi, 481 F. Supp. 1028 (D. Haw. 1979) 38

Hirschfeld v. Stone, 193 F.R.D. 175 (S.D.N.Y. 2000) 38

Human Touch DC, Inc. v. Merriweather, No. 15-CV-00741 (APM), 2015 WL 12564166 (D.D.C. May 26, 2015) 37

Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333 (1977) 16

In Re: Executive Office of the President, Petitioner, 215 F.3d 20 (D.C. Cir. 2000) 36

League of Women Voters of U.S. v. Newby, 838 F.3d 1 (D.C. Cir. 2016) 17, 37, 40

Liquid Energy Pipeline Ass'n v. Fed. Energy Regul. Comm'n, 109 F.4th 543 (D.C. Cir. 2024) 32

Metro. Wash. Chapter, Associated Builders & Contractors, Inc. v. D.C., 62 F.4th 567 (D.C. Cir. 2023) 16

Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983) 29

Nat'l Fed. Of Indep. Bus. v. OSHA, 595 U.S. 109 (2022) 34

Nat'l R.R Passenger Corp. (Amtrak) v. Sublease Interest Obtained Pursuant to an Assignment & Assumption of Leasehold Interest Made as of Jan. 25, 2007, No. 22-1043, 2024 WL 34443596 (D.D.C. July 15, 2024) 16

Nat'l Sec. News Serv. v. Dep't of the Navy, 584 F. Supp. 2d 94 (D.D.C. 2008) 38

Nat'l Treasury Emps. Union v. United States, 101 F.3d 1423 (D.C. Cir. 1996) 19

Newsom v. Norris, 888 F.2d 371 (6th Cir. 1989) 39

NLRB v. Electro–Voice, Inc., 83 F.3d 1559 (7th Cir. 1996) 40

Open Communities All. v. Carson, 286 F.Supp. 3d 148 (D.D.C. 2017) 37, 40

PETA v. Dep't of Ag., 797 F.3d 1087 (D.C. Cir. 2015) 17, 19, 21

Plante v. Gonzalez, 575 F.2d 1119 (5th Cir. 1978) 38

Pursuing Am.'s Greatness v. FEC, 831 F.3d 500 (D.C. Cir. 2016) 16

Pye ex rel. N.L.R.B. v. Excel Case Ready, 238 F.3d 69 (1st Cir. 2001) 40

Soundboard Association v. F.T.C., 888 F.3d 1261 (D.C. Cir. 2018) 23

U.S. Army Corps of Eng'rs v. Hawkes Co., Inc., 578 U.S. 590 (2016) 22

Venetian Casino Resort, L.L.C. v. EEOC, 409 F.3d 359 (D.C. Cir. 2005) 18

Venetian Casino Resort, L.L.C. v. EEOC, 530 F.3d 925 (D.C. Cir. 2008) 22

Warth v. Seldin, 422 U.S. 490 (1975) 17

Whitman-Walker Clinic, Inc. v. HHS, 485 F. Supp. 3d 1 (D.D.C. 2020) 37

Statutes

5 U.S.C. § 706 15

12 U.S.C. §§ 5514-15, 5562-64 12

15 U.S.C. § 1023 35

18 U.S.C. § 1832 31

18 U.S.C. § 1832(a) 6

18 U.S.C. § 208(a) 31

20 C.F.R. § 10.10 (2025) 4, 5, 26, 32

29 C.F.R. § 71 26

31 U.S.C. § 1535(a) 34

31 U.S.C. § 501 35

40 U.S.C. § 11331(a). 28

42 U.S.C. § 4342 35

42 U.S.C. § 6611 35

44 U.S.C. § 2201 36

44 U.S.C. § 3553(h)(2)(F) 28

44 U.S.C. § 3554(a)(1)(A) 27, 28, 30

44 U.S.C. § 3554(a)(1)(A). 27

44 U.S.C. § 3572(c)(1) 26

45 C.F.R. § 164.306(a) 27

45 C.F.R. §§ 5b.2(a) 27

5 U.S.C. § 2302(b)(9)(D) 25

5 U.S.C. § 552(b)(4) 6

5 U.S.C. § 552(b)(7) 6

5 U.S.C. § 702 15

5 U.S.C. §§ 552a(b)(1)-(13 15

50 U.S.C. § 3021 35

Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA). Pub. L. No. 107-347, §§ 501-526, 116 Stat. 2900 (2002) 7

Exec. Order No. 14158, Establishing and Implementing the President's 'Department of Government Efficiency' (Jan. 20, 2025) 1, 2

Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-58 25, 26

Privacy Act of 1974, 88 Stat. 1896 (1974), *codified as amended at* 5 U.S.C. § 552a 14, 24

Pub. L. 104–191, 110 Stat. 1936 9

Rules

12 C.F.R. 1070.40-48 32

12 C.F.R. § 1070.59 28

12 C.F.R. § 1070 13

45 C.F.R. § 5b 32

65 Fed. Reg. 48000, 48000-03 (Aug. 4, 2000) (SORN 09-70-0513) 10

67 Fed. Reg. 4965, 4965 (Feb. 1, 2002) (SORN 09-90-0010 11

73 Fed. Reg. 11643, 11644 (March 4, 2008) (SORN 09-70-0512) 10

84 Fed. Reg. 2230, 2231-32 (Feb. 16, 2019) (SORN 09-70-0541) 10

86 Fed. Reg. 68262, 68263-64 (Dec. 1, 2021) (SORN 09-90-2103) 10

Disclosure of Loan-Level HMDA Data, 84 Fed. Reg. 649, 664-65 (Jan. 31, 2019) 13

Other Authorities

Julia Press & Saleha Mohsin, W*hy Key U.S. Economic Data is under Threat*, BNN Bloomberg (Dec. 12, 2024), https://www.bnnbloomberg.ca/business/company-news/2024/12/12/why-key-us-economic-data-is-under-threat 7

About OSHA, U.S. Dep't of Labor, OSHA, https://www.osha.gov/aboutosha (last accessed Feb 12, 2025) 5

Aimee Picchi, *The White House says Elon Musk is a "special government employee." Here's what that means*, CBS News (Feb. 6, 2025), https://www.cbsnews.com/news/elon-musk-special-government-employee-what-does-that-mean/. 2

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 7

Anna Wilde Matthews and Liz Essley Whyte, *DOGE Aides Search Medicare Agency Payment Systems for Fraud*, The Wall Street Journal (Feb. 5, 2025), https://www.wsj.com/politics/elon-musk-doge-medicare-medicaid-fraud-e697b162 8

Bobby Allen et al., *Musk's team takes control of key systems at Consumer Financial Protection Bureau*, NPR (Feb. 7, 2025), https://www.npr.org/2025/02/07/g-s1-47322/musks-team-takes-control-of-key-systems-at-consumer-financial-protection-bureau. 11

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 6

CFPB, *CFPB Hits 10 Million Complaints Milestone*, YouTube.com (Jan. 22, 2025), https://www.youtube.com/watch?v=ALcMFm7zaGg 12

CFPB, *Mortgage Data (HMDA)*, https://www.consumerfinance.gov/data-research/hmda/ 13

CFPB, *Privacy Impact Assessment, Consumer Response System* (Aug. 2024), https://files.consumerfinance.gov/f/documents/cfpb_consumer-response-system-pia-v2_2024-08.pdf. 12

CFPB, *Privacy Impact Assessment, Supervision, Enforcement, and Fair Lending Data* at 3 (Jan. 26, 2016), https://files.consumerfinance.gov/f/2016_cfpb_privacy-impact-assessment-supervision-enforcement-and-fair-lending-data.pdf 13

CMS, CMS Breach Response Handbook (Nov. 7, 2022), https://security.cms.gov/policy-guidance/cms-breach-response-handbook 27

CMS, FAQ: What is HIGLAS, https://www.cms.gov/research-statistics-data-and-systems/computer-data-and-systems/higlas/downloads/faq.pdf#:~:text=HIGLAS%20strengthens%20the%20management%20of,collect%20outstanding%20debts%20more%20timely (accessed on Feb. 9, 2025)..... 8

CMS, Medicaid Integrity Program Systems (Dec. 28, 2017), https://www.hhs.gov/foia/privacy/sorns/09700599/index.html (SORN 09-70-0599)..... 10

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. Pol'y 1, 4 (2023). 7

Consumer Financial Protection Bureau, *Privacy Impact Assessments (PIAs)*, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ 12

Ctr. for Medicare & Medicaid Servs., *CMS Statement on Collaboration with DOGE*, (Feb. 5, 2025), https://www.cms.gov/newsroom/press-releases/cms-statement-collaboration-doge 9

Dan Diamond et al., *DOGE broadens sweep of federal agencies, gains access to health payment systems*, The Washington Post (Feb. 5, 2025), https://www.washingtonpost.com/health/2025/02/05/doge-health-agencies-labor/ 8

Dep't of Gov. Efficiency (@DOGE), X (Feb. 7, 2025, 4:10 PM EST), https://x.com/DOGE/status/1887972340446683576 8

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). 4

Elon Musk (@elonmusk), X (Feb. 11, 2025, 1:23 AM), https://x.com/elonmusk/status/1889198569518719122..... 8

Elon Musk (@elonmusk), X (Feb. 5, 2025 12:01 PM ET), https://x.com/elonmusk/status/1887184902543577590..... 8

Elon Musk's DOGE has swept into 15 federal agencies. Here's what to know, Wash. Post (Feb. 8, 2025), https://www.washingtonpost.com/business/2025/02/08/elon-musk-doge-federal-agencies-cuts-employees/. 2

Enforcement, U.S. Dep't of Labor, Emp. Benefits Sec. Admin.,https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/enforcement (last accessed Feb. 10, 2025) 5

Faiz Siddiqui et al., *19-year-old Musk surrogate takes on roles at State Department and DHS*, Wash. Post (Feb. 10, 2025), https://www.washingtonpost.com/business/2025/02/10/musk-doge-state-department-surrogate/. 3

Frequently Asked Questions: Complaints and the Investigation Process, U.S. Dep't of Labor, Wage and Hour Division, https://www.dol.gov/agencies/whd/faq/workers (last accessed Feb. 5, 2025) 5

General Departmental Management, OpenOMB (accessed on Feb. 6, 2025), https://openomb.org/file/11293991 35

HHS, SORN 09-70-0514 (Dec. 21, 2017), https://www.hhs.gov/foia/privacy/sorns/09700514/index.html 10

HHS, SORN 09-70-0525 (Feb. 7, 2019), https://www.hhs.gov/foia/privacy/sorns/09700525/index.html 10

Holly Otterbein and Megan Messerly, *Vought takes helm at CFPB after Musk incursion*, POLITICO (Feb. 8, 2025), https://www.politico.com/news/2025/02/08/vought-takes-helm-at-cfpb-after-musk-incursion-00203247 11

Ivan Pereira and Emily Chang, *Here are all the agencies that Elon Musk and DOGE have been trying to dismantle so far*, ABC News (Feb. 11, 2025), https://abcnews.go.com/Politics/elon-musks-government-dismantling-fight-stop/story?id=118576033 2

Janet L. Norwood, *One Hundred Years of BLS*, Monthly Lab. Rev., at 3 (July 1985), https://www.bls.gov/opub/mlr/1985/07/art1full.pdf 6

Jason Koebler et al., *DOGE Employees Ordered to Stop Using Slack While Agency Transitions to a Records System Not Subject to FOIA*, 404 Media (Feb. 5, 2025), https://www.404media.co/doge-employees-ordered-to-stop-using-slack-while-agency-transitions-to-a-records-system-not-subject-to-foia/ 35

Katie Miller (@katierosemiller), X (Feb. 5, 2025, 5:26 PM), https://x.com/katierosemiller/status/1887311943062499425 35

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/ 6

Matt Egan, *Consumer watchdog ordered to stop fighting financial abuse and to work from home as HQ temporarily shuts down*, CNN (Feb. 9, 2025), https://www.cnn.com/2025/02/09/business/cfpb-vought-stop-activity/index.html 11

Minho Kim, *Trump's Declaration Allows Musk's Efficiency Team to Skirt Open Records Laws*, N.Y. Times (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/us/politics/trump-musk-doge-foia-public-records.html?smid=url-share 35

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 7

Musk's DOGE Reportedly Digging Into Medicare Payment System, PYMNTS (Feb. 5, 2025), https://www.pymnts.com/politics/2025/musks-doge-reportedly-digging-into-medicare-payment-system/. 8

NIST SP-800-53, *Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce: National Institute of Standards and Technology (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf 28

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) 6

Paresh Dave et al., *Elon Musk's DOGE is Working on a Custom Chatbot Called GSAi*, Wired ... 3

Privacy Impact Assessment – OFCCP – OFCCP Information Systems, U.S. Dep't of Labor, Off. Assistant Sec'y Admin. & Mgmt., https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy/ofccp/ofis (last accessed Feb. 11, 2025) 5

Privacy Impact Assessments, https://www.hhs.gov/pia/index.html [https://web.archive.org/web/20250123181425/https://www.hhs.gov/pia/index.html]. 9

Privacy Impact Assessments, U.S. Dep't of Labor, Office of the Assistance Sec'y for Admin. & Mgmt., https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy (last accessed Feb. 5, 2025) 4

See CMS, Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://security.cms.gov/learn/health-insurance-portability-and-accountability-act-1996-hipaa (accessed on Feb. 12, 2025) 27

Stacy Cowley et al., *With Attack on Consumer Bureau, Musk Removes Obstacle to His 'X Money' Vision*, N.Y. Times (Feb. 12, 2025), https://www.nytimes.com/2025/02/12/business/elon-musk-cfpb-x-money.html 13

U.S. Bureau of Lab. Stat., *About the U.S. Bureau of Labor Statistics*, https://www.bls.gov/bls/about-bls.htm (last accessed Feb. 5, 2025) 6

U.S. Digital Service, Report to Congress (2016), https://www.usds.gov/report-to-congress/2016/ 35

U.S. Gov't Accountability Off., GAO-16-602, Digital Service Programs (Aug. 15, 2016) 35

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 35

United States DOGE Service, OpenOMB (accessed on Feb. 6, 2025), https://openomb.org/file/11409329..... 35

Zach Montague and Dana Goldstein, *Musk Team Announces Millions in Cuts to Education Dept. Amid Legal Pushback*, N.Y. Times (Feb. 11, 2025), https://www.nytimes.com/2025/02/11/us/politics/musk-doge-education-data.html 2

INTRODUCTION

The federal government is the custodian of vast troves of information about nearly every American citizen. Many agencies may hold private identifying information, such as names, addresses, and social security numbers. Others hold personal, sensitive details such as individual Americans' wage histories or medical records. Law enforcement agencies hold tips, complaints, or records of interviews conducted to assist law enforcement, many of which are shared confidentially to shield reporting individuals from retaliation.

The government needs this information from the American people to effectively serve the public. But it has also long been sensitive to the need for confidentiality and public confidence that confidentiality will be safeguarded. The collection, storage, and conditions for disclosure of confidential personal information and other sensitive information by federal agencies is tightly regulated by a number of laws, evolved over decades, designed to provide Americans assurance that their data won't be disclosed or misused.

The new U.S. DOGE Service and U.S. DOGE Service Temporary Organization (collectively, "DOGE") has upended these assurances. DOGE is a new government entity that is led by Elon Musk, an unappointed, unelected, temporarily-serving official with multiple concurrent business concerns before federal regulators.

In the short weeks since the inauguration of the Trump Administration, DOGE has run roughshod over the protections of Americans' data. In agency after agency, a handful of DOGE staffers enter and claim (and are usually granted) near-absolute access to a wealth of sensitive information systems, without any apparent training in privacy or ethics protocols. These staffers then proceed to access these systems without limitation or scrutiny from experienced agency staff about appropriate and lawful access to sensitive databases.

The legal violations resulting from DOGE's seizure of agency information systems are myriad and flagrant. They threaten millions of Americans with imminent and direct harm, while also risking key government operations. For Plaintiffs, the impending harms are catastrophic: the potential disclosure of personal and sensitive financial and health information of millions of their members; the potential revelation of the identities of members who confidentially provided evidence of employer malfeasance; the loss of valuable tools to protect American workers and consumers, many of which rely on confidentiality to be effective.

Whether DOGE is malevolently stealing Americans' information for private gain, or simply lacks the patience and restraint to comply with the legal protections afforded to Americans' data, its activities in the sensitive systems of the Department of Labor (DOL), Department of Health and Human Services (HHS), and Consumer Financial Protection Bureau (CFPB) must be halted.

Factual Background

I. The Establishment of DOGE

On the day of his inauguration, President Trump created the "Department of Government Efficiency," a new entity in the White House Executive Office of the President. Exec. Order No. 14158, Establishing and Implementing the President's 'Department of Government Efficiency' (Jan. 20, 2025) (the "EO"). DOGE is technically two entities with an unclear division of labor between them: what was formerly known as the United States Digital Service (renamed the "U.S. DOGE Service"), plus a new temporary organization known as the "U.S. DOGE Service Temporary Organization." *See* EO § 1.

DOGE is headed, by Elon Musk, a businessman concurrently serving as an advisor to the President Trump.[1] While DOGE's nominal ambit involves "modernizing Federal technology and software to maximize governmental efficiency and productivity," EO § 1, in practice Mr. Musk has described it as "the wood chipper for bureaucracy. DOGE's activities since President Trump's inauguration suggest Mr. Musk's description is more accurate.

Since Inauguration Day, DOGE personnel have sought and obtained unprecedented access to information systems across more than a dozen federal agencies, including, in addition to those named as Defendants, the United States Agency for International Development (USAID), the Department of Treasury, the Office of Personnel Management (OPM), and the Department of Education.[2] DOGE personnel have also played critical roles in the ongoing dissolution of USAID and CFPB, the takeover of OPM and the General Services Administration, and have been involved in ongoing efforts to cripple the Department of Education.[3]

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

---

[1] *See, e.g.*, Aimee Picchi, *The White House says Elon Musk is a "special government employee." Here's what that means*, CBS News (Feb. 6, 2025), https://www.cbsnews.com/news/elon-musk-special-government-employee-what-does-that-mean/.

[2] *See* Ivan Pereira and Emily Chang, *Here are all the agencies that Elon Musk and DOGE have been trying to dismantle so far*, ABC News (Feb. 11, 2025), https://abcnews.go.com/Politics/elon-musks-government-dismantling-fight-stop/story?id=118576033; *see also Elon Musk's DOGE has swept into 15 federal agencies. Here's what to know*, Wash. Post (Feb. 8, 2025), https://www.washingtonpost.com/business/2025/02/08/elon-musk-doge-federal-agencies-cuts-employees/.

[3] *See id.*; *see also* Zach Montague and Dana Goldstein, *Musk Team Announces Millions in Cuts to Education Dept. Amid Legal Pushback*, N.Y. Times (Feb. 11, 2025), https://www.nytimes.com/2025/02/11/us/politics/musk-doge-education-data.html.

employees who resist their unlawful commands, and then beginning to re-work the agencies at their will. This process moves incredibly quickly, with agencies transformed roughly overnight; or fully dismantled within a week. Many DOGE staffers appear to be working across multiple agencies concurrently,[4] potentially collecting sensitive information from multiple databases across agencies and providing opportunities to combine and cross-reference data in ways that were never contemplated by the security plans for those systems. DOGE is reportedly working on building a "chatbot and other AI tools to analyze huge swaths of contract and procurement data" within the General Services Administration, and DOGE has "moved swiftly in recent weeks to bring aboard more AI tools" into the federal government.[5]

II. Threats to DOL, HHS, and CFPB

A. DOL establishes the DOL DOGE Access Policy and authorizes DOGE to access DOL systems.

On February 4, employees at DOL were given notice by agency leadership that the following day, DOGE staff would enter the Department and begin their work. Ex. F ¶ 9. DOL leaders articulated the policy that would govern DOGE's access to DOL systems: DOL employees were instructed to do whatever DOGE asked, not push back, not ask questions, provide access to any DOL system DOGE requested access to, and not worry about any security

[4] Faiz Siddiqui et al., *19-year-old Musk surrogate takes on roles at State Department and DHS*, Wash. Post (Feb. 10, 2025), https://www.washingtonpost.com/business/2025/02/10/musk-doge-state-department-surrogate/.

[5] Paresh Dave et al., *Elon Musk's DOGE is Working on a Custom Chatbot Called GSAi*, Wired (Feb. 6, 2025), https://www.wired.com/story/doge-chatbot-ai-first-agenda/.

protocols in doing so. *Id.* This approach, the "DOL DOGE Access Policy," was understood by employees to carry a threat of termination for noncompliance. *See id.* [6]

The DOL DOGE Access Policy grants access to dozens of data sources containing private and sensitive information at the agency. DOL lists over 50 different systems containing personally identifiable information across its functions.[7] Unlawful changes to these systems' (and others') access or control could have substantial negative effects, for individual privacy as well as for agency effectiveness.

For example, DOL administers a number of databases that contain sensitive personal information about individuals within its systems, such as:

Federal Employees' Compensation Act (FECA): DOL administers workers compensations programs, and in the process collects and maintains records related to workers' injuries,[8] such as medical records and bills, compensation payment records, consumer credit reports and personal financial information such as financial statements, assets, liabilities, income, and expenses.[9] Given the sensitive nature of these records, regulations require they be "considered confidential and may not be released, inspected, copied or otherwise disclosed,"

---

[6] In their response to Plaintiffs' Motion for a Temporary Restraining Order, Defendants did not dispute the existence of this policy. *See* Defs.' TRO Resp., ECF No. 16; *see also* Declaration of Adam Ramada ("Ramada Decl."), ECF No. 16-1.

[7] *Privacy Impact Assessments*, U.S. Dep't of Labor, Office of the Assistance Sec'y for Admin. & Mgmt., 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).

[8] 20 C.F.R. § 10.10 (2025); *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).

[9] *Id.*

except under certain proscribed circumstances, and only if such release is consistent with the purpose for which the record was created.[10]

Employee Benefits Security Administration (EBSA): This DOL subcomponent regulates employee benefit plans, and in conducting enforcement activities, collects sensitive data on every single participant in a plan, such as social security numbers, pay status, and accrued benefits, or health information including claims and appeals for union members and their immediate families.[11]

In addition to personal sensitive information, DOL undertakes a number of enforcement activities against employers for violations of things like wage & hour requirements, workplace safety laws, and antidiscrimination laws.[12] In each of these regimes, the ability of DOL to collect confidential information from workers to report wrongdoing is critical to their ability to undertake enforcement, so that workers can provide DOL honest information without fear of retaliation from their employers. *See, e.g.*, Ex. A ¶¶ 8-9; Ex. B ¶¶ 6-9; Ex. C. ¶¶ 6-7; Ex. D. ¶¶ 6-7; Ex. J ¶¶ 6-8; Ex. K ¶¶ 6-8; Ex. L ¶¶ 8-13, 16, 19-20; Ex. N ¶ 8; Ex. O ¶ 8; Ex. U ¶¶ 10, 13, 14-15; Ex. V ¶¶ 4-7.

---

[10] 20 C.F.R. § 10.10 (2025).

[11] Enforcement, U.S. Dep't of Labor, Emp. Benefits Sec. Admin.,https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/enforcement (last accessed Feb. 10, 2025); *see also* Ex. E ¶¶ 7-9.

[12] *See* Frequently Asked Questions: Complaints and the Investigation Process, U.S. Dep't of Labor, Wage and Hour Division, https://www.dol.gov/agencies/whd/faq/workers (last accessed Feb. 5, 2025); About OSHA, U.S. Dep't of Labor, OSHA, https://www.osha.gov/aboutosha (last accessed Feb 12, 2025); Privacy Impact Assessment – OFCCP – OFCCP Information Systems, U.S. Dep't of Labor, Off. Assistant Sec'y Admin. & Mgmt., https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy/ofccp/ofis (last accessed Feb. 11, 2025).

Notably, Mr. Musk's companies have also frequently 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.[13] Under normal circumstances, non-public information regarding those investigations would not be available to Mr. Musk. *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) (FOIA exemption for records or information compiled for law enforcement purposes).

The Bureau of Labor Statistics (BLS): BLS also houses sensitive information at DOL. It was founded in 1884 to collect and publish disinterested information about labor markets that "could promote effective, rational, and equitable decisionmaking."[14] 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."[15]

---

[13] *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).

[14] Janet L. Norwood, *One Hundred Years of BLS*, Monthly Lab. Rev., at 3 (July 1985), https://www.bls.gov/opub/mlr/1985/07/art1full.pdf.

[15] U.S. Bureau of Lab. Stat., *About the U.S. Bureau of Labor Statistics*, https://www.bls.gov/bls/about-bls.htm (last accessed Feb. 5, 2025).

BLS's independence and autonomy is core to its status as a flagship data source among federal agencies.[16] Congress has specifically protected statistical agencies from undue interference 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 requires statistical agencies to pledge confidentiality when collecting individual data and restricts disclosure for any purpose besides statistical reporting. 44 U.S.C. §§ 3572(a)(2), (c).

But BLS's independence is politically tenuous, and the agency's data is always at risk of a presidential administration deciding to alter its data or prevent its publication to shape economic news.[17] This risk is notable under a President who has previously attacked the BLS's credibility when its reporting was politically inconvenient, accusing the agency of "fraudulently manipulating job statistics,"[18] and calling their data "phoney."[19]

B. HHS establishes the HHS DOGE Access Policy.

On February 5, reports began to emerge that DOGE employees were seeking access to HHS systems, including the Healthcare Integrated General Ledger Accounting System

---

[16] 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. Pol'y 1, 4 (2023).

[17] *See, e.g.*, Julia Press & Saleha Mohsin, W*hy Key U.S. Economic Data is under Threat*, BNN Bloomberg (Dec. 12, 2024), https://www.bnnbloomberg.ca/business/company-news/2024/12/12/why-key-us-economic-data-is-under-threat/.

[18] 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.

[19] 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.

(HIGLAS), which is a key Centers for Medicare and Medicaid Services' (CMS) "payment and contracting systems,"[20] which was implemented to "strengthen[] the management of Medicare accounts receivables and allow[] CMS to collect outstanding debts more timely."[21] Mr. Musk confirmed that DOGE was seeking access to CMS payment systems in a social media post alleging that HHS, specifically CMS, "is where the big money fraud is happening."[22] DOGE has also sought access to personnel records at the Centers for Disease Control (CDC) and the National Institutes of Health (NIH), where DOGE was able to identify for cancellation more than 60 government contracts.[23]

Shortly after the DOGE team's presence at HHS became public, HHS issued a statement

---

[20] *See, e.g.*, Anna Wilde Matthews and Liz Essley Whyte, *DOGE Aides Search Medicare Agency Payment Systems for Fraud*, The Wall Street Journal (Feb. 5, 2025), https://www.wsj.com/politics/elon-musk-doge-medicare-medicaid-fraud-e697b162; Dan Diamond et al., *DOGE broadens sweep of federal agencies, gains access to health payment systems*, The Washington Post (Feb. 5, 2025), https://www.washingtonpost.com/health/2025/02/05/doge-health-agencies-labor/; *Musk's DOGE Reportedly Digging Into Medicare Payment System*, PYMNTS (Feb. 5, 2025), https://www.pymnts.com/politics/2025/musks-doge-reportedly-digging-into-medicare-payment-system/.

[21] CMS, FAQ: What is HIGLAS, https://www.cms.gov/research-statistics-data-and-systems/computer-data-and-systems/higlas/downloads/faq.pdf#:~:text=HIGLAS%20strengthens%20the%20management%20of,collect%20outstanding%20debts%20more%20timely (accessed on Feb. 9, 2025).

[22] Elon Musk (@elonmusk), X (Feb. 5, 2025 12:01 PM ET), https://x.com/elonmusk/status/1887184902543577590. Mr. Musk later doubled down on his outlandish claim, asserting—again, by posting on his social media company—that he was "100% certain that the magnitude of the fraud in federal entitlements (Social Security, Medicare, Medicaid, Welfare, Disability, etc) exceeds the combined sum of every private scam you've ever heard by FAR." Elon Musk (@elonmusk), X (Feb. 11, 2025, 1:23 AM), https://x.com/elonmusk/status/1889198569518719122.

[23] *See* Diamond et al., *supra* note 20 (reporting that DOGE requested "lists of employees who have less than a year of service and those who are in two-year probationary period"); *see* also Dep't of Gov. Efficiency (@DOGE), X (Feb. 7, 2025, 4:10 PM EST), https://x.com/DOGE/status/1887972340446683576.

that not only confirmed that DOGE had been granted "appropriate access to CMS systems and technology" but also announced that authorizing such access was part of a "collaboration with DOGE" (the "HHS DOGE Access Policy").[24]

The HHS DOGE Access Policy is gravely concerning because HHS and its various components hold a great deal of personally identifiable information, as well as personal health information, much of which is subject to the Privacy Act, 5 U.S.C. § 552a. HHS has seemingly removed its Privacy Impact Assessment database but, according to an archived snapshot, HHS maintains over 400 systems containing protected personal information across its many subcomponents.[25] Some sensitive records at HHS components also include personal health information, which is further subject to protection under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, 110 Stat. 1936; *see also* 45 C.F.R. § 160.103 (prohibiting disclosure, except in certain situations not relevant here, of "individually identifiable health information").

As relevant here, CMS maintains systems of records containing personal and health information about beneficiaries of Medicaid and Medicare, including their "[n]ame, address, phone number, email, address, and SSN or other identifying number." *See* 84 Fed. Reg. 2230,

[24] Ctr. for Medicare & Medicaid Servs., *CMS Statement on Collaboration with DOGE*, (Feb. 5, 2025), https://www.cms.gov/newsroom/press-releases/cms-statement-collaboration-doge.

[25] *Privacy Impact Assessments*, https://www.hhs.gov/pia/index.html [https://web.archive.org/web/20250123181425/https://www.hhs.gov/pia/index.html].

2231-32 (Feb. 16, 2019) (SORN 09-70-0541) (containing a "comprehensive database" of "enrollment, eligibility, and paid claims data about Medicaid recipients").[26]

In addition to information about Medicare and Medicaid beneficiaries and the people who provide their healthcare, HHS also maintains systems of records containing a great deal of information abouts its own employees and their families, such as

> name, email and telephone contact information, Social Security Number, date of birth, work and home addresses, pay plan and grade, dates and hours worked, dates, hours or amounts of leave accrued, used, awarded or donated, travel benefits and allowances and educational allowances (including educational allowances for dependents of commissioned corps personnel), certifications and licenses affecting pay, personnel orders, special positions (*e.g.*, hazardous duty) affecting pay, bank account information, and amounts withheld and allotted for income tax, insurance, retirement, Thrift Saving Plan, flexible spending account, voluntary leave transfers, charitable contributions, garnishments, and other purposes.
>
> 80 Fed. Reg. 48538, 48540 (Aug. 13, 2015) (SORN 09-90-1402).[27]

---

[26] *See also, e.g.*, 73 Fed. Reg. 11643, 11644 (March 4, 2008) (SORN 09-70-0512) (containing "samples of the United States population served by programs administered by CMS and [the Social Security Administration ("SSA")]"); CMS, Medicaid Integrity Program Systems (Dec. 28, 2017), https://www.hhs.gov/foia/privacy/sorns/09700599/index.html (SORN 09-70-0599) (containing "information on Medicaid beneficiaries, and physicians and other providers involved in furnishing services to Medicaid beneficiaries"); 65 Fed. Reg. 48000, 48000-03 (Aug. 4, 2000) (SORN 09-70-0513) (containing "Medicare hospital insurance benefits records, Part B benefits records, home health benefits records, and Medicare hospital benefits records"); HHS, SORN 09-70-0514 (Dec. 21, 2017), https://www.hhs.gov/foia/privacy/sorns/09700514/index.html (containing summaries "of all services rendered to a Medicare beneficiary, from the time of admission through discharge, for a stay in an inpatient hospital and/or Skilled Nursing Facilities'); HHS, SORN 09-70-0525 (Feb. 7, 2019), https://www.hhs.gov/foia/privacy/sorns/09700525/index.html (containing the "tax identification, and social security number (SSN) for each physician, non-physician practitioner and medical group" that seeks reimbursement from Medicare).

[27] *See also, e.g.*, 86 Fed. Reg. 68262, 68263-64 (Dec. 1, 2021) (SORN 09-90-2103) (containing information related to requests for accommodations in the workplace, such as a note from a treating physician or, if the request is for a religious accommodation, "records describing the individual's religious beliefs, practices, or observances"); 67 Fed. Reg. 4965, 4965 (Feb. 1,

The access that the HHS DOGE Access Policy authorizes to these and other systems of records will have substantial negative effects on the privacy interests of Plaintiffs and their members, as well as for agency effectiveness.

C. CFPB establishes the CFPB DOGE Access Policy.

On Friday, February 7, DOGE staff arrived at the CFPB, and "gained access to internal computer systems that manage the agency's human resources, procurement, and finance systems."[28] Acting Director Vought reportedly emailed agency staff a message the same day stating that DOGE personnel were authorized to "begin work on all unclassified CFPB systems."[29] This policy, the "DOGE CFPB Access Policy," grants DOGE staff essentially unfettered access to CFPB systems. It was coupled with additional order that CFPB staff were to essentially halt all substantive work, and stay out of CFPB headquarters for the entire week,[30] likely leaving DOGE staff unsupervised and unsupported by CFPB staff with existing access to and knowledge of the agency's systems.

2002) (SORN 09-90-0010) (containing "the records of all HHS employees and their family members" who have used an Employee Assistance Program).

[28] Bobby Allen et al., *Musk's team takes control of key systems at Consumer Financial Protection Bureau*, NPR (Feb. 7, 2025), https://www.npr.org/2025/02/07/g-s1-47322/musks-team-takes-control-of-key-systems-at-consumer-financial-protection-bureau.

[29] Holly Otterbein and Megan Messerly, *Vought takes helm at CFPB after Musk incursion,* POLITICO (Feb. 8, 2025), https://www.politico.com/news/2025/02/08/vought-takes-helm-at-cfpb-after-musk-incursion-00203247.

[30] Matt Egan, *Consumer watchdog ordered to stop fighting financial abuse and to work from home as HQ temporarily shuts down,* CNN (Feb. 9, 2025), https://www.cnn.com/2025/02/09/business/cfpb-vought-stop-activity/index.html.

CFPB houses many sensitive data sources and processes. The agency lists over 40 different systems containing personally identifiable information across its functions.[31] Unlawful changes to these systems' (and others') access or control could have substantial negative effects, for individual privacy as well as for agency effectiveness.[82]

For example, the CFPB collects, stores, and analyzes complaints submitted by consumers about problems they have encountered with consumer financial products and services such as mortgage, credit cards, and debt collection. These complaints frequently contain personally identifying information and sensitive financial information about individual consumers such as Social Security numbers and account and routing numbers. Consumers submit complaints with the expectation they will be protected from disclosure. The CFPB has received over 10 million consumer complaints. CFPB, *CFPB Hits 10 Million Complaints Milestone*, YouTube.com (Jan. 22, 2025), https://www.youtube.com/watch?v=ALcMFm7zaGg. These complaints are stored as part of a broader case-management system called the Consumer Response System. CFPB, *Privacy Impact Assessment, Consumer Response System* (Aug. 2024), https://files.consumerfinance.gov/f/documents/cfpb_consumer-response-system-pia-v2_2024-08.pdf.

The CFPB also collects and stores a wide variety of sensitive and valuable information in carrying out its other statutory responsibilities, include supervising certain categories of financial institutions via on-site examinations and investigating and prosecuting violations of the laws the agency administers. 12 U.S.C. §§ 5514-15, 5562-64. That information includes personally

[31] Consumer Financial Protection Bureau, *Privacy Impact Assessments (PIAs)*, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

identifiable information about individual consumers, trade secrets and other proprietary business information, exchanges between the Bureau and supervised entities that would be protected under the bank-examiner privilege, information submitted by and that would reveal the identity of whistleblowers, and information that would otherwise protected from disclosure under the Bureau's regulations as "confidential investigative information" and "confidential supervisory information." *See* 12 C.F.R. §§ 1070.2, 1070.4. This competitively sensitive information has direct relevance for Mr. Musk's business interests.[32] It is stored in several systems of records notices, including the CFPB's Depository Institution Supervision Database, Enforcement Database, and Civil Penalty Fund and Bureau-Administered Redress Program Records. CFPB, *Privacy Impact Assessment, Supervision, Enforcement, and Fair Lending Data* at 3 (Jan. 26, 2016), https://files.consumerfinance.gov/f/2016_cfpb_privacy-impact-assessment-supervision-enforcement-and-fair-lending-data.pdf.

Similarly, the Bureau collects and makes available "the most comprehensive source of publicly available information on the U.S. mortgage market." CFPB, *Mortgage Data (HMDA)*, https://www.consumerfinance.gov/data-research/hmda/. These data help show whether lenders are serving the housing needs of their communities; they give public officials information that helps them make decisions and policies; and they shed light on lending patterns that could be discriminatory. *Id.* The public data are modified to protect applicant and borrower privacy, such as by excluding property address and applicant's credit score. *See Disclosure of Loan-Level HMDA Data*, 84 Fed. Reg. 649, 664-65 (Jan. 31, 2019).

---

[32] *See, e.g.*, Stacy Cowley et al., *With Attack on Consumer Bureau, Musk Removes Obstacle to His 'X Money' Vision*, N.Y. Times (Feb. 12, 2025), https://www.nytimes.com/2025/02/12/business/elon-musk-cfpb-x-money.html.

Statutory and Legal Framework

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.

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.* § 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).[33]

II. 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).

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*, 599 F. Supp. 2d 1, 3 n.2 (D.D.C. 2009) ("[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

[33] 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.

public interest—merge." *D.A.M. v. Barr*, 474 F. Supp. 3d 45, 67 (D.D.C. 2020) (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"); *Nat'l R.R Passenger Corp. (Amtrak) v. Sublease Interest Obtained Pursuant to an Assignment & Assumption of Leasehold Interest Made as of Jan. 25, 2007*, 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.

A. Plaintiffs have standing.

As a threshold matter, Plaintiffs have standing. *Barton v. District of Columbia*, 131 F. Supp. 2d 236, 243 n.6 (D.D.C. 2001) ("The first component of the likelihood of success on the merits prong usually examines whether the plaintiffs have standing."). Organizations, like Plaintiffs, can establish standing by showing either associational or organizational injury.

To demonstrate associational standing, a plaintiff must show that "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Metro. Wash. Chapter, Associated Builders & Contractors, Inc. v. D.C.*, 62 F.4th 567, 572 (D.C. Cir. 2023) (quoting *Hunt v. Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977)). When an organization seeks prospective

relief on behalf of its members, "actual participation by individual members is generally not required." *Am. Ass'n of Cosmetology Schools v. Devos*, 258 F. Supp. 50, 67 (D.D.C. 2017) (quoting *Warth v. Seldin*, 422 U.S. 490 (1975)).

To establish organizational standing, a plaintiff must show (1) that "the agency's action or omission to act injured" or will injure "the organization's interest and" (2) "whether the organization used" or will use "its resources to counteract that harm." *PETA v. Dep't of Ag.*, 797 F.3d 1087, 1094 (D.C. Cir. 2015). Where "new obstacles unquestionably make it more difficult for [organizational plaintiffs] to accomplish their primary mission . . . , they provide injury for purposes of both standing and irreparable harm." *See League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 9 (D.C. Cir. 2016); *see also Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 395 (2024) (standing established if a defendant "directly affected and interfered with [the plaintiff's] core business activities").

1. Plaintiffs AFL, AFGE, CWA, and SEIU have demonstrated standing to challenge the unlawful disclosure of Department of Labor data.

Plaintiffs AFL, AFGE, CWA, and SIEU have associational and organizational standing to challenge the unlawful disclosure of Department of Labor data.

They have associational standing because, first and foremost, each union's members have suffered or will suffer significant, irreparable harms from Defendants' illegal access to and disclosure of their data, giving those members standing in their own right. Ex. A ¶ 19; Ex. C. ¶ 5; Ex. D. ¶ 5; Ex. E ¶¶ 7-9; Ex. F ¶¶ 7, 13-15; Ex. G ¶ 7; Ex. H ¶ 7; Ex. I ¶ 7; Ex. L ¶¶ 8, 20; Ex. N ¶ 6; Ex. O ¶ 6; Ex. U ¶¶ 9, 12, 14, 16; Ex. V ¶ 4 (individual members whose sensitive personal and/or financial data is held in Defendant DOL's systems); Ex. A ¶¶ 8-9; Ex. B ¶¶ 6-9; Ex. C. ¶¶ 6-7; Ex. D. ¶¶ 6-7; Ex. J ¶¶ 6-8; Ex. K ¶¶ 6-8; Ex. L ¶¶ 8-13, 16, 19-20; Ex. N ¶ 8; Ex. O ¶ 8; Ex. U ¶¶ 10, 13, 14-15; Ex. V ¶¶ 4-7 (individual members whose identity should remain confidential

in connection with enforcement matters); *see also Venetian Casino Resort, L.L.C. v. EEOC*, 409 F.3d 359, 367 (D.C. Cir. 2005) (finding that an employer had standing to challenge an EEOC policy that threatened to expose confidential information). The harms are germane to these unions' missions of supporting workers in matters before the Department of Labor, Ex. A ¶ 2; Ex. F ¶ 3, Ex. L ¶ 2; Ex. U ¶ 2—matters requiring the confidentiality that the Department has promised them. And while individual members are not necessary to litigate these harms, because the harms are universal to all members whose information will be compromised, *see* Ex. A ¶¶ 8, 9, 19; Ex. F ¶ ¶ 13-15; Ex. L ¶¶ 8-13, 16, 19-20; Ex. U ¶¶ 9-10, 12-16, each union has submitted one or more declarations identifying particular members who are substantially likely to suffer these harms, and listing these harms in detail, *see, e.g.*, Ex. B ¶¶ 6-9; Ex. C. ¶¶ 5-7; Ex. D. ¶¶ 6-7; Ex. E ¶¶ 7-9; Ex. G ¶ 7; Ex. H ¶ 7; Ex. I ¶ 7; Ex. J ¶¶ 6-8; Ex. K ¶¶ 6-8; Ex. N ¶¶ 6, 8; Ex. O ¶¶ 6, 8; Ex. V ¶¶ 4-7.

These union plaintiffs also have demonstrated organizational standing. They have alleged significant and imminent harms to their daily activities that would result from the data breaches. Specifically, their core activities of obtaining relief for labor violations on behalf of their union members will be made substantially more difficult because members will be less inclined to come forward about workplace abuses knowing that their information may not be kept private. *See, e.g.*, Ex. F. ¶ 17, Ex. L ¶¶ 10-11, 15-17; Ex. U ¶¶ 10, 13. 15-16. *See Food & Drug Admin.*, 602 U.S. at 395 (2024) (impact on core activities); Moreover, the exposure of private information about their clients or members will require staff to divert precious time and resources to countering that exposure and counseling members on how to respond when they could and should be engaged in their core purpose of protecting workers' rights. *See, e.g.*, Ex. F ¶ 19; Ex. L ¶¶ 17-19; Ex. U ¶ 17*; Conservative Baptist Ass'n of Am., Inc. v. Shinseki*, 42 F. Supp.

3d 125, 132 (D.D.C. 2014) (noting diversion of resources away from "core activities" is a cognizable injury (internal quotation marks and citations omitted)); *Nat'l Treasury Emps. Union v. United States*, 101 F.3d 1423, 1429 (D.C. Cir. 1996) (noting organizations have standing where challenged actions are "at loggerheads with the stated mission of the plaintiff" (internal quotation marks and citations omitted)). The data breaches would also decrease membership (and therefore membership dues), resulting in economic injury. *See, e.g.*, Ex. F ¶ 17; Ex. U ¶ 17; *see Action All. of Senior Citizens of Greater Philadelphia v. Heckler*, 789 F.2d 931, 938 (D.C. Cir. 1986) (finding standing where organization "alleged inhibition of their daily operation"). These injuries are not "self-inflicted." *Shinseki*, 42 F. Supp. 3d at 132 (D.D.C. 2014) (citations omitted).

The unions are likewise injured in much the same way as their members: They face an imminent threat of the disclosure of their own sensitive data and information, which they are routinely required to submit to OLMS pursuant to the Labor Management Reporting and Disclosure Act, 42 U.S.C. § 401 *et seq.* Through these submissions, Unions pass along highly confidential information to OLMS in the form of financial records, information about union officers, and information about union organizing efforts (including membership lists and data concerning participation in officer elections). Ex. A ¶¶ 12-15; Ex. U ¶ 18. The disclosure of this information to Defendants would be "highly damaging" to unions, Ex. A. ¶ 15, potentially revealing information crucial to the Unions' strategies and impairing their abilities to pursue their missions. *PETA*, 797 F.3d at 1094-96 (D.C. Cir. 2015) (finding an organization had standing where government action inhibited "one of the primary ways" it accomplished its mission (internal quotation marks and citations omitted)); *Capital Area Immigrants' Rights Coalition ("CAIR") v. Trump*, 471 F. Supp. 3d 25, 38 (D.D.C. 2020) (finding organizations had

shown standing because defendants' actions would have frustrated plaintiffs' ability to provide legal services, "a core component" of plaintiffs' mission).

2. Plaintiffs CWA, AFSCME, and SEIU have demonstrated standing to challenge the unlawful disclosure of HHS data.

Plaintiffs CWA, AFSCME, and SEIU each have associational and organizational standing to challenge the unlawful disclosure of HHS data. They have associational standing because each union's members have suffered or will suffer significant, irreparable harms from Defendants' illegal access to and disclosure of their data, including sensitive personal health data, giving those members standing in their own right. The harms are germane to these unions' missions of providing healthcare to their members and the public at large, which would become virtually impossible if patients no longer trusted them and HHS with their data. *See* Ex. M ¶¶ 7-9; Ex. U ¶¶ 20-21; Ex. Z ¶¶ 5-14. Individual members are not necessary to litigate these harms, because the harms are universal to all members' whose information will be compromised, but each union has submitted one or more declarations identifying particular members who are substantially likely to suffer these harms, and listing these harms in detail. *See* Ex. P ¶¶ 5-7; Ex. Q ¶¶ 4-7; Ex. R ¶¶ 4-7; Ex. S ¶¶ 4-8; Ex. T ¶¶ 5-8; Ex. W ¶¶ 9-10; Ex. Z ¶¶ 10-14; Ex. AA ¶¶ 8-13.

SEIU also has organizational standing with respect to the HHS breaches. It has alleged significant and imminent harms to its daily activities that would result from the unlawful activity, including the inability to secure healthcare for individual members and advocate for healthcare reform on behalf of all of them. *See* Ex. M ¶¶ 8-9 (confidentiality crucial to SEIU's efforts to secure healthcare for members). Advocacy for access to healthcare, including protecting and expanding access to Medicare and Medicaid is core to SEIU's mission, purpose, and daily activities. *Id.* ¶¶ 4-7. By compromising the quality of service provided by Medicare and

Medicaid, the DOGE HHS Access Policy will decrease the value of SEIU's extensive work to expand and protect these services. *See PETA*, 797 F.3d at 1095; *CAIR*, 471 F. Supp. 3d at 38.

3. Plaintiffs EAMF and VPLC have demonstrated standing to challenge the unlawful disclosure of CFPB data.

Finally, Plaintiffs EAMF and VPLC have shown organizational standing to challenge data breaches at the CFPB. First, each has alleged significant harms to their daily activities. VPLC and EAMF are non-profit legal services organizations that exist to serve low-income clients in consumer protection matters; they rely on CFPB data and often refer clients to CFPB's confidential consumer complaint service. Ex. X ¶¶ 2-4, 9-14; Ex. Y ¶¶ 2-5, 7. Confidentiality of the database is critical to these organizations' work with the customers they serve, *see, e.g.*, Ex. X ¶¶ 17-19 ("I could not in good conscience tell people to send their private financial and personal information to a system that others could then use to exploit them"). Without being able to rely on the confidentiality of CFPB data, these organizations will have to spend significant additional time and resources on less efficient ways of processing consumer complaints and reporting financial fraud, diverting resources from other core activities. *See* Ex. X at ¶¶ 16, 17, 22 ("To replicate what the complaint tool does . . . would be difficult if not impossible and would strain our already limited resources"); Ex. Y at ¶ 8 (Without an effective complaint tool, "our counselors . . .. would need to devote more time and resources to get the same result. It's a lot harder fighting with a bank of debt collector when you're just an individual consumer. It's easier when the company is receiving your complaint from a government agency."); *see also PETA*, 797 F.3d at 1095; *CAIR*, 471 F. Supp. 3d at 38.

B. Plaintiffs are likely to succeed on their APA claims.

1. Defendants' sharing of data and information systems with DOGE constitutes final agency action.

Defendants' DOGE Access Policies, which, whether on their own accord or at the direction of DOGE, grant DOGE employees access to information systems, including 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)). Defendants' 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 Defendants' 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, which the government did not dispute as to the Department of Labor a factual matter at the earlier hearing in this case, is not informal; rather, it is a decision of agency policy and practice. Analysis of the second prong is equally clear: Defendants' decisions have determined their obligations to disclose data and information within their control, affected the rights of the entities about whom they retain data, and created significant legal consequences as a result of Defendants' violation of numerous laws.

And should the Court conclude that Defendants' decisions to disclose their 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.

2. Defendants' DOGE Access Policies Are Contrary to Law.

Each of Defendant's DOGE Access Policies are contrary to law. They each violate a variety of laws, including the Privacy Act and various agency-specific regulations.

a) Defendants' Policies Violate the Privacy Act.[34]

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,

[34] Defendants' violations of the Privacy Act are final agency actions contrary to law under the APA, as detailed in this section. But they also violate the Privacy Act directly. When an agency "fails to comply with" 5 U.S.C. § 552a(b) "in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction." 5 U.S.C. § 552a(g)(1)(D). In addition to the violations of the APA discussed in this section, the Privacy Act provides an alternative, direct form of relief for Plaintiffs' claims.

"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). "[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.

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.* § 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." *Id.* § 552a(b).

Agency Defendants' systems collectively house hundreds of systems of records subject to the Privacy Act, many of which contain personally identifiable information.[35] Because DOGE is an entity within the White House rather than within any of the Agency Defendants, any disclosure of records containing PII by the Department to DOGE would fall under the prohibition in § 552a(b). While § 552a(b) contains thirteen exceptions, none of them apply here.[36]

b) DOL's Policy Is Contrary to Additional Statutes and Regulations.

In addition to violating the Privacy Act, DOL's DOGE Access Policy also flouts its own agency-specific rules and regulations in numerous respects.

First, it includes an instruction by DOL to its employees that is contrary to 5 U.S.C. § 2302(b)(9)(D), which prohibits threatening a federal employee with termination for "refusing to obey an order that would require the [employee] to violate a law."

Second, it is contrary to the Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551-58, which requires agencies to provide information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized

---

[35] *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); *Privacy Impact Assessments*, U.S. Dep't of Health & Hum. Servs., https://www.hhs.gov/pia/index.html [https://web.archive.org/web/20250123181425/https://www.hhs.gov/pia/index.html] (HHS maintains over 400 systems containing PII across the agency and its subcomponents); *Privacy Impact Assessments*, CFPB, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/ (over 40 tools and systems with privacy impact assessments).

[36] During the Feb. 7, 2025 hearing in this case, Defendants posited that the DOGE DOL Access Policy might be permitted under the "routine use" exception. 5 U.S.C. § 552a(b)(3). But a routine use must be both "compatible with the purpose for which [a record] was collected," *id.* § 552a(a)(7), and previously published in the Federal Register with opportunity for comment as part of each system of records notice. *Id.* § 552a(e)(4)(D). The broad, sudden, nature of the DOGE Access Policies cannot meet the requirements of the routine use exception.

access [or] use" of information or information systems maintained by the agency. 44 U.S.C. § 3554(a)(1)(A). The breadth of the DOL DOGE Access Policy authorizes access without the careful, tailored approach required by FISMA.

Third, it is contrary to established DOL confidentiality requirements for various sets of sensitive data, both agency-wide, *see* 29 C.F.R. § 71 (implementing regulations for the Privacy Act), and program by program. *See, e.g.* 20 C.F.R. 10.10 (regulations treating all "records relating to claims for benefits" under FECA as "confidential" and not permitted to be "released, inspected, copied, or otherwise disclosed" except in accordance with the Freedom of Information Act (FOIA) and the Privacy Act). DOL is required to "inform its employees of the provisions of the Privacy Act, including the Act's civil liability and criminal penalty provisions," and instruct employees of their duty to, among other things "[p]rotect the security of records," "[e]nsure the accuracy . . . of records," and "[a]void the unauthorized disclosure . . . of records." 29 C.F.R. § 71.13(a). It also requires that, unless authorized by the Privacy Act, DOL employees "[d]isclose no record to anyone, for any use, unless authorized by the Act." *Id.* § 71.13(b)(8).

The blanket nature of the DOL DOGE Access Policy cannot comply with the requirements of DOL's own regulations imposing tailored, system-by-system requirements and importing the structure and policies of the Privacy Act.

Fourth, it grants DOGE personnel access to BLS data, in violation of the applicable confidentiality protections set forth in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CISPEA), 44 U.S.C. § 3572(c)(1) (prohibiting disclosure of information of information collected under a pledge of confidentiality for exclusively statistical purposes).

c) HHS' Policy Is Contrary to Additional Statutes and Regulations.

The HHS DOGE Access Policy is also contrary to the Privacy Act and FISMA, which, as explained above, 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). It is additionally contrary to HHS regulations implementing the Privacy Act, which "establish[] agency policies and procedures for the maintenance of records" and the disclosure of personal or health information, 45 C.F.R. §§ 5b.2(a), 5b.9, and HIPAA, which imposes "standards, requirements, and implementation specifications" for "covered entities with respect to protected health information," *id.* § 164.500. As a "covered entity" under HIPAA,[37] HHS' regulations require CMS to, among other things, "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information" in its possession. 45 C.F.R. § 164.306(a).

The HHS DOGE Access Policy grants broad access to sensitive information, including health information provided to CMS by beneficiaries of Medicare and Medicaid, in a manner that is contrary to the aforementioned laws and regulations.

d) CFPB's Policy Is Contrary to Additional Statutes and Regulations.

Like the policies of HHS and the Department of Labor, the CFPB DOGE Access Policy is inconsistent with FISMA. 44 U.S.C. § 3554(a)(1)(A). FISMA requires agencies to develop

---

[37] *See* CMS, Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://security.cms.gov/learn/health-insurance-portability-and-accountability-act-1996-hipaa (accessed on Feb. 12, 2025); *see also* CMS, CMS Breach Response Handbook (Nov. 7, 2022), https://security.cms.gov/policy-guidance/cms-breach-response-handbook ("CMS's administration of Medicare and Medicaid make the agency a covered entity under HIPAA and subject to the law's reporting and notification requirements when PHI is breached.").

security systems and protocols to protect sensitive or confidential information in compliance with regulations and standards developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce. 44 U.S.C. § 3553(h)(2)(F), 40 U.S.C. § 11331(a). The National Institute of Standards and Technology (NIST) promulgates those standards, which, among other things, require agencies to "[p]hyiscally control[] and securely store[]" both "digital and/or non-digital media" and "protect[] information system media until the media are destroyed." NIST SP-800-53, *Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce: National Institute of Standards and Technology (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Agencies must also "enforce[] physical access authorizations" including by "control[ling] visitor activity." *Id*. These controls are an integral part of FISMA's requirement that security protocols be "commensurate" with "the risk and magnitude of the harm resulting from unauthorized use, disclosure, disruption, modification, or destruction" of information. 44 U.S.C. § 3554(a)(1)(A). The CFPB's decision to grant DOGE access to all of its information systems is contrary to these requirements.

Moreover, it conflicts with CFPB restrictions on disclosure of sensitive data, set forth via policy and regulation. *See, e.g.*, 12 C.F.R. § 1070.59 (prohibiting unauthorized disclosures of personal information except in accordance with the requirements of 5 U.S.C. § 552a(b)); *Id.*§ 1070.40 *et seq.* (governing disclosure of confidential information); *Id.*§ 1070.4 ("employees . . . or others in possession of a record of the CFPB that the CFPB has not already made public, are prohibited from disclosing such records, without authorization, to any person who is not an employee of the CFPB.").

3. Defendants' DOGE Access Policies Are Arbitrary and Capricious.

Defendants' DOGE Access Policies are also arbitrary and capricious. Under arbitrary-and-capricious review, "the agency 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. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (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).

Here, Defendants decided to hand over vast amounts of data, including personal identifying information about millions of American citizens. Yet they have made no attempt to articulate their reasoning. Nor have they acknowledged the catastrophic consequences—be that retaliation, chilling, indignity, or financial harm—that will surely follow from the immediate exposure of personal identifying information contained in these far reaching information systems: to understate it, "an important aspect of the problem," *Id.* at 43; *see also Dickson v. Sec'y of Def.*, 68 F.3d 1396, 1404 (D.C. Cir. 1995) (explaining that "[t]he requirement that agency action not be arbitrary and capricious includes a requirement that the agency adequately explain its result" and holding invalid agency action where agency "failed to provide anything approaching a reasoned explanation for its decisions" (internal quotations omitted)).

In considering how to shape information access policies, Defendants had hordes of guidance from statutes and their own regulations about core considerations to be prioritized. The

Privacy Act, for example, places a variety of affirmative requirements on agencies, such as requiring that each agency record access regimes establish clear "rules of conduct" for people with systems access and training on the "rules and requirements of the Privacy Act." *See* 5 U.S.C. § 552a(e)(9). It 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).

Further, the Act requires that system access rules are clearly defined to the public *prior* to systems being established or revised, with notice and an opportunity for public feedback. *See id.* §§ 552a(e)(4), (e)(11). And, as described in previous sections, each agency has in place a variety of regulations implementing the Privacy Act as well as more specific regulations governing access to particular systems.

Similarly, FISMA requires agencies to evaluate the risks and harms of potential unauthorized disclosure of information and establish protections commensurate with those risks. *See* 44 U.S.C. § 3554(a)(1)(A).

The vast array of laws and regulations governing the disclosure of sensitive government information reflect the myriad considerations that Congress and the agencies themselves have previously understood to constrain agencies' policies with respect to maintenance and disclosure private information. 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 Access Policies.

Defendants' DOGE Access Policies also fail to account for the substantial risks of sensitive information concerning DOGE personnel's outside business interests being disclosed through sweeping DOGE access to agency systems. Both DOL and CFPB host information that is relevant to Mr. Musk's outside businesses, including records of enforcement activities (past and ongoing) at his companies, confidential consumer complaints about his companies, and information about potential regulation of personal finance apps, a market that he is reportedly about to enter. *See infra* §§ I.A, C. These agencies also hold similar information about Mr. Musk's competitors. But there is no indication that the DOL DOGE Access Policy or CFPB DOGE Access Policy have been tailored 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).

Finally, Defendants utterly fail 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. *See, e.g.*, Ex. A ¶ 6; Ex. L ¶ 10 ("The promise of confidentiality is an essential condition to encourage workers to come forward."); Ex. O ¶ 8 ("I am afraid that if Waffle House finds out I filed a complaint against the company, against me . . . . I fear that I could be fired or that I would lose the opportunity to get a cook position."). "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." *Dep't of Homeland Sec. v. Regents of the Univ. of Cal.*, 591 U.S. 1, 30 (2020) (internal quotation marks and citations omitted).

4. Defendants' DOGE Access Policies Are Procedurally Infirm.

Each of the Department of Labor, the CFPB, and HHS maintains confidentiality requirements for various systems and datasets within their control, which may only be accessed or released under identified and limited circumstances. *See, e.g.* 20 C.F.R. 10.10 (governing FECA at Department of Labor); 12 C.F.R. 1070.40-48 (governing confidential data at CFPB); 45 C.F.R. part 5b (privacy act regulations for HHS). To modify these requirements, which were promulgated through notice and comment rulemaking, each respective agency must "afford notice of a proposed rulemaking and an opportunity to comment prior to a rule's promulgation, amendment, modification, or repeal." *Liquid Energy Pipeline Ass'n v. Fed. Energy Regul. Comm'n*, 109 F.4th 543, 547 (D.C. Cir. 2024) (emphasis added).

The Department of Labor, CFPB, and HHS policies of granting DOGE unrestricted access to the information in their systems represent radical alterations to each agency's confidentiality requirements; yet none of the agencies undertook notice and comment rulemaking—nor any other formal process—to modify or repeal those requirements. Nor is it any answer to characterize the agencies' new policies as exceptions to their prior and permanent ones; the policies do not contemplate such exceptions, and in any event, notice and comment is required even for brief pauses of rules adopted by notice and comment. *Clean Air Council v. Pruitt*, 862 F.3d 1, 8-9 (D.C. Cir. 2017) (agency is required to follow notice and comment even to "issue a brief stay" of a rule promulgated through notice and comment).

As discussed above, the Privacy Act, 5 U.S.C. § 552a(e)(4), requires agencies to publish SORNs in the Federal Register and to provide an opportunity for public comment. And each time

an agency seeks to add a new category of routine use for the information covered by a SORN, it must do so by notice and comment. 5 U.S.C. § 552a(e)(11). But the agencies here have attempted to create a new routine use for information in their systems of record—blanket disclosure to DOGE—without following the required notice and comment processes for creating a new routine use.

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

By the President's own design, DOGE is a creature of Executive Order only and—unlike the predecessor U.S. Digital Service, whose vacant shell DOGE now inhabits—has no basis in statute. *See generally* E.O. That structure was carefully selected by the President, seemingly in order to bolster the argument that DOGE is not subject to transparency laws, like FOIA, but the President's choice comes at a tradeoff. Specifically, by creating DOGE as a free-floating component of the Executive Office of the President (EOP), disconnected from any source of statutory authority, DOGE has no direct statutory authority to exercise and its powers are thus limited to providing advice and recommendations to the President. Actions DOGE takes in excess of that legitimate role are, accordingly, *ultra vires* and should be given no legal force or effect. Of particular relevance to this action, the inter-agency personnel agreements with federal agencies that DOGE purported to execute, *see* Ramada Decl. ¶ 5, which Defendants have pointed to as justification for their decisions to grant DOGE personnel broad access that would otherwise violate federal privacy laws, are *ultra vires* and of no legal force or effect. Actions taken by DOGE personnel to direct agency officials to authorize their access to agency systems are, likewise, unlawful.

Under the Constitution, only Congress has the "authority to create offices and to provide for the method of appointment to those offices." *Freytag v. Comm'r*, 501 U.S. 868, 883 (1991).

See also Nat'l Fed. Of Indep. Bus. v. OSHA, 595 U.S. 109, 117 (2022) ("Administrative agencies are creatures of statute."). Components of the Executive Branch, accordingly, "possess only the authority that Congress has provided." *Nat'l Fed. Of Indep. Bus.*, 595 U.S. at 117. With respect to inter-agency personnel agreements, Congress provided legal authority for exactly that purpose through the Economy Act of 1932, which regulates whether and when federal employees can be temporarily detailed to new agencies. The Economy Act provides that, under certain circumstances, "[t]he head of an agency or major organizational unit *within an agency* may place an order with a major organizational unit within the same agency *or another agency* for goods or services[.]" 31 U.S.C. § 1535(a) (emphasis added). For purposes of Title 15 of the U.S. Code, "'agency' means a department, agency, or instrumentality of the United States Government." *Id.* § 101. Because DOGE is not an "agency or a major organizational unit within an agency" for purposes of the Economy Act, it cannot lawfully enter into agreements to detail its personnel to lawfully established federal agencies.

To understand why DOGE's authority is limited in this manner, a close examination of its structure is required. As described above, DOGE was established by an Executive Order renaming the pre-existing U.S. Digital Service. *See* E.O. § 1. The U.S. Digital Service, which Defendants have correctly observed routinely entered into Economy Act agreements with federal agencies, *see* Ramada Decl. ¶ 3, was established by Presidential directive but organized under the Office of Management and Budget (OMB) and its work was supervised by the Deputy Director of

Management.[38] The E.O. creating DOGE severs that link to OMB by making clear that DOGE is not only organized within EOP, but also that the official in charge of DOGE, the DOGE Administrator, reports only to the White House Chief of Staff. *See* E.O. § 3(b). Further evidence of DOGE's independence from OMB is the manner in which it receives its funding. Whereas U.S. Digital Service apportionments flowed into an OMB account for "General Departmental Management," DOGE receives apportionments directly.[39]

DOGE's structure is unusual[40] but unambiguous. Multiple White House officials have asserted that DOGE "falls under the Presidential Records Act" (PRA) and that it is not, therefore, subject to FOIA.[41] If that is the White House's position, then DOGE's "function" is definitionally

---

[38] *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).

[39] *Compare* General Departmental Management, OpenOMB (accessed on Feb. 6, 2025), https://openomb.org/file/11293991 (describing and linking to OMB apportionment records), *with* United States DOGE Service, OpenOMB (accessed on Feb. 6, 2025), https://openomb.org/file/11409329 (same). *See also* Jason Koebler et al., *DOGE Employees Ordered to Stop Using Slack While Agency Transitions to a Records System Not Subject to FOIA*, 404 Media (Feb. 5, 2025), https://www.404media.co/doge-employees-ordered-to-stop-using-slack-while-agency-transitions-to-a-records-system-not-subject-to-foia/.

[40] Other components of EOP were created by statute. *See, e.g.*, 15 U.S.C. § 1023 (creating the Council of Economic Advisers); 31 U.S.C. § 501 (creating OMB); 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).

[41] *See* Minho Kim, *Trump's Declaration Allows Musk's Efficiency Team to Skirt Open Records Laws*, N.Y. Times (Feb. 10, 2025), https://www.nytimes.com/2025/02/10/us/politics/trump-musk-doge-foia-public-records.html?smid=url-share; *see also* Katie Miller (@katierosemiller), X (Feb. 5, 2025, 5:26 PM), https://x.com/katierosemiller/status/1887311943062499425 (contending that the E.O. made DOGE "subject to Presidential Records [Act]").

limited "to advis[ing] or assist[ing] the President, in the course of conducting activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President." 44 U.S.C. § 2201.[42] Courts have long recognized that EOP components serving that advisory function are not "agencies" under federal law. *See, e.g.*, *Armstrong v. Exec. Off. of the President*, 90 F.3d 553 (D.C. Cir. 1996) (National Security Council not an "agency" under FOIA); *In Re: Executive Office of the President, Petitioner*, 215 F.3d 20 (D.C. Cir. 2000) (EOP not an "agency" under the Privacy Act); *Haddon v. Walters*, 43 F.3d 1488 (D.C. Cir. 1995) (Executive Residence not an "agency" under Title VII); GAO, *Argus Secure Technology, LLC*, B-419422; B-419422.2 (Office of Administration not an "agency" under Federal Property and Administrative Services Act of 1949).

President Trump made an intentional choice to establish DOGE in the manner set forth in the E.O. and Defendants must accept the associated tradeoffs, including that DOGE cannot lawfully enter into Economy Act agreements; direct operations or decisions at federal agencies, such as the creation of DOGE Access Policies at issue in this case; direct adverse employment actions against agency employees who question DOGE's authority; or exercising management authority over agency operations.

II. Continuing to Allow DOGE to Unlawfully Access Systems and Records Will Cause Plaintiffs to Suffer Immediate, Irreparable Injury.

For many of the same reasons that Plaintiffs have established standing, *supra*, they have also demonstrated that the sharing of information by Labor, HHS, and CFPB with DOGE will

---

[42] *Armstrong v. Exec. Off. of the President, Off. of Admin.*, 1 F.3d 1274, 1292 (D.C. Cir. 1993) (noting that, to balance separation of powers concerns, "Congress . . . explicitly provided that the PRA would apply only to records that 'fall outside the scope of FOIA because they are not agency records'").

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). 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 All. for Hippocratic Med.*, 602 U.S. at 395 (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").

DOGE gaining unauthorized access to sensitive employment, health, disability, and financial data will cause irreparable harm. *See Human 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").

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.[43] 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. Ex. F ¶¶ 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

[43] 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.

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 to Defendant Agencies. As Plaintiffs have declared, their members routinely report legal violations to Labor, HHS, and CFPB. *See infra* Sections 4(A)(1)-(3). Defendant Agencies' guarantees of confidentiality are not only required by law, but also essential to these workers' willingness to report these legal violations. Plaintiffs and their members reasonably fear retaliation from reporting, which is why the submissions are confidential. *See, e.g.*, Ex. A ¶ 6 ("This assurance [of confidentiality] is vital because fear of employer retaliation is a powerful deterrent[.]"); Ex. C ¶ 7 ("The promise of confidentiality is an essential condition"). 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.

Indeed, courts have recognized that creating a chilling effect from engaging in First Amendment activity, such as reporting violations of the law, constitutes irreparable harm. As expressed by the Supreme Court, "[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 Defendant Agencies' 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 Defendant Agencies and their programs to ensure fair treatment of their members. *See infra* Sections 4(A)(1)-(3). Rapid, arbitrary, and ill-considered fundamental changes to Defendant Agencies' work and responsibilities will wreak havoc for Plaintiffs, their members, and the communities they serve. *Cf.*, *e.g.*,. *Regents of the Univ. of Calif.*, 591 U.S. at 30-33 (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 All.*, 286 F. Supp. 3d at 179 (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 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 foregoing reasons, Plaintiffs respectfully request that this Court grant their motion and enter an order temporarily restraining Agency Defendants from providing DOGE personnel access to systems containing non-public information or the records contained therein, directing DOGE personnel to return or destroy any copies of material previously accessed from agency systems and records, directing Agency Defendants to remove any software installed by DOGE personnel on agency systems, and enjoining DOGE personnel from exercising *ultra vires* authority with respect to Agency Defendants.

Dated: February 12, 2025

Respectfully submitted,

/s/ Aman T. George

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)
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
sperryman@democracyforward.org
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

* Admitted *pro hac vice*
** Motion for admission forthcoming
*** Motion for admission *pro hac vice* forthcoming