UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN FEDERATION OF LABOR AND CONGRESS OF INDUSTRIAL ORGANIZATIONS,
815 Black Lives Matter Plaza NW,
Washington, DC 20006.

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO,
80 F Street NW,
Washington, D.C. 20001,

AMERICAN FEDERATION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO,
1625 L Street, NW,
Washington, D.C. 20036,

SERVICE EMPLOYEES INTERNATIONAL UNION, AFL-CIO,
1800 Massachusetts Ave. NW,
Washington, DC 20036,

COMMUNICATIONS WORKERS OF AMERICA, AFL-CIO
501 3rd Street, NW, 6th Floor
Washington, DC 20001,

ECONOMIC POLICY INSTITUTE
1225 I St NW #600
Washington, DC 20005,

VIRGINIA POVERTY LAW CENTER
919 East Main Street, Suite 610
Richmond, VA 23219

ECONOMIC ACTION MARYLAND FUND
2209 Maryland Avenue
Baltimore, MD 21218

Case No. 1:25-cv-00339-JDB

AMERICAN FEDERATION OF TEACHERS
555 New Jersey Avenue NW Washington, DC 20001,

Plaintiffs,

vs.

DEPARTMENT OF LABOR
200 Constitution Ave., NW,
Washington, DC 20210

VINCE MICONE, in his official capacity as Acting Secretary, Department of Labor
200 Constitution Ave., NW,
Washington, DC 20210

DEPARTMENT OF HEALTH & HUMAN SERVICES,
200 Independence Avenue SW
Washington, DC 20201

DOROTHY A. FINK, in her official capacity as Acting Secretary, Department of Health and Human Services
200 Independence Avenue SW
Washington, DC 20201

CONSUMER FINANCIAL PROTECTION BUREAU
1700 G Street NW
Washington, DC 20552

RUSSELL VOUGHT, in his official capacity as Acting Director, Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

U.S. DIGITAL SERVICE (U.S. DOGE SERVICE)
736 Jackson Pl NW
Washington, DC 20503

U.S. DOGE SERVICE TEMPORARY ORGANIZATION
736 Jackson Pl NW
Washington, DC 20503

Defendants.

PLAINTIFFS' FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. Since President Trump's inauguration on January 20, the "U.S. DOGE Service," led by White House official Elon Musk, has launched a sweeping campaign to access highly-sensitive information systems and dismantle and restructure multiple federal agencies unilaterally.

2. The speed of these efforts is core to the project. At every step, DOGE is violating multiple laws, from constitutional limits on executive power, to laws protecting civil servants from arbitrary threats and adverse action, to crucial protections for government data collected and stored on hundreds of millions of Americans.

3. DOGE seeks to gain access to sensitive agency systems and records before courts can stop them, dismantle agencies before Congress can assert its Constitutional prerogatives in the federal budget, and intimidate and threaten employees who stand in their way, without regard for the consequences.

4. The results have already been catastrophic. DOGE has seized control of some of the most carefully protected information systems housed at the Treasury Department, taken hold of all sensitive personnel information at the Office of Personnel Management, and dismantled an entire agency within a week.

5. DOGE's spread through the government continues to be rapid, and this case seeks to protect the privacy and the legal rights of millions of Americans who depend upon three of those agencies: the Department of Labor, the Department of Health and Human Services, and the Consumer Financial Protection Bureau.

6. DOGE employees are either seeking or have been granted access to information systems controlled by these agencies, which they should be legally barred from. In at least one of these agencies, employees have been threatened with termination if they seek to protect the integrity of sensitive systems. And at all of these agencies, DOGE claims power and authority that Congress has never granted them, and that they may not legally exercise.

7. As detailed below, DOGE's access to sensitive information systems, with the blessings of the other agency Defendants in this matter, lacks statutory authority and violates the Privacy Act and the Administrative Procedure Act.

8. Absent this Court's intervention, DOGE will have access to highly sensitive data, including, among many others, medical and benefits information about all federal workers with worker compensation or Black Lung claims, the identities of vulnerable workers who have sought the Department's protection via wage and hour or occupational safety complaints, and investigative and litigation records of the Bureau of Labor Statistics data crucial to an accurate understanding of the state of our economy.

9. DOGE will also have access to Department of Labor records concerning investigations of Mr. Musk's businesses, as well as records containing the sensitive trade secrets of his business competitors, which are held by the Department of Labor and Consumer Financial Protection Bureau. No other business owner on the planet has access to this kind of information on his competitors, and for good reason.

10. DOGE's access to systems of records within the Department of Health and Human Services exposes personal and health information of Medicare and Medicaid beneficiaries, as well as personal information of the healthcare providers who care for them. And it also exposes the personnel information of HHS' own employees, including those represented by Plaintiff AFGE, among many other kinds of sensitive personal and health information.

11. And from information and data held by the Consumer Financial Protection Bureau, DOGE will also have access to sensitive personal information about individual consumers—whether from complaints the consumers submitted to the CFPB themselves, or from records obtained during Bureau investigations and examinations.

12. Plaintiffs file this complaint and seek a temporary restraining order to maintain the status quo until the Court has an opportunity to more fully consider the illegality of the proposed actions.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises under federal law, specifically the Privacy Act, 5 U.S.C. § 552a, and the Administrative Procedure Act, 5 U.S.C. § 701, *et seq*.

14. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) because Defendants are (or purport to exercise the authority of) agencies of the United States and officers or employees of those federal agencies who are sued in their official capacity. Further, Defendants are headquartered in the District of Columbia, where a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred.

PARTIES

15. The American Federation of Labor and Congress of Industrial Organizations ("AFL-CIO") is a federation of 63 national and international labor organizations with a total

membership of over 13 million working men and women. The AFL-CIO is headquartered in Washington, D.C.

16. The American Federation of Government Employees ("AFGE") is a labor organization and unincorporated association that is affiliated with the AFL-CIO, headquartered in Washington, D.C. AFGE, the largest federal employee union, represents approximately 800,000 federal civilian employees through its affiliated councils and locals in every state in the United States. AFGE represents thousands of employees at the Department of Labor, including at various DOL components across the country. It also represents employees of the Department of Health & Human Services, including at the Centers for Medicare & Medicaid Services, the National Institute for Occupational and Health Safety ("NIOSH") at the Centers for Disease Control ("CDC"), and the National Institutes of Health ("NIH").

17. The American Federation of State, County & Municipal Employees, AFL-CIO ("AFSCME") is a national labor organization and unincorporated membership association headquartered in Washington, D.C. AFSCME is the largest trade union of public employees in the United States, with around 1.4 million members organized into approximately 3,400 local unions, 58 councils and other affiliates in 46 states, the District of Columbia, and Puerto Rico. AFSCME, through its affiliate District Council 20 and its constituent local unions, represents federal civilian employees in agencies and departments across the federal government.

18. Service Employees International Union, AFL-CIO ("SEIU") is a labor organization of approximately two million working people in the United States and Canada united by the belief in the dignity and worth of workers and the services they provide. SEIU's vision for a just society includes one where working people have access to healthcare,

particularly retirees and individuals who are Medicare beneficiaries. SEIU is headquartered in Washington, D.C.

19. The Communications Workers of America, AFL-CIO ("CWA") is a union of hundreds of thousands of public and private sector workers in communities across the United States, Canada, Puerto Rico, and other U.S. territories. Its members work in telecommunications and IT, the airline industry, manufacturing, federal service contracts, news media, broadcast and cable television, education, health care, public service, and other fields. It is headquartered in Washington, D.C.

20. Economic Policy Institute ("EPI") is a nonprofit, nonpartisan think tank created in 1986 to include the needs of low- and middle- income workers in economic policy discussions. EPI conducts research and analysis on the economic status of working America, proposes public policies that protect and improve working conditions of low- and middle-income workers, and assesses policies with respect to how well they further these goals. EPI is headquartered in Washington, D.C.

21. Plaintiff Virginia Poverty Law Center ("VPLC") is a nonprofit organization that since 1978 has worked to break down systemic barriers that keep low-income Virginians in the cycle of poverty through advocacy, education, litigation, and direct counseling and referral services. VPLC is headquartered in Richmond, VA.

22. Plaintiff Economic Action Maryland Fund ("EAMF") is a nonprofit organization that advances economic inclusion and financial justice through research, advocacy, consumer education, and direct services. EAMF is headquartered in Baltimore, MD.

23. Plaintiff American Federation of Teachers ("AFT") is a membership organization representing 1.8 million members, who reside in almost every U.S. state, the District of

Columbia, Puerto Rico, and Guam, and who are employed as pre-K through 12th-grade teachers, early childhood educators, paraprofessionals, and other school-related personnel; higher education faculty and professional staff; federal, state, and local government employees; and nurses and other healthcare professionals. AFT's purpose is to promote fairness, democracy, economic opportunity, and high-quality public education, healthcare, and public services for students, their families, and communities their members serve. AFT does so by ensuring its members receive fair pay and benefits for their critical work, and by fighting for safe working conditions that also benefit students, patients and all those who use public services. Helping children and students is at the core of AFT's mission. So too is the economic security and dignity of AFT's members and their families. AFT is headquartered in Washington, DC.

24. Defendant the Department of Labor ("DOL") is a federal agency headquartered in Washington, D.C. with responsibilities governing occupational safety and health, wage and hour standards, unemployment benefits, reemployment services, and economic statistics.

25. Defendant Vince Micone is the Acting Secretary of the Department of Labor. He is sued in his official capacity.

26. Defendant Consumer Financial Protection Bureau ("CFPB") is a federal financial regulatory agency headquartered in Washington, D.C. charged with administering federal consumer protection laws and regulating a broad swath of consumer financial products and services.

27. Defendant Russell Vought is the Acting Director of the CFPB. He is sued in his official capacity.

28. Defendant Department of Health and Human Services ("HHS") is a federal regulatory agency headquartered in Washington, D.C. comprised of thirteen operating divisions,

which are collectively responsible for regulating various aspects of the nation's healthcare system and promoting public health.

29. Defendant Dorothy Fink is the Acting Secretary of HHS. She is sued in her official capacity.

30. Defendant U.S. DOGE Service ("USDS") is a federal entity situated within the Executive Office of the President in Washington, D.C. Upon information and belief, its work is directed by Elon Musk, who is reportedly serving in the Trump-Vance Administration as a Special Government Employee ("SGE"). Mr. Musk is the wealthiest person in the world, with an estimated net worth of over $400 billion. Concurrent with his tenure in government, Mr. Musk has numerous large business concerns, many of which have substantial ties to the federal government and U.S. politics. They include SpaceX, a space technology company and extensive federal government contractor; Tesla Motors, an electric vehicle company; Neuralink, a neurotechnology startup seeking to embed computer hardware into the human brain; the Boring Company, a tunnel construction company; and X, formerly known as Twitter, a large social media platform.

31. Defendant U.S. DOGE Service Temporary Organization is a federal temporary organization situated within the Executive Office of the President in Washington, D.C..[1]

LEGAL FRAMEWORK

The Privacy Act of 1974

32. 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

[1] Because the division of labor, personnel, authority, and responsibility between the U.S. DOGE Service and U.S. DOGE Service Temporary Organization is not clear, this complaint will simply refer to them collectively as "DOGE."

other things, "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose . . . and that adequate safeguards are provided to prevent misuses of such information." Privacy Act of 1974 § 2(b), 2(b)(4), 88 Stat. 1896 (1974), *codified as amended at* 5 U.S.C. § 552a. "[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies," Congress decided "to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Id.* § 2(a)(5), 88 Stat. 1896, 1896.

33. 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).

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

35. As relevant for this case, the Privacy Act regulates the disclosure of records and imposes requirements on agencies to responsibly maintain their recordkeeping systems.

36. With respect to disclosure, the Act provides, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a(b).[2]

[2] This provision contains a number of exceptions, listed at 5 U.S.C. § 552a(b)(1)-(13), none of which apply to make DOGE's access to agency systems and records permissible.

The Federal Information Security Modernization Act of 2014

37. The Federal Information Security Modernization Act of 2014 ("FISMA"), 44 U.S.C. §§ 3551-58, requires agencies to provide information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized access [or] use" of information or information systems maintained by the agency. 44 U.S.C. § 3554(a)(1)(A).

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

39. "[S]enior agency officials" are required to "provide information security for the information and information systems that support the operations and assets under their control," including understanding the risks of "unauthorized access, use, disclosure, disruption, modification, or destruction" of sensitive agency records, and implementing policies designed to reduce those risks. *See* 44 U.S.C. § 3554(a)(2).

The Administrative Procedure Act

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

FACTUAL ALLEGATIONS

I. The "Department of Government Efficiency."

41. On November 12, 2024, then President-Elect Trump announced his intent to create the "Department of Government Efficiency" ("DOGE") to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget," to help "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[3]

42. On the day of his inauguration, January 20, 2025, President Trump signed Executive Order 14158, Establishing and Implementing the President's "Department of Government Efficiency," ("the E.O."), reorganizing and renaming the United States Digital Service as the United States DOGE Service, established in the Executive Office of the President.[4]

43. The E.O. established the role of U.S. DOGE Service Administrator in the Executive Office of the President, reporting to the White House Chief of Staff.[5]

44. The E.O. further established within U.S. DOGE Service a temporary organization known as "the U.S. DOGE Service Temporary Organization." The U.S. DOGE Service Temporary Organization is headed by the U.S. DOGE Service Administrator and is tasked with advancing "the President's 18-month DOGE agenda."[6]

45. The E.O. also requires each Agency Head to establish a "DOGE Team" comprised of at least four employees within their respective agencies. DOGE Teams are required

---

[3] *See* Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, 7:46 PM ET), https://truthsocial.com/@realDonaldTrump/posts/113472884874740859.
[4] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025).
[5] *Id.* at § 3(b).
[6] *Id.*

to "coordinate their work with [U.S. DOGE Service] and advise their respective Agency Heads on implementing the President's DOGE Agenda."[7]

46. The E.O. directs Agency Heads to take all necessary steps "to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems,"[8] but makes no mention of this directive being subject to applicable law. The E.O. nominally directs the U.S. DOGE Service to adhere to "rigorous data protection standards."[9]

47. The E.O. does not vest any statutory authority in DOGE.

48. Multiple DOGE officials have asserted that DOGE "falls under the Presidential Records Act,"[10] which applies to, in relevant part, "a unit or individual of the Executive Office of the President whose function is to advise or assist 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.

II. DOGE'S Pattern of Rapidly Entering Agencies, Seizing Critical Systems, and Unilaterally Dismantling and Restructuring them

49. Since Inauguration Day, DOGE personnel have sought and obtained unprecedented access to information systems across numerous federal agencies, including the United States Agency for International Development, the Department of Treasury, the National Oceanic and Atmospheric Administration, the Office of Personnel Management, and the Department of Education.

---

[7] *Id.* at § 3(c).
[8] *Id.* at 4(b).
[9] *Id.*
[10] 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]").

50. DOGE personnel also played critical roles in the dismantling of the U.S. Agency for International Development and ongoing concurrent efforts to largely cripple the Department of Education.

51. DOGE's behavior repeats itself across virtually every agency it enters: swooping in with new DOGE staff, demanding access to sensitive systems, taking employment action against employees who resist their unlawful commands, and then beginning to re-work the agencies at their will. This process moves incredibly quickly, with agencies transformed roughly overnight, or fully dismantled within a week.

52. Many DOGE staffers appear to be working across multiple agencies concurrently,[11] 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.

[11] *See, e.g.*, Tim Marchman and Matt Giles, *This DOGE Engineer Has Access to the National Oceanic and Atmospheric Administration*, Wired (Feb. 5, 2025), https://www.wired.com/story/doge-engineer-noaa-data-google-musk-climate-project-2025/; Vittoria Elliott et al., *The US Treasury Claimed DOGE Technologist Didn't Have 'Write Access' When He Actually Did*, Wired (Feb. 6, 2026), https://www.wired.com/story/treasury-department-doge-marko-elez-access/; Avi Asher-Schapiro et al., *Elon Musk's Demolition Crew*, ProPublica (Feb. 6, 2025), https://projects.propublica.org/elon-musk-doge-tracker/ (DOGE staffer Nikhil Rajpal working at NOAA, CFPB, and OPM); Asher-Shapiro; Ella Nilsen and Sean Lyngaas, *Trump energy secretary allowed 23-year-old DOGE rep to access IT systems over objections from general counsel*, CNN (Feb. 7, 2025), https://www.cnn.com/2025/02/06/climate/doge-energy-department-trump/index.html (DOGE staffer Luke Farritor working at HHS and Department of Energy); Evan Weinberger, *Musk's DOGE Descends on CFPB With Eyes on Shutting It Down*, Bloomberg Law (Feb. 7, 2025), https://news.bloomberglaw.com/banking-law/musks-doge-descends-on-consumer-financial-protection-bureau; Asher-Shapiro (DOGE staffer Gavin Kliger working at CFPB, OPM, and USAID); Makena Kelly and Zoe Schiffer, *Elon Musk's Friends Have Infiltrated Another Government Agency*, Wired (Jan. 31, 2025), https://www.wired.com/story/elon-musk-lackeys-general-services-administration/; Asher-Shapiro; Laura Barrón-López (@lbarronlopez), X (Feb. 3, 2025, 2:05 PM), https://x.com/lbarronlopez/status/1886491276729544809 (DOGE staffer Edward Coristine working at OPM, Small Business Administration, and General Services Administration).

53. 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.[12]

A. Sensitive data takeovers at Treasury and OPM

54. Shortly before President Trump's inauguration, DOGE operatives demanded access to sensitive Treasury systems, including the system used by the Bureau of the Fiscal Service ("BFS"), to control the vast majority of federal payments.[13]

55. The career official serving as Acting Secretary of the Treasury prior to Secretary Bessent's confirmation denied DOGE operatives' request for access to the BFS payment system, and was subsequently placed on administrative leave.[14]

56. Following his confirmation, Secretary Bessent granted DOGE operatives access to BFS, though the precise identities of DOGE personnel with access, and their level of access, are not reliably known by the public.[15]

[12] 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/.

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

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

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

57. According to some reporting, DOGE personnel had the ability to stop individual payments from the BFS system, to change data in the system, or to alter system code.[16]

58. On February 8, a judge in the Southern District of New York issued a Temporary Restraining Order halting DOGE's access to Treasury systems, finding that granting DOGE access to those systems "presents the risk of disclosure and confidential information and [a] heightened risk that the systems in question will be more vulnerable than before to hacking." *Order Granting Temporary Restraining Order, New York v. Trump,* No. 25 Civ. 1144, slip op. at 2 (S.D.N.Y. Feb. 8, 2025).

59. In the wake of that decision, Mr. Musk for the first time described at least some of DOGE's work at Treasury as seeking to ensure that payment categorization codes in outgoing government payments are no longer left blank, requiring every payment to "include a rationale for the payment," and require more frequent updating of Treasury's "DO-NOT-PAY" list.[17] According to Mr. Musk, career Treasury employees rather than DOGE staff will be implementing these changes.[18]

60. Mr. Musk described said the DOGE team and Treasury had jointly agreed to this work, although he did not indicate whether it was the full extent of DOGE's work and plans in Treasury's sensitive systems.[19]

---

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

[17] Elon Musk (@elonmusk), X (Feb. 8, 2025, 2:51 PM ET), https://x.com/elonmusk/status/1888314848477376744.

[18] *Id.*

[19] *See id.*

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

62. DOGE personnel directed OPM staff to grant them high-level access to OPM computer systems, and quickly took control of them, including systems containing large troves of personally identifiable information. DOGE personnel individuals also locked career civil servants at OPM out of at least some of those systems, giving them completely unchecked control over the systems and the information they contain.[21]

63. The identities of the DOGE personnel who have access to Treasury and OPM systems and to whom sensitive information has been disclosed are not yet clear, and to the extent there is available information on those individuals, it is only available from public reporting.

B. Agency dismantlement at USAID and the Department of Education

64. During the week of January 27th, Elon Musk and his team began joining staff calls at USAID,[22] and the DOGE team asked "detailed questions during meetings about

[20] *Id.*
[21] Tim Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, Reuters (Feb. 1, 2025), https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.
[22] Will Steakin et al., *Turmoil inside USAID as Musk calls the agency 'criminal' and says it 'has to die.'* ABC News (Feb. 3, 2025), https://abcnews.go.com/Politics/turmoil-inside-usaid-doge-reps-offices-senior-officials/story?id=118368900.

organizational charts, contractors and aid programs."[23]

65. Over the course of the next several days, DOGE staff presided over the rapid shutdown of the agency, ordering the issuance of termination notices to employees without due process,[24] and gaining access to USAID systems by terminating employees who resisted granting access.[25]

66. By February 2, more than 1,000 USAID employees and contractors had been fired or furloughed from USAID,[26] and Mr. Musk bragged the next day about "feeding USAID into the woodchipper."[27] On February 4th, USAID sent out an email, placing nearly its entire workforce on administrative leave.[28]

67. A similar pattern is playing out at the Department of Education, with DOGE staff entering the agency with intent to cut spending and agency staff,[29] gaining access to "multiple

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

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

[25] *Id.*

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

[27] Elon Musk (@elonmusk), X (Feb. 3, 2025, 1:54 AM ET), https://x.com/elonmusk/status/1886307316804263979.

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

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

sensitive internal systems,"[30] and Mr. Musk tweeting about the dismantling of the agency.[31]

III. Threats to the Department of Labor

A. DOGE's access to the Department of Labor

68. Last Tuesday, February 4, a journalist shared on social media that her sources told her that "DOGE is going after the Department of Labor next. DOL workers have been ordered to give DOGE access to anything they want-or risk termination."[32]

69. As detailed in the attached affidavit of Rushab Sanghvi, General Counsel of Plaintiff AFGE, one of AFGE's members substantiated this report. DOL leadership told that that when Mr. Musk and his team visit DOL, they are to do whatever they ask, not to push back, not to ask questions. They were told to provide access to any DOL system they requested access to and not to worry about any security protocols; just do it. Based on leadership's statements, the employee believed they could face termination if they did not comply.

70. On February 5, many of the plaintiffs in this case filed an initial complaint and sought a temporary restraining order to halt DOGE's access to DOL's systems. Initial Complaint (Feb. 5, 2025), ECF No. 1; Motion for a Temporary Restraining Order (Feb. 5, 2025), ECF No. 2. Counsel for Plaintiffs and DOL jointly called this Court's chambers about Plaintiffs' Complaint and Motion. During that call, DOL's counsel confirmed that the reported meeting between DOGE staff was underway. At this Court's suggestion, DOL agreed to commit to

[30] *Id.*

[31] Elon Musk (@elonmusk), X (Feb. 3, 2025, 10:50 PM ET), https://x.com/elonmusk/status/1886623446907400676.

[32] Kim Kelly (@GrimKim), X (Feb. 4, 2025, 5:04 PM ET), https://x.com/GrimKim/status/1886898588099240401.

halting DOGE access to DOL systems until this Court could consider Plaintiffs' pending TRO motion. *See* Order Setting Hearing (Feb. 5, 2025), ECF No. 5.

71. On February 6, Defendants filed a declaration from a DOGE employee at DOL purporting to describe his status as a detailee from DOGE to the Department. Memorandum in Opposition to Motion for Temporary Restraining Order, Ex. 1 (Adam Ramada Declaration) (Feb. 6, 2025), ECF No. 16-1. The declarant did not contest that DOL employees had been ordered to give DOGE access to all DOL systems on the threat of termination. The declarant did not state that the DOGE detailees at the Department would only serve a detail at one agency at a time. Nor did the declarant state that DOGE detailees would be solely accountable to leadership at DOL, and not to leadership at DOGE. The declarant did not produce any written documentation demonstrating the contours of or legal approval of his detail or the details of other DOGE personnel.

72. On February 7, this Court ruled against Plaintiffs' TRO motion, finding that Plaintiffs had not adequately pled standing to bring this case.

73. DOGE staff are now permitted to enter DOL and gain access to sensitive systems to which they are not lawfully allowed access. DOGE staff may also attempt to begin an unlawful wholesale dismantling or restructuring of the agency to suit the private business interests or political preferences of DOGE leaders or President Trump.

B. Ongoing Department enforcement against Mr. Musk's companies and competitors

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

75. The Occupational Safety and Health Administration ("OSHA") within the Department is responsible for enforcing safety standards at American companies. OSHA has investigated Mr. Musk's space technology company, SpaceX, over multiple safety incidents, and

has fined SpaceX in connection with one worker's death and seven other serious safety incidents.[33]

76. OSHA has also investigated and issued fines to Tesla for unsafe working conditions in its factories.[34]

77. OSHA also has open investigations into the Boring Company, and has issued it multiple fines for serious citations, according to OSHA's website.[35]

78. On information and belief, the Department of Labor also currently has open investigations into one or more competitors of Mr. Musk's companies.

79. Mr. Musk would ordinarily be unable to access non-public information regarding those investigations. *See* 18 U.S.C. § 1832(a) (Trade Secrets Act); 5 U.S.C. § 552(b)(4) (FOIA exemption for trade secrets); 5 U.S.C. § 552(b)(7) (FOIA exemption for records or information compiled for law enforcement purposes).

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

---

[33] 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/ .

[34] 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.

[35] 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).

C. Sensitive and valuable systems within the Department of Labor

81. Many sensitive data sources and processes are housed within the Department, including some classified information. The Department lists over 50 different systems containing personally identifiable information across its functions.[36] 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. There is no public indication that Mr. Musk or DOGE personnel on leave from Mr. Musk's corporate interests will be recused from access to any of this data.

83. Some examples follow.

1. FECA

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

85. Because DOL administers all workers' compensation claims for federal employees, it is responsible for all of these records.[37] FECA records include highly sensitive personal information, including the following information:

---

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

[37] 20 C.F.R. 10.10; *see also* DOL/GOVT-1, available at https://www.govinfo.gov/content/pkg/PAI-2023-DOL/xml/PAI-2023-DOL.xml#govt1 (last accessed Feb. 5, 2025)

> Reports of injury by the employee and/or employing agency; claim forms filed by or on behalf of injured Federal employees or their survivors seeking benefits under FECA; forms authorizing medical care and treatment; other medical records and reports; bills and other payment records; compensation payment records; formal orders for or against the payment of benefits; transcripts of hearings conducted; and any other medical, employment, or personal information submitted or gathered in connection with the claim. The system may also contain information relating to dates of birth, marriage, divorce, and death; notes of telephone conversations conducted in connection with the claim; information relating to vocational and/or medical rehabilitation plans and progress reports; records relating to court proceedings, insurance, banking and employment; articles from newspapers and other publications; information relating to other benefits (financial and otherwise) the claimant may be entitled to; and information received from various investigative agencies concerning possible violations of Federal civil or criminal law. The system may also contain information relating to certain claims under the War Hazards Compensation Act (WHCA).
>
> The system may also contain consumer credit reports on individuals indebted to the United States, information relating to the debtor's assets, liabilities, income and expenses, personal financial statements, correspondence to and from the debtor, information relating to the location of the debtor, and other records and reports relating to the implementation of the Federal Claims Collection Act (as amended), including investigative reports or administrative review matters. Individual records listed here are included in a claim file only insofar as they may be pertinent or applicable to the employee or beneficiary.[38]

86. Given the sensitive nature of these records, regulations require they be "considered confidential and may not be released, inspected, copied or otherwise disclosed" except under certain proscribed circumstances, and only if such release is consistent with the purpose for which the record was created.[39]

87. In FY 2024, over 86,000 new FECA cases were created, implicating the privacy interests of tens of thousands of federal employees.[40]

---

[38] DOL /GOVT-1.

[39] 20 C.F.R. 10.10.

[40] Office of Workers' Compensation Programs, *Federal Employees' Compensation Act (FECA) Claims Administration*, https://www.dol.gov/agencies/owcp/FECA/about (last accessed Feb. 5, 2025).

2. The Wage and Hour Division

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

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

90. The Department promises that all information shared with the Wage and Hour Division is confidential, including the complaints; the name of the complainant and the nature of the complaint.[41] Complaint information is stored in the Wage & Hour Investigative Support and Reporting Database ("WHISARD"). The Privacy Impact Assessment for WHISARD states that "The WHISARD system does not share PII information with any internal organizations" within the Department, and that "WHISARD does not share PII with any external organization."[42]

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

3. Occupational Safety and Health Administration

92. The Occupational Safety and Health Administration's mission is to assure America's workers have safe and healthful working conditions free from unlawful retaliation.

---

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

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

93. Workers are able to file complaints with OSHA about injuries, safety issues, and retaliation. They may do so with their names or as anonymous whistleblowers.

94. Workers are also interviewed by OSHA in connection with workplace safety investigations.

95. OSHA conducts interviews in private, and stores records of these interviews, including signed statements and OSHA's pledges of confidentiality in its case files.[43] Confidentiality is necessary to encourage vulnerable workers to come forward with information about their worksite and employer and to protect against retaliation. In the context of this case, disclosure of OSHA records to the leader of multiple companies with ongoing OSHA investigations presents clear risks both to workers and to the integrity of OSHA's enforcement efforts.

96. OSHA's databases include but are not limited to OSHA's Integrated Management Information Systems,[44] which houses OSHA complaints both against Tesla and against Tesla's competitors. This database makes some information regarding complaints public.[45] DOGE personnel gaining access to the non-public information contained in these complaints could provide confidential information to Mr. Musk, such as regarding a claimant's personal information, or regarding claims against his competitors.

---

[43] *See* OSHA Field Operations Manual, Ch. 3 § VII.I, https://www.osha.gov/fom/chapter-3.

[44] *See* OSHA Integrated Management Information System, https://www.osha.gov/ords/imis/establishment.html (last accessed Feb. 5, 2025).

[45] *See, e.g.*, 20 partially publicly available complaints against Tesla in 2024, *available at* https://www.osha.gov/ords/imis/establishment.search?p_logger=1&establishment=TESLA&State=all&officetype=all&Office=all&sitezip=&p_case=all&p_violations_exist=all&startmonth=01&startday=01&startyear=2024&endmonth=12&endday=31&endyear=2024 (last accessed Feb. 9, 2025).

4. *Employee Benefits Security Administration*

97. The Employee Benefits Security Administration (EBSA) regulates employee benefit plans, and undertakes enforcement activities for violations of the Employee Retirement Income Security Act of 1974 (ERISA) and related laws.[46]

98. EBSA conducts investigations into potentially improper activity in employment health pension plans, many of which are operated or sponsored by unions, and in doing so collects sensitive investigation information into its Enforcement Management System.[47]

99. EBSA does not share EMS information "with any organization external to EBSA," and "PII contained in EMS is not shared with external organizations."[48]

5. The Office of Federal Contract Compliance Programs

100. The Office of Federal Contract Compliance Programs (OFCCP) enforces compliance by federal contractors with equal employment opportunity and affirmative action laws, and other federal contract provisions.[49]

101. OFCCP relies on, in part, interviews with employees and complaints from employees to undertake its enforcement activities.[50]

---

[46] *See About EBSA*, https://www.dol.gov/agencies/ebsa/about-ebsa (last accessed Feb. 10, 2025); *Enforcement*, https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/enforcement (last accessed Feb. 10, 2025).

[47] *Privacy Impact Assessment – EBSA – Enforcement Management System (EMS)*, https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/enforcement (last accessed Feb. 10, 2025).

[48] *Id.*

[49] *Privacy Impact Assessment – OFCCP – OFCCP Information Systems*, https://www.dol.gov/agencies/oasam/centers-offices/ocio/privacy/ofccp/ofis (last accessed Feb. 11, 2025).

[50] *See* 41 C.F.R. § 60-300.60(a)(1)(ii), 60-300.61.

102. Confidentiality is crucial to OFCCP's investigations; for example, OFCCP provides that any person filing a complaint with OFCCP "may request that OFCCP keep his or her identity confidential, and OFCCP will protect the individual's confidentiality wherever that is possible given the facts and circumstances in the complaint."[51]

6. The Office of Labor-Management Standards

103. The Office of Labor-Management Standards (OLMS) administers and enforces the Labor Management Reporting and Disclosure Act, which supplies standards for democracy and fiscal responsibility in labor organizations.[52]

104. As part of its work, OLMS conducts audits and investigations of labor organizations to ensure unions are complying with their legal obligations and to investigate alleged LMRDA violations.[53]

105. Investigation files by OLMS contain sensitive information collected for law enforcement purposes, disclosure of which is tightly controlled by DOL regulations.[54]

106. Financial investigations by OLMS involve detailed audits of unions' expenditures and bank accounts.[55] Election investigations by OLMS to ensure integrity of union member

---

[51] *Id.* § 60-300.61(b)(2). *See also*, *Federal Contract Compliance Manual, 2F Interviews*, OFCCP, https://www.dol.gov/agencies/ofccp/manual/fccm/chapter-2-site-review/2f-interviews [https://web.archive.org/web/20250203092711/https://www.dol.gov/agencies/ofccp/manual/fccm/chapter-2-site-review/2f-interviews] (investigators "must inform interviewees that the interview is kept confidential to the maximum extent possible.").

[52] *See Privacy Impact Assessment – OLMS – Electronic Labor Organization Reporting system*, https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/enforcement (last accessed Feb. 10, 2025).

[53] *About OLMS*, https://www.dol.gov/agencies/olms/about (last accessed Feb. 10, 2025).

[54] *See, e.g.*, 29 C.F.R. § 71.50-52.

[55] *See, e.g.*, OLMS, *Conducting Audits in Unions – A Guide for Trustees*, https://www.dol.gov/agencies/olms/regs/compliance/union-audit-guide#fig2.

investigations involve reviews of sensitive union materials such as eligibility lists, ballots, notices, and tally sheets.[56]

7. The Bureau of Labor Statistics

107. The Bureau of Labor Statistics ("BLS") was established in 1884, with a goal of collecting and publishing disinterested information about labor markets that "could promote effective, rational, and equitable decision-making."[57]

108. 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."[58]

109. BLS is one of the "flagship" sources of statistics published by federal agencies.[59]

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

> Autonomy supports data quality directly by allowing leaders and staff to adhere to professional standards. It also supports trust in and use of the products of a statistical agency by reducing suspicions that the products have been manipulated for political purposes. Higher trust and better data quality operate in a positive feedback cycle with survey participation. And data quality and trust are necessary for people to use data products.[60]

---

[56] *See* OLMS, *LMRDA Election Investigation Profile*, https://www.dol.gov/agencies/olms/compliance-assistance/publications/lmrda-election-investigation-profile.

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

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

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

[60] *Id.* at 4.

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

112. Congress also sought to protect the collection of confidential data by statistical agencies in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA). Pub. L. No. 107-347, § 501-526, 116 Stat. 2900 (2002), *codified at* 44 U.S.C. §§ 3572-73. CIPSEA sought to use "[p]ledges of confidentiality by agencies" to "provide assurances to the public that information about individuals or organizations or provided by individuals or organizations for exclusively statistical purposes will be held in confidence and will not be used against such individuals or organizations in any agency action." 44 U.S.C. § 3571(2). As such CIPSEA provides that, among other things, "[d]ata or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent." *Id.* § 3572(c)(1). Further, disclosures may be permitted "only when the head of the agency approves such disclosure and the disclosure is not prohibited by any other law." *Id.* § 3572(c)(2).

113. BLS's independence can be a source of political angst, as it has a long tradition of releasing benchmark data on the state of the U.S. economy with minimal advance notice to political leaders at the White House before the public release.[61]

114. This is because BLS data releases often "move markets" and have other significant effects on the U.S. economy.[62]

115. When President Trump has previously taken issue with economic indicators released by BLS, he has attacked the Bureau's credibility, accusing them of "fraudulently manipulating job statistics,"[63] and calling their data "phoney."[64]

116. Political leaders may wish for a BLS that is less independent; one that, for example, is more willing to give the White House longer notice of economic data so that the President can prepare his messaging; or one that alters data to support the President's political needs.

117. A DOGE takeover of the type seen at other agencies could overturn over a century of the BLS's independence and turn it from a reliable source of data across the economy into a far less valuable political mouthpiece.

---

[61] Tucker Higgins, *Trump can spin economic numbers – but he likely can't manipulate them, experts say*, CNBC (Sep. 10, 2019), https://www.cnbc.com/2019/09/10/experts-say-trump-probably-cant-manipulate-economic-data-for-2020-bid.html.

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

[63] 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.

[64] 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.

IV. Threats to the Department of Health and Human Services

A. DOGE is currently accessing systems of records within HHS components.

118. On February 5, the same day that Plaintiffs originally filed this lawsuit, reports began emerging that DOGE employees had access to Department of Health and Human Services ("HHS") systems, including "key payment and contracting systems."[65]

119. According to some reporting, DOGE employees had been on site at HHS locations since Monday, February 3, though public reporting did not emerge until February 5.[66]

120. Mr. Musk seemingly confirmed the reporting that same day, posting a screenshot to his social media account of a Wall Street Journal headline reading "DOGE Aides Search Medicare Agency Payment Systems for Fraud," and commenting "Yeah, this is where the big money fraud is happening."[67]

121. The screenshot about which Mr. Musk commented also included commentary from another user about the headline: "The motherlode is now being tapped for the first, but not the last time. This is where the real big savings are."[68]

122. The headline is a reference to the Centers for Medicare and Medicaid Services ("CMS"), an HHS component.

---

[65] *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.

[66] *See, e.g.*, *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/ ("Sources told the WSJ DOGE employees have been on site at CMS all week.").

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

[68] *Id.*

123. On February 5, shortly after the DOGE team's presence became public, HHS leadership issued a statement indicating that two senior HHS employees "were leading the collaboration with DOGE, including ensuring appropriate access to CMS systems and technology."[69]

124. Nevertheless, that same day, public reporting indicated that DOGE employees had already requested access to systems including the Healthcare Integrated General Ledger Accounting System ("HIGLAS").[70]

125. "HIGLAS is a single, integrated dual-entry accounting system that standardizes and centralizes federal financial accounting functions for all of CMS's programs."[71] It supports CMS' major business functions and "exchanges data with other systems that are necessary to support financial management."[72] Of particular importance, it was implemented to "strengthen[]the management of Medicare accounts receivables and allow[] CMS to collect outstanding debts more timely."[73]

---

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

[70] 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/.

[71] CMS, CMS Research, Statistics, Data & Systems- Healthcare Integrated General Ledger Accounting System (HIGLAS) (Nov. 18, 2016), https://www.hhs.gov/guidance/document/cms-healthcare-integrated-general-ledger-accounting-system-higlas.

[72] CMS, HIGLAS Architecture (Sept. 10, 2024), https://www.cms.gov/about-cms/information-systems/higlas/higlas-architecture.

[73] 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).

126. DOGE has also visited the Centers for Disease Control ("CDC"), where it requested "lists of employees who have less than a year of service and those who are in two-year probationary period."[74]

127. On February 7, the DOGE account on X posted a screenshot from an HHS database showing a contract award for a project funded by the National Institutes of Health ("NIH"), which DOGE had apparently identified for cancellation, along with more than 60 other contracts.[75]

128. On February 11, Mr. Musk wrote on X that, "[a]t this point," 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."[76]

129. On information and belief, DOGE has gained or intends to gain access to systems of records at other HHS components, as well.

B. Sensitive and valuable systems within HHS.

130. HHS and its various components hold a great deal of personally identifiable information, which is subject to the Privacy Act. According to an archived snapshot of HHS's Privacy Impact Assessment database (the current website no longer appears to be functional), HHS maintains over 400 systems containing PII across the agency and its subcomponents.[77]

---

[74] Diamond et al., *supra* note 70.

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

[76] Elon Musk (@elonmusk), X (Feb. 11, 2025, 1:23 AM), https://x.com/elonmusk/status/1889198569518719122. At the time he created this post, Mr. Musk had changed the username for his X account to "Harry Bolz."

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

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.

131. Subject to certain exceptions not applicable here, HIPAA protects from disclosure "individually identifiable health information" that is "[t]ransmitted by electronic media" or "[t]ransmitted or maintained in any other form or medium." 45 C.F.R. § 160.103. In general, covered entities are "permitted to use or disclose that information 'for treatment, payment, or health care operations.'" *ACA Int'l v. Fed. Commc'ns Comm'n*, 885 F.3d 687, 712 (D.C. Cir. 2018) (quoting 45 C.F.R. § 164.506(a)).

132. All told, HHS has 11 operating divisions with more than 220 systems of records that contain sensitive and protected material.[78] Some examples of particularly relevant and sensitive systems of records follow.

1. Personal and health information for Medicare and Medicaid beneficiaries.

133. CMS maintains a number of systems containing the personally identifiable information and personal health information of Medicare and Medicaid beneficiaries.

134. With respect to Medicaid, CMS maintains systems of records containing:

a. "samples of the United States population served by programs administered by CMS and [the Social Security Administration ("SSA")]," which have the "[n]ame, social security number, Medicaid identification number, health insurance claim number, eligibility for SSA and CMS programs, and benefit

[78] *See* U.S. Dep't of Health and Human Services, HHS Systems of Records Notices (SORNs) (Apr. 11, 2023), https://www.hhs.gov/foia/privacy/sorns/index.html.

record information" of each program participant, 73 Fed. Reg. 11643, 11644 (March 4, 2008) (SORN 09-70-0512);

b. a "comprehensive database" of "enrollment, eligibility, and paid claims data about Medicaid recipients," which has the "[n]ame, address, phone number, email, address, and SSN or other identifying number" of, among other individuals, Medicaid recipients, Medicaid providers, the parents and guardians of Medicaid or CHIP recipients who are minors, 84 Fed. Reg. 2230, 2231-32 (Feb. 16, 2019) (SORN 09-70-0541); and

c. "information on Medicaid beneficiaries, and physicians and other providers involved in furnishing services to Medicaid beneficiaries," including a "Medicaid identification number, name, address, social security number (SSN), health insurance claim number (HICN), date of birth, gender, ethnicity and race, medical services, equipment, and supplies for which Medicaid reimbursement is requested, and materials used to determine amount of benefits allowable under Medicaid."[79]

135. CMS also maintains systems of records relating to Medicare beneficiaries and their providers, including some containing:

a. "Medicare hospital insurance benefits records, Part B benefits records, home health benefits records, and Medicare hospital benefits records," which includes "notices of utilization and explanation of Medicare benefits," as well as the "[n]ame; address; health insurance claims number (HIC); dates of

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

service; and the contractor assigned claim control number" for each Medicare beneficiary, 65 Fed. Reg. 48000, 48000-03 (Aug. 4, 2000) (SORN 09-70-0513);[80]

b. 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 (SNF)," as well as "Supplemental Security Income (SSI) entitlement information . . . and enrollment data on Medicare beneficiaries";[81] and

c. the "tax identification, and social security number (SSN) for each physician, non-physician practitioner and medical group" that seeks reimbursement from Medicare, as well as "information concerning a provider's birth, residence, medical education, and eligibility information for Medicare reimbursement."[82]

136. Plaintiffs have members who are beneficiaries of Medicare and, accordingly, have personally identifiable information and personal health information within the systems of records to which DOGE has been granted access.

137. Plaintiffs' members are also healthcare providers who seek reimbursement for their services from Medicare or Medicaid, which requires the disclosure of personally identifiable information and personal health information about their patients to HHS. These

[80] These records are considered by CMS to be so sensitive that "[a]ccess to all servers is controlled, . . . limited to only those support personnel with a demonstrated need for access," and servers are "kept in a locked room accessible only by specified management and system support personnel." *Id.* at 48001.

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

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

members reasonably fear that the disclosure of information to DOGE will chill their patients from candidly disclosing sensitive or even embarrassing health information, which imperils the trust that is essential to the patient-provider relationship. Cumulatively, this will impede Plaintiffs' healthcare provider members from doing their jobs to the best of their abilities.

2. Personal information about HHS employees and their family members.

138. 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, including systems containing:

a. "all records used by HHS to process and determine requests for accommodation made verbally or in writing by HHS civilian employees, HHS contractors, and HHS visitors," which includes "all records that may support a determination regarding an accommodation request," including the original request, "records describing the individual's medical conditions and the accommodation requested," a note from a treating physician, and, if the request is a religious accommodation, "records describing the individual's religious beliefs, practices, or observances," 86 Fed. Reg. 68262, 68263-64 (Dec. 1, 2021) (SORN 09-90-2103);

b. "the records of all HHS employees and their family members" who have used an Employee Assistance Program ("EAP"), as well as "the records of other Federal employees and their family members using the EAP through a

contractual agreement between HHS and their organizations," 67 Fed. Reg. 4965, 4965 (Feb. 1, 2002) (SORN 09-90-0010);[83]

c. records "about HHS personnel . . . ; current and former applicants for employment with HHS; and HHS employees' dependents, survivors, beneficiaries, and current and former spouses," which includes the following personally identifying information:

> 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).

139. Allowing unlawful access to these systems (and others) could have substantial negative effects for individual privacy, including medical privacy, as well as for agency effectiveness.

[83] "An Employee Assistance Program (EAP) is a voluntary, work-based program that offers free and confidential assessments, short-term counseling, referrals, and follow-up services to employees who have personal and/or work-related problems, . . . such as alcohol and other substance abuse, stress, grief, family problems, and psychological disorders." U.S. Office of Personnel Management, Employee Assistance Program (EAP), https://www.opm.gov/frequently-asked-questions/work-life-faq/employee-assistance-program-eap/what-is-an-employee-assistance-program-eap/ (accessed on Feb. 9, 2025).

140. Plaintiffs have members who are employed by HHS and, accordingly, have personally identifiable information within the systems of records to which DOGE has been granted access.

V. Threats to the Consumer Financial Protection Bureau

A. Recent threats to access sensitive data held by CFPB and to dismantle the agency.

141. Even before the current administration took office, Elon Musk and his associates began targeting the CFPB for dismantling.

142. Weeks after the election, Marc Andreessen, a venture capitalist and prominent supporter of the Trump campaign, used an appearance on a podcast to excoriate the CFPB as unconstitutional and dedicated to "terror[izing] financial institutions," "terrorizing anyone who tries to do anything new in financial services," and "debanking"—that is, pressuring depository institutions to cease providing services to—those whose politics the agency disagrees with.

143. In 2021, the CFPB entered into a consent agreement resolving allegations against LendUp Loans, a company that made online consumer loans, that LendUp had deceived consumers and violated the terms of a previous consent order. Marc Andreessen's venture capital firm, Andreessen Horwitz, was a prominent investor in LendUp.

144. The day after Andreessen's podcast appearance, Musk responded with a social media post stating: "Delete CFPB. There are too many duplicative regulatory agencies."

145. Musk's social media company, X, is reportedly working with Visa to launch a system for real-time electronic payments later this year.[84] The CFPB's regulatory purview

[84] Wyatte Grantham-Philips, *Elon Musk's X partners with Visa on payment service in an effort to become an 'everything app,'* AP News (Jan. 28, 2025) https://apnews.com/article/elon-musk-x-money-visa-payments-ed4538e0be2deb5fb5767ffb39ba25f3

includes electronic consumer payment systems and credit cards. *See generally* 12 U.S.C. 5481(15).

146. On Friday, February 7, DOGE came for the CFPB.

147. Following the same pattern that has played out at other agencies, three young men associated with DOGE arrived at the agency that morning and sought access to CFPB systems. Initial news reports described that they soon "gained access to internal computer systems that manage the agency's human resources, procurement, and finance systems."[85]

148. That afternoon, Musk posted on social media the words "CFPB RIP" followed by an image of a tombstone.

149. That evening, and following the same pattern as occurred as USAID, the CFPB's homepage, www.consumerfinance.gov, was replaced with the message "404: Page not found." As of the date of this filing, other parts of the CFPB's website appeared to remain functional.

150. Acting Director Vought reportedly emailed agency staff a message on February 7 stating that DOGE personnel were authorized to "begin work on all unclassified CFPB systems."[86]

151. On February 8, Acting Director Vought emailed agency staff instructing them to stop the vast majority of CFPB work.[87]

---

[85] 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.

[86] 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

[87] Philip Melanchthon Wegmann (@PhilipWegmann), X (Feb. 8, 2025, 9:07 PM ET), https://x.com/PhilipWegmann/status/1888409309937070128.

152. Later that night, Acting Director Vought announced via his own social media account that he had requested a $0 quarterly budget for CFPB operations.[88]

153. Sometime on February 8, the CFPB's official account on "X" (the social media website formerly known as Twitter) was deleted.

154. In an all-hands email, CFPB employees were also informed that the agency's "DC Headquarters Building will be closed this week (2/10-2/14)," and employees and contractors were told "to work remotely unless instructed otherwise" by Mr. Vought.[89]

B. *Sensitive and valuable systems with CFPB.*

155. Many sensitive data sources and processes are housed within the CFPB. The agency lists over 40 different systems containing personally identifiable information across its functions. Unlawful changes to these systems' (and others') access or control could have substantial negative effects, for individual privacy as well as for agency effectiveness.[90]

156. There is no public indication that Mr. Musk or DOGE personnel on leave from Mr. Musk's corporate interests will be recused from access to any of this data, which includes "hundreds of complaints about [Mr. Musk's] electric car company Tesla."[91]

157. Some examples of sensitive databases follow.

1. Consumer complaint data.

---

[88] Russell Vought (@russvought), X (Feb. 8, 2025, 10:03 PM ET), https://x.com/russvought/status/1888423503537360986.

[89] 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.

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

[91] Eric Lipton and Kirsten Grind, *Elon Musk's Business Empire Scores Benefits Under Trump Shake-up*, N.Y. Times (Feb. 11, 2025), https://www.nytimes.com/2025/02/11/us/politics/elon-musk-companies-conflicts.html.

158. Among its other functions, the CFPB collects, stores, and analyzes complaints submitted by consumers. These complaints describe consumers' experiences using a broad range of consumer products or services, from mortgages, credit cards, student loans, and credit reporting. Consumers can submit these complaints in multiple ways but do so most commonly through the CFPB's online complaint portal, https://www.consumerfinance.gov/complaint/.

159. The information consumers submit in and alongside their complaints include sensitive personal identifying information such as names, Social Security numbers, addresses, and birthdays. It also includes sensitive financial information such as bank account and routing numbers, credit card numbers, credit history and credit score, income and tax information, and information about specific purchases.

160. The CFPB has received over 10 million consumer complaints. These complaints are stored as part of a broader case-management system called the Consumer Response System.

2. Supervision, enforcement and fair lending data.

161. The CFPB's statutory responsibilities include supervising certain categories of financial institutions via on-site examinations and investigating and prosecuting violations of the laws the agency administers.

162. The Bureau collects a wide variety of sensitive and valuable information in carrying out these functions. That information includes personally 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. pt. 1070.

3. Market monitoring data

163. The CFPB also collects information to "monitor for risks to consumers in the offering or provision of consumer financial products or services, including developments in markets for such products or services." 12 U.S.C. § 5512(b)(4).

164. The CFPB is generally prohibited from disclosing information collected under this authority except in aggregate form. 1070 C.F.R. 1040 *et seq.*

165. The CFPB recently collected extensive market monitoring data about technology companies, including at least one in direct competition with business interests of Mr. Musk.[92]

166. This information includes details about product monetization and data harvesting, access to which would allow Mr. Musk to learn otherwise unavailable information about the operations of a competitor.[93]

4. Home Mortgage Disclosure Act (HMDA) Data

167. The Home Mortgage Disclosure Act (HMDA) requires certain financial institutions to collect, record, report, and disclose information about their mortgage lending

[92] Consumer Financial Protection Bureau, Newsroom, *CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans* (Oct. 21, 2021), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-tech-giants-to-turn-over-information-on-their-payment-system-plans/ (Facebook among recipients of market monitoring orders).

[93] Consumer Financial Protection Bureau, *ORDER TO FILE INFORMATION ON PAYMENTS PRODUCTS* (Oct. 21, 2021), https://files.consumerfinance.gov/f/documents/cfpb_section-1022_generic-order_2021-10.pdf

information. Covered financial institutions file their HMDA data with the CFPB using the HMDA Platform, a web-based data submission system.

168. CFPB makes available this data to the public. The CFPB describes its HMDA data as "the most comprehensive source of publicly available information on the U.S. mortgage market."

169. 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. The public data are modified to protect applicant and borrower privacy.

HARMS TO PLAINTIFFS

170. Plaintiffs are numerous unions, AFL-CIO, AFGE, AFSMCE, SEIU, CWA, and AFT, collectively representing millions of members, as well as EPI, VPLC, and EAMF.

C. Harms to AFL-CIO.

171. Plaintiff AFL-CIO includes 63 labor organizations and over 13 million members.

172. AFL-CIO and its member organizations routinely bring complaints and claims under the Fair Labor Standards Act and the Occupational Safety and Health Act to the Department of Labor. These claims are brought on behalf of vulnerable workers, who, without the Department of Labor's assistance, would be deprived of even minimum wage and safe working conditions.

173. AFL-CIO and its member organizations are only able to bring such claims due to the confidentiality guaranteed by the Department of Labor. Indeed, this confidentiality is essential to workers' decisions to come forward.

174. AFL-CIO and its member organizations also assist members when participating in workplace safety investigations by OSHA. OSHA regularly interviews employees at workplaces

with safety concerns, and represents to employees that their statements will be kept confidential. This confidentiality is crucial to allowing workers to speak frankly about potentially unsafe conditions without fear of retaliation by their employers. These statements are stored in OSHA's investigation files.

175. Should Defendants or their associates improperly access and/or disseminate the confidential information in Department of Labor's data systems, that would cause irreparable injury to the AFL-CIO, its member organizations, and its members. The individuals who confidentially provided information to DOL about violations of labor laws will be likely be irreparably harmed including facing employment retaliation, for providing this information to DOL, and others will be chilled from making such complaints in the future.

176. Affiliates of the AFL-CIO also routinely submit claims on behalf of their members under the Black Lung Benefits Act, administered by the Department of Labor. These claims include sensitive medical, personal, and financial information. AFL-CIO, its affiliates, and their members will be irreparably harmed if this sensitive information is improperly accessed and/or disseminated, including by being chilled from making such claims in the future.

177. Plaintiff AFL-CIO and it affiliate unions also sponsor, often jointly with employers, employee benefit plans subject to ERISA, and those plans have responded to investigations by EBSA. Those plans provide both health and retirement benefits to union employees and members. Over the course of those investigations, EBSA has collected a wide range of sensitive information about union employees and members, including names, addresses, social security numbers, earnings data, and personal health records. The AFL-CIO, its affiliates, and their members will be irreparably harmed if this sensitive information is improperly accessed and/or disseminated.

178. Plaintiff AFL-CIO and its member unions are also regularly subject to audit, and occasionally investigation, by DOL OLMS. In the course of these proceedings, OLMS collects and confidentially stores in investigation files sensitive financial and membership information on the unions in question. The disclosure of these records would irreparably harm AFL-CIO, its affiliates, and its members, by providing protected information to unions' negotiating counterparties and by disclosing PII of its members.

A. Harms to AFGE.

179. Plaintiff AFGE represents over 800,000 federal and D.C. government workers, including workers at DOL and HHS.

180. These employees' sensitive personnel information, including employment information (such as social security numbers, tax forms such as W-2, banking information for payment purposes, and similar) are stored in DOL and HHS data systems.

181. These employees face irreparable harm to their privacy interests if this information is improperly accessed or disseminated (such as by being downloaded to a private server). Once the information is improperly accessed and/or disseminated, recovery may be difficult, and information may already have been used for impermissible purposes.

182. These employees, like any federal employee, may be injured on the job and therefore entitled to workers' compensation. In such instances, they must file claims with the Department of Labor through the Federal Employees' Compensation Act Claims Administration. These claims include sensitive personal information such as medical records, including about injuries, illness, prognosis, long-term effects of an injury, medical appointments and treatment plans. These claims also include sensitive personal information such as financial information, regarding costs, benefits, taxes, and similar. AFGE assists members in filing for these claims including approximately 1,500 such claims in 2024.

183. AFGE and its members will be irreparably harmed if this sensitive private information, including medical information, financial information, and personnel information, is improperly accessed and or/disseminated.

184. AFGE members who are employees at the Department of Labor have also been ordered to violate the law by granting access to sensitive systems in violation of the Privacy Act, FISMA, CISPEA, the APA, and other statutes. At least one of these statutory schemes, the Privacy Act, creates individual civil and criminal liability for employees who violate the law with the requisite degree of knowledge. AFGE members will be irreparably harmed by being exposed to criminal and civil liability if they violate the law on the orders of Department officials or DOGE personnel.

185. In addition, AFGE members will be chilled from exercising their rights to seek workers' compensation for injuries on the job if their private information, reported confidentially as part of their workers' compensation claims, is released publicly. AFGE and its members have a significant interest in multiple categories of records maintained by DOL, including records of a sensitive nature which would harm AFGE and its members if disclosed. As the chief enforcement entity of many labor statutes for which it has both investigative and prosecutorial authority, DOL conducts investigations, and maintains sensitive records in connection therewith, regarding a wide range of matters involving AFGE, including but not limited to employer violations of AFGE members' rights in the areas of wage and hour law, occupational safety and health, and more. DOL's Employment and Training Administration is the top federal agency overseeing the nation's Unemployment Insurance system, which provides critical benefits (involving sensitive beneficiary information) to AFGE members.

B. Harms to AFSCME.

186. AFSCME is the largest trade union of public employees in the United States, with around 1.4 million members organized into approximately 3,400 local unions, 58 councils and affiliates in 46 states, the District of Columbia and Puerto Rico.

187. AFSCME represents many healthcare providers, including through its affiliate, United Nurses Association of California/Union of Health Care Professionals, which represents over 40,000 nurses and other healthcare professionals. AFSCME represents public and private sector physicians through its affiliate, United Association of Physicians and Dentists ("UAPD"). Over 100,000 AFSCME members, represented through its affiliated United Domestic Workers, provide Medicaid-funded in-home support services to Medicaid beneficiaries.

188. The AFSCME members who work in healthcare and treat patients with Medicare or Medicaid are required to submit certain personally identifiable information to HHS as part of the reimbursement process. Those members also transmit a great deal of personally identifiable information and personal health information about their patients to HHS and understand that maintaining privacy over those records is of paramount importance to the trust that is essential to the patient-provider relationships that underpin their work. HHS' decision to allow access to DOGE-affiliated personnel undercuts that trust and risks disrupting the patient-provider relationships that are important to AFSCME's members.

C. Harms to SEIU.

189. Plaintiff SEIU represents approximately 2 million members in healthcare, the public sector, and property services, and has over 150 affiliates across the United States, Canada, and Puerto Rico.

190. SEIU regularly assists and supports its members in filing numerous legal complaints with the Department of Labor, including under the Fair Labor Standards Act and the Occupational Safety and Health Act.

191. For example, SEIU recently filed a complaint against Waffle House for violations of the Fair Labor Standards Act.

192. SEIU, and its affiliate unions and members, relies on the guarantee that the Department of Labor will keep the identity of complainants confidential. Many workers would not otherwise report violations due to legitimate fears of employer retaliation.

193. Should the confidential information in Department of Labor's data systems be improperly accessed and/or disseminated, that would cause irreparable injury to SEIU, its affiliate unions, and its members, including but not limited to the workers involved in the Waffle House complaint. The individuals who made complaints, their personal information and the details of the complaints that make them identifiable, will likely be irreparably harmed including facing the risk of employment retaliation for making such claims.

194. Others will be chilled from making such complaints in the future. Indeed, DOGE's access to other government systems has been broadly publicized and therefore if they gain unlawful access to Department of Labor systems even for a short period of time it will cause devastating, irreparable harm to SEIU, its members, and its affiliate unions. Even the mere threat of unauthorized disclosure effects harms to existing complainants and chills other workers from vindicating their rights.

195. SEIU is also invested in HHS' stewardship of the sensitive personal and health information it maintains.

196. SEIU represents approximately one million members who work in the healthcare industry, including in health systems and nursing homes, and who provide in-home care for elderly and disabled individuals. SEIU's members include doctors, nurses, home care and nursing home workers, lab technicians, environmental service workers, dietary aides and certified nursing assistants—all of whom work on the frontlines of care in our communities.

197. A critical part of SEIU's mission is our advocacy for broad access to healthcare, including advocacy in support of government programs such as the Medicare and Medicaid programs. For over 20 years, SEIU has led healthcare advocacy efforts in cities, states, and the federal government. SEIU members have drafted and delivered petitions to Congress, made millions of calls to Congress, hosted town halls with elected officials, and submitted tens of thousands of comments to regulatory agencies including the Department of Health and Human Services ("HHS") and its sub-agencies. Specifically, SEIU leaders and members have engaged in advocacy in support of healthcare access in the following areas: passage of the Affordable Care Act, increased access to services funded by Medicaid, including advocating for expansion of Medicare coverage to include vision and dental care, long-term care benefits, and lowering the eligibility age; Medicare Advantage program reform efforts; prescription drug reform; expanded Medicaid funding and workforce standards for Medicaid Home- and Community-Based Services programs; and improved staffing regulations in acute care and nursing home facilities.

198. The privacy and confidentiality of Medicare beneficiaries' data is an important component of SEIU's healthcare advocacy efforts. SEIU's membership includes approximately 197,000 members who are over 65 years old and are assumed to be, and in many cases are confirmed to be, Medicare beneficiaries. This is approximately 10% of SEIU's total membership.

199. SEIU's members rely on privacy and confidentiality protections to be able to access quality healthcare and see improved health outcomes, which is central to SEIU's mission. SEIU believes that all healthcare decisions should be between the healthcare provider and the patient. HHS' decision to recklessly grant access to its databases, which contain personal information and medical billing information, puts this fundamental tenet of healthcare at risk.

200. Maintaining the confidentiality of personal health information of SEIU members who are Medicare beneficiaries is important to SEIU. SEIU's members, many of whom are both healthcare workers and Medicare beneficiaries, place a high value on the privacy of their personal healthcare information and have an expectation that it will be maintained in a confidential manner. They understand that medical privacy is the cornerstone of quality patient care, which leads to improved health outcomes and a high quality of life for SEIU's members and working people.

201. HHS' failure to safeguard the personal and health information of SEIU's members will also chill some members from having candid discussions with their providers, which will result in less effective and informed care, including preventive care. That will, in turn, undermine SEIU's efforts to secure quality healthcare for our members.

202. SEIU members also include approximately 500,000 members who provide in-home care services funded by the Medicaid program. Those members have personally identifiable information in HHS systems of records related to their participation in state Medicaid programs as individual providers, including their name, date of birth and their national provider identifier. They likewise rely on the confidentiality, privacy, and security protections provided by HHS.

D. Harms to CWA.

203. Plaintiff CWA—which represents workers across industries including telecommunications, airlines, education, and healthcare—has filed numerous complaints with Department of Labor divisions and sub-agencies in recent years and has helped its members participate in subsequent investigations in its efforts to maintain minimum industry standards. For example, CWA files third-party complaints with the Department of Labor's Wage and Hour Division on behalf of workers alleging violations under the Service Contract Act. CWA also helps their members file complaints with the Occupational Safety and Health Administration and collect supporting documentation. And CWA helps their members file complaints with the Office of Federal Contract Compliance Programs to help counter discrimination.

204. CWA members rely on assurances of confidentiality when submitting these complaints to the Department of Labor, which include personal identifying information. These workers often fear retaliation from their employers. CWA's ability to make assurances of the Department's confidentiality policies is important to CWA members who submit information to the Department and CWA in conducting its work helping them to do so. The privacy interests of these employees and CWA's ability to continue encouraging them to report labor law violations are imperiled by DOGE access to Department Records. Encouraging employees to report without confidentiality assurances would require CWA to divert legal and organizing staff time away from other CWA work, such as supporting other campaigns to form a union and to obtain collective bargaining agreements. It could also impact CWA's membership, as its work and victories on labor violations are often a driver of membership.

205. CWA itself submits confidential information to the Department's Office of Labor-Management Standards (OLMS) based on complaints members file with OLMS alleging that CWA or one of its locals has infringed upon rights protected by the Labor Management

Reporting and Disclosure Act (LMRDA). The disclosure of sensitive information of the type provided in OLMS investigations to DOGE has the ability to harm CWA reputationally, and, in turn, impact its organizing abilities.

206. CWA members also submit claims to DOL's Office of Federal Contract Compliance Programs (OFCCP) to ensure that employers who are federal contractors follow applicable antidiscrimination laws and regulations.

207. During OFCCP investigations, OFCCP collects information on reporting employees and builds investigation files to aid in enforcement of federal laws. Confidentiality of the information OFCCP collects is of utmost importance to allow employees to report discrimination and violations of their rights without fear of retaliation and reprisal.

208. If OFCCP investigation files were to be disclosed, CWA members who have reported discrimination would suffer irreparable harm by being faced with risk of retaliation. And CWA and its members would be harmed by the weakening of OFCCP's ability to enforce federal civil rights laws that would result from no longer being able to rely on confidential reporting as a tool to vindicate workers' rights.

209. CWA also represents healthcare providers, including doctors, who rely on promises of confidentiality to conduct their work. These members often obtain sensitive information, including information protected by HIPAA, under the promise that it will remain confidential. And these members work in places, such as hospitals, that submit this sensitive information to HHS—for example in the form of information submitted to CMS for insurance reimbursements or to the Health Resources and Services Administration for transplants. The assurances these members make encourages patients to be as transparent with these medical

provider members as possible and allows these members to do their jobs to the best of their abilities.

210. If HHS files were to be disclosed, it would hamper the ability of CWA members to do their jobs and harm CWA's mission to ensure its members, including its health-care worker members, are able to operate most effectively.

E. Harm to AFT.

211. AFT represents nearly two million members in education, whose interests touch each of the Defendant Agencies' operations. AFT advocates for the safety, fair treatment, and opportunities for its members.

212. AFT works to secure safe workplaces for its members, including, as necessary, working with members to submit complaints to OSHA and cooperate with OSHA's workplace safety investigations. Confidentiality in OSHA's complaint and investigation processes is critical to protecting AFT members' identities and facilitating effective resolution of workplace safety investigations.

213. Breaches of OSHA data by exposing sensitive data systems to DOGE would irreparably harm AFT's members who provided confidential information to OSHA, exposing them to a threat of retaliation, and weaken OSHA's ability to protect the interests of AFT's members, by weakening the credibility of their pledge of confidentiality and making it more difficult for them to collect comprehensive, actionable information on workplace safety concerns.

214. AFT represents 490,000 members who are retirees, many of whom receive benefits under Medicare.

215. Maintaining the confidentiality of personal health information of AFT members who are Medicare beneficiaries is important to AFT. AFT members have an expectation that

personal healthcare information will be maintained in a confidential manner, and in a manner that facilitates candid discussions between members and their healthcare providers.

216. AFT actively works to secure quality healthcare for its members, and that work (and the wellbeing of AFT's members) will be negatively impacted if the promise of patient and health record confidentiality is breached, resulting in less informed and less effective care.

217. AFT also advocates for the financial well-being of its members, including how to protect themselves from unreliable or abusive lending practices. AFT relies, in part, on data collected by CFPB to understand the scale of consumer financial problems facing its members and educate its members about how to make an impact.[94] If CFPB's public complaint database, which contains redacted information from confidential consumer complaints, were to be compromised by a breach of confidentiality, consumers will be less likely to submit complaints to the CFPB, and its data will be less useful to AFT in advocating for its members' interests.

F. Harm to EPI.

218. EPI is a non-profit organization with over 35 years of experience analyzing the effects of economic policy on the lives of working people in the United States. EPI research intentionally centers on low- and middle-income working families in economic policy discussions at the federal, state, and local levels, ensuring every worker has access to a good job with fair pay, affordable health care, retirement security, and a union. EPI research and analysis is grounded in data, including public government data from the Bureau of Labor Statistics, Bureau of Economic Analysis, and U.S. Census. EPI is concerned that the federal government

[94] *See, e.g.*, *The MOHELA Papers: The Rise of a Student Loan Servicing Giant and the Fall of the Student Loan System*, Student Borrower Protection Center & AFT 1, 12 (Feb. 2024), https://www.mohelapapers.org/_files/ugd/588c1d_3a7d1b423b2b44a7a9844942002471f5.pdf (joint report on loan servicer's mismanagement of Public Service Loan Forgiveness program, relying in part on a review of "nearly 3,000 complaints" received and published by CFPB).

produces, and the general public have access to, quality and accurate data to help inform economic policy making decisions.

219. Plaintiffs' missions are also all deeply intertwined with the Department's operations. Plaintiffs rely on the Department and its programs to ensure fair treatment of American workers. Were Defendants permitted to allow DOGE to wreak the sort of rapid, arbitrary, and ill-considered fundamental changes to the Department's work, responsibilities, and personnel that it has at other agencies, Plaintiffs, their members, and the communities they serve would be gravely impacted.

G. Harm to VPLC and EAMF

220. Plaintiffs Virginia Poverty Law Center (VPLC) and Economic Action Maryland Fund (EAMF) will be directly harmed by the improper access and/or dissemination of sensitive and confidential information held by Defendant Consumer Financial Protection Bureau (CFPB).

221. Such information includes millions of consumer complaints about financial products and services submitted to CFPB and held in a system of records known as the Consumer Response System. Consumer complaints housed in the Consumer Response System frequently contain personal identifying information and sensitive financial information, including Social Security numbers and account numbers. Consumers submit complaints to CFPB with the expectation that this information will be protected from unlawful disclosure.

222. VPLC and EAMF each provide direct services to consumers experiencing difficulties with financial products and services, from mortgages to debt collection to predatory loans. The consumer complaint system provides an irreplaceable tool for VPLC and EAMF to help these consumers find solutions. Filing a complaint with CFPB takes minutes and costs nothing, but can deliver concrete results for consumers in need. Both VPLC and EAMF direct consumers seeking help to file complaints with the CFPB.

223. If the integrity of the complaint system were compromised, or if the system were taken down entirely, VPLC and EAMF would not be able to recommend that consumers submit complaints that may contain confidential personal and financial data. They would also no longer be able to rely on the information currently provided by the public complaint database, a system CFPB uses to make public redacted versions of consumer complaints, for consumers who opt in when filing a complaint.

224. VPLC and EAMF rely on the public complaint database, as well as other data the CFPB makes public, to carry out their direct services work as well as other core parts of their missions. They would be directly harmed if these resources were taken down or the integrity of the data stored in CFPB systems of records were compromised.

225. The additional time and resources that VPLC and EAMF would be required to devote to providing direct assistance to consumers and to understand emerging problems in the market would necessarily increase without the CFPB complaint system and other CFPB resources. That in turn would require shifting money and resources from the other core missions of VPLC and EAMF.

CLAIMS FOR RELIEF

COUNT ONE
Ultra Vires
(Defendants U.S. DOGE Service and U.S. DOGE Service Temporary Organization)

226. Plaintiffs reallege and incorporate by reference the paragraphs written above.

227. DOGE is purely a creation of executive order; no statute directed or contemplated its existence.

228. DOGE's limited functions are to advise and assist the President; it is not empowered to perform any other functions.

229. DOGE has no authority in law to direct operations or decisions at government agencies. Despite this, as alleged above, DOGE personnel have directed operations and decisions—including some operations that appear to be contrary to law—at multiple agencies thus far, including Defendants' agencies.

230. On information and belief, DOGE personnel have directed DOL employees to provide them with access to DOL systems or information from those systems, and DOL leadership have directed DOL employees to grant such access.

231. CFPB leadership have also granted DOGE personnel access to all unclassified CFPB systems.

232. DOGE personnel have also been granted access to various sensitive systems at HHS and have further directed agency staff to compile targeted individualized personnel information, likely in order to direct staff reductions.

233. DOGE does not have authority to direct DOL, CFPB, or HHS officials to grant DOGE personnel access to sensitive systems at DOL, CFPB, or HHS. Any directions to agency officials to grant them access are *ultra vires*.

234. DOGE also has no authority in law to access or alter restricted-access systems at federal agencies, even if access was granted by officials who are lawfully serving DOL, CFPB, or HHS officials.

235. Likewise, DOGE has no authority to enter into inter-agency personnel agreements with DOL, CFPB, or HHS. Any such agreements are *ultra vires* and have no legal force or effect. In particular, any such agreements cannot convert DOGE personnel into employees of DOL, CFPB, or HHS or otherwise confer on DOGE authority to either compel authorization to access records systems or to access those systems at DOL, CFPB, or HHS.

236. On information and belief, DOGE personnel will also direct employment actions and agency restructuring in order to effectuate DOGE's operational policy objectives at DOL, CFPB, and HHS. Such directions are also *ultra vires*.

COUNT TWO
Administrative Procedure Act, 5 U.S.C. § 706(2)(A), (C), (D)
(Defendant Department of Labor)

237. Plaintiffs reallege and incorporate by reference the paragraphs written above.

238. DOL has instructed employees to "provide access to any DOL system they requested access to and not to worry about any security protocols" and indicated that failure to comply with this directive will result in adverse employment actions, including termination.

239. This directive establishes a Department of Labor policy regarding the terms of DOGE's access to Department of Labor systems and records (the "DOL DOGE Access Policy"), which constitutes a final agency action that has caused injuries to Plaintiffs that have no other adequate remedy in a court. Accordingly, relief is available under the Administrative Procedure Act. 5 U.S.C. §§ 702, 704.

240. The DOL DOGE Access Policy is contrary to multiple legal requirements and fails to demonstrate reasoned agency decisionmaking.

241. The DOL DOGE Access Policy is inconsistent with the Privacy Act, which prohibits disclosure of records from systems of records absent certain conditions. 5 U.S.C. § 552a(b). Disclosure from DOL's systems of records to DOGE personnel would not meet any of the conditions enumerated in 5 U.S.C. § 552a(b), and would therefore be inconsistent with the Privacy Act. Although the Privacy Act provides a cause of action for money damages where an agency's noncompliance has "an adverse effect on an individual," *see* 5 U.S.C. § 552a(g)(1)(D), such relief is not available to Plaintiffs or, if it is, will not provide complete relief for their

injuries, which are caused by the Department of Labor's unlawful policy and the ongoing unlawful access the DOL DOGE Access Policy permits.

242. The DOL DOGE Access Policy also includes an instruction by DOL to its employees that is inconsistent with 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."

243. The DOL DOGE Access Policy also 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). On information and belief, DOGE personnel are likely to demand access to BLS data and, pursuant to the DOL DOGE Access Policy, Department of Labor employees have been instructed to comply with that demand or face termination, notwithstanding that doing so would violate CISPEA.

244. The DOL DOGE Access Policy is further inconsistent with 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 access [or] use" of information or information systems maintained by the agency. 44 U.S.C. § 3554(a)(1)(A). On information and belief, the DOL DOGE Access Policy authorizes access without requiring the protections mandated by FISMA.

245. The DOL DOGE Access Policy is further inconsistent with established Department of Labor confidentiality requirements for various sets of sensitive data, including requirements set forth in regulation. *See, e.g.* 20 C.F.R. 10.10 (FECA) ("All records relating to

claims for benefits, including copies of such records maintained by an employer, are considered confidential and may not be released, inspected, copied or otherwise disclosed except as provided in the Freedom of Information Act and the Privacy Act of 1974 or under the routine uses provided by DOL/GOVT-1 if such release is consistent with the purpose for which the record was created.").

246. The DOL DOGE Access Rule also fails to consider many "important aspects of the problem" it purports to solve. *See Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). Among other things, it fails to consider the impact of such unfettered access on the privacy interests of DOL and other federal employees in their health and benefits information, in workers compensation claims held by the agency, and the significant potential to chill reporting of wage and hour or OSHA violations. It also failed to account for the reliance interests of federal employees and workers everywhere who have provided the Department of Labor with confidential personal information with the expectation that such information would be protected.

247. The DOL DOGE Access Rule also failed to consider whether authorizing access to DOGE personnel, who have a close relationship with Mr. Musk, would allow Mr. Musk to improperly access complaints against Mr. Musk's companies or information related to active Department of Labor investigations into Mr. Musk's companies. For example, 20 OSHA complaints regarding Tesla were filed with the Department in 2024 alone.[95] Providing access to that sensitive data to Mr. Musk and DOGE personnel with ties to Mr. Musk's corporate interests,

[95] *See* https://www.osha.gov/ords/imis/establishment.search?p_logger=1&establishment=TESLA&State=all&officetype=all&Office=all&sitezip=&p_case=all&p_violations_exist=all&startmonth=01&startday=01&startyear=2024&endmonth=12&endday=31&endyear=2024

as well as access to confidential complaints and investigations regarding his competitors, would undermine and conflict with relevant standards for labor investigations, as well as ethics laws, including 18 U.S.C. § 208(a).

248. The DOL DOGE Access Policy has also effectively revoked pre-existing Department of Labor policies and regulations governing disclosure of sensitive DOL records and information, including under FECA. *See, e.g.*, 20 C.F.R. 10.10. The DOL DOGE Access Policy made these substantial and legally significant changes without affording "interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments," 5 U.S.C. § 553(c), when affording notice-and-comment was legally required.

249. For these reasons, the DOL DOGE Access Policy is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," *id.* § 706(2)(A); "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.* § 706(2)(C); and was established "without observance of procedure required by law," *id.* § 706(2)(D). It should, accordingly, be held unlawful and "set aside." *Id.* § 706(2).

COUNT THREE
Administrative Procedure Act, 5 U.S.C. § 706(2)(A), (C), (D)
(Defendant Consumer Financial Protection Bureau)

250. Plaintiffs reallege and incorporate by reference the paragraphs written above.

251. As described above, CFPB has changed its disclosure rules to allow for DOGE staff to access, at a minimum, all unclassified information systems within the CFPB. These changes constitute a CFPB policy governing DOGE's access to CFPB systems and records (the "CFPB DOGE Access Policy"). The CFPB DOGE Access Policy constitutes final agency action, which constitutes a final agency action that has caused injuries to Plaintiffs that have no other

adequate remedy in a court. Accordingly, relief is available under the Administrative Procedure Act. 5 U.S.C. §§ 702, 704.

252. The CFPB DOGE Access Policy is contrary to multiple legal requirements.

253. The CFPB DOGE Access Policy is inconsistent with the Privacy Act, which prohibits disclosure of records from systems of records absent certain conditions. 5 U.S.C. § 552a(b). Disclosure from CFPB's systems of records to DOGE personnel would not meet any of the conditions enumerated in 5 U.S.C. § 552a(b), and would therefore be inconsistent with the Privacy Act. Although the Privacy Act provides a cause of action for money damages where an agency's noncompliance has "an adverse effect on an individual," *see* 5 U.S.C. § 552a(g)(1)(D), such relief is not available to Plaintiffs or, if it is, will not provide complete relief for their injuries, which are caused by CFPB's unlawful policy and the ongoing unlawful access the CFPB DOGE Access Policy permits.

254. The CFPB DOGE Access Policy is also inconsistent with 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). On information and belief, the CFPB DOGE Access Policy authorizes access without requiring the protections mandated by FISMA.

255. The CFPB DOGE Access Policy also conflicts with CFPB restrictions on disclosure of sensitive data, which were previously set 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.").

256. The CFPB DOGE Access Policy effectively revokes these preexisting CFPB regulations governing disclosure of CFPB information. *See, e.g.*, 12 C.F.R. § 1070.59; *id.*§ 1070.40 *et seq.*; *id.*§ 1070.4. CFPB made these substantial and legally significant changes without affording "interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments," 5 U.S.C. § 553(c), when affording notice-and-comment was legally required.

257. For these reasons, the CFPB DOGE Access Policy is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," *id.* § 706(2)(A); "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.* § 706(2)(C); and was established "without observance of procedure required by law," *id.* § 706(2)(D). It should, accordingly, be held unlawful and "set aside." *Id.* § 706(2).

COUNT FOUR
Administrative Procedure Act, 5 U.S.C. § 706(2)(A), (C), (D)
(Defendant Department of Health and Human Services)

258. HHS has similarly adopted a policy governing its authorization of DOGE personnel to access sensitive HHS systems and records (the "HHS DOGE Access Policy"), which constitutes a final agency action that has caused injuries to Plaintiffs that have no other adequate remedy in a court. Accordingly, relief is available under the Administrative Procedure Act. 5 U.S.C. §§ 702, 704.

259. The HHS DOGE Access Policy is contrary to multiple legal requirements.

260. The HHS DOGE Access Policy is inconsistent with the Privacy Act, which prohibits disclosure of records from systems of records absent certain conditions. 5 U.S.C. §

552a(b). Disclosure from HHS's systems of records to DOGE personnel would not meet any of the conditions enumerated in 5 U.S.C. § 552a(b), and would therefore be inconsistent with the Privacy Act. Although the Privacy Act provides a cause of action for money damages where an agency's noncompliance has "an adverse effect on an individual," *see* 5 U.S.C. § 552a(g)(1)(D), such relief is not available to Plaintiffs or, if it is, will not provide complete relief for their injuries, which are caused by HHS's unlawful policy and the ongoing unlawful access the HHS DOGE Access Policy permits.

261. The HHS DOGE Access Policy is also inconsistent with 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). On information and belief, the CFPB DOGE Access Policy authorizes access without requiring the protections mandated by FISMA.

262. The HHS DOGE Access Policy is also inconsistent with HHS regulations implementing the Privacy Act, 45 C.F.R. § 5b, and HIPAA, which applies to the many records at HHS that contain personal health information, *see* 45 C.F.R. § 160.103.

263. By establishing a policy that flatly contradicts with these preexisting regulations, HHS has effectively revoked or altered applicable policies and regulations, without the opportunity for notice and comment, which was required. *See* 5 U.S.C. § 553(c).

264. For these reasons, the HHS DOGE Access Policy is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," *id.* § 706(2)(A); "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.* § 706(2)(C); and

was established "without observance of procedure required by law," *id.* § 706(2)(D). It should, accordingly, be held unlawful and "set aside." *Id.* § 706(2).

COUNT FIVE
Violations of the Privacy Act, 5 U.S.C. § 552a(b)
(Defendants DOL, CFPB, HHS, and DOGE)

265. Plaintiffs reallege and incorporate by reference the paragraphs written above.

266. The Privacy Act, 5 U.S.C. § 552a(b), prohibits disclosure of records from systems of records absent certain conditions.

267. Disclosure from Defendants' systems of records to DOGE personnel would not meet any of the conditions enumerated in 5 U.S.C. § 552a(b), and would therefore be inconsistent with the Privacy Act.

268. 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).

269. Accordingly, and alternatively, Plaintiffs are entitled to relief under the Privacy Act for the injuries described above stemming from unauthorized disclosures by Defendants DOL, CFPB, HHS, and DOGE.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

270. Declare that the decisions by DOL, HHS, and CFPB (collectively, "Agency Defendants") to authorize DOGE personnel to access agency systems and records containing sensitive information are unlawful;

271. Enjoin Agency Defendants from granting DOGE personnel access to their systems and records, except as consistent with applicable law.

272. Direct DOGE personnel to immediately return or destroy all copies of material unlawfully accessed from agency systems and records;

273. Direct Agency Defendants to remove any software installed by DOGE personnel on agency systems;

274. Enjoin Agency Defendants from taking adverse personnel actions against any employee who shields Agency Defendant systems or records from unauthorized disclosure to DOGE;

275. Enjoin Agency Defendants from providing non-public information or access to such information to any person with a personal or financial interest in that non-public information;

276. Enjoin DOGE from exercising any *ultra vires* authority with respect to Agency Defendants;

277. Grant appropriate temporary, preliminary, or permanent injunctive relief to prevent Defendants DOGE and its employees or agents from accessing, disclosing, or retaining Agency Defendants' information in violation of law, installing software on Agency Defendants' systems, or from exercising *ultra vires* authority with respect to Agency Defendants;

278. Award Plaintiffs their costs, reasonable attorneys' fees, and any other disbursements as appropriate; and

279. Grant any other relief this Court deems appropriate.

Dated: February 11, 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

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