UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO,

ASSOCIATION OF ADMINISTRATIVE LAW JUDGES, INTERNATIONAL FEDERATION OF PROFESSIONAL AND TECHNICAL ENGINEERS JUDICIAL COUNCIL 1, AFL-CIO,

VANESSA BARROW, GEORGE JONES, DEBORAH TOUSSANT, and DOES 1–100,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT, an agency of the United States,

CHARLES EZELL, in his official capacity as Acting Director of the Office of Personnel Management,

U.S. DOGE SERVICE f/k/a U.S. DIGITAL SERVICE,

ACTING U.S. DOGE ADMINISTRATOR,

U.S. DOGE TEMPORARY SERVICE a/k/a the "DEPARTMENT OF GOVERNMENT EFFICIENCY," and

ELON MUSK, in his capacity as director of the U.S. DOGE TEMPORARY SERVICE,

Defendants.

Case No. _____-cv-_____

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

NATURE OF THE ACTION AND RELIEF SOUGHT

1. Plaintiffs, current and former employees of the United States government and unions acting on behalf of employees of the United States government, bring this action against

Defendants U.S. Office of Personnel Management ("OPM"), an agency of the United States, and Charles Ezell, in his official capacity as Acting Director of OPM (together, the "OPM Defendants"), as well as Defendants the U.S. DOGE Service f/k/a Digital Service ("USDS"), the unidentified Acting Director of USDS, the U.S. DOGE Service Temporary Organization a/k/a the "Department of Government Efficiency" ("DOGE"), and Elon Musk, in his capacity as director of the USDTSO (collectively, the "DOGE Defendants"). Plaintiffs seek declaratory and injunctive relief to halt OPM Defendants' unlawful, systematic, wholesale, continuous, and ongoing disclosure of Plaintiffs' and their members' sensitive personal data to DOGE Defendants and their agents, including to Elon Musk or to any other person.

2. Defendant OPM maintains, under strict disclosure and accounting protocols prescribed by the Privacy Act of 1974, 5 U.S.C. § 552a (the "Privacy Act"), the highly sensitive personal and employment information of tens of millions of current and former federal employees, contractors, and job applicants. Those records include: identifying information like name, birthdate, home address and phone number, and social security number; demographic information like race/ethnicity, national origin, and disability; education and training information; employment information like work experience, union activities, salaries, performance, and demotions; personal health records and information regarding life insurance and health benefits; financial information like death-benefit designations and savings programs; classified-information nondisclosure agreements; and information concerning family members and other third parties referenced in background checks and health records. OPM also maintains information on employees in highly sensitive roles for whom even acknowledging their government employment may be problematic. For example, the CIA recently sent an unclassified email listing the first name and last initial of employees hired by the CIA in the last

two years.[1]

3. Donald J. Trump was inaugurated as President on January 20, 2025. The same day, he issued an executive order titled "Establishing and Implementing the President's "Department of Government Efficiency" (the "Executive Order"). Under the Executive Order, the United States Digital Service was renamed the United States DOGE Service, and a "temporary organization" was established under 5 U.S.C. § 3161 entitled "the U.S. DOGE Service Temporary Organization."

4. Under the Executive Order, the USDS and DOGE were established in the Executive Office of the President. USDS was previously part of the Office of Management and Budget.

5. The Executive Order directs the USDS Administrator to "work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." It also directs agency heads to "take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems." The Executive Order claims to "displace[] all prior executive orders and regulations, insofar as they are subject to direct presidential amendment, that might serve as a barrier to providing USDS access to agency records and systems as described above."

6. During the presidential campaign, President Trump announced that his top campaign donor, billionaire entrepreneur Elon Musk, would be a director of DOGE. It is widely reported that, since the inauguration, Musk has played the top leadership role in DOGE activities

[1] https://www.nytimes.com/2025/02/05/us/politics/cia-names-list.html.

across the federal government, and that currently he purportedly serves as a "special government employee."[2] The Trump administration has not publicly revealed the employment status of other individuals who are part of DOGE.

7. On information and belief, Musk and other DOGE actors were not government employees at the time they demanded and received access to the OPM computer networks containing Plaintiffs' and their members' personal information.

8. In violation of the Privacy Act, on or about January 20, 2025, OPM Defendants gave unrestricted, wholesale access to OPM systems and records to DOGE Defendants and DOGE's agents, including Musk, Akash Bobba, Luke Farritor, Gautier Cole Killian, Gavin Kliger, Ethan Shaotran, and Edward Coristine. Coristine is a 19-year-old who is now widely known by his online identity "Big Balls" and who, according to the *New York Times*, was fired from cybersecurity firm Path Network in 2022 following (according to a recent firm statement) "an internal investigation into the leaking of proprietary information that coincided with his tenure."[3]

9. OPM Defendants gave DOGE Defendants and DOGE's agents—many of whom are under the age of 25 and are or were until recently employees of Musk's private companies—"administrative" access to OPM computer systems, without undergoing any normal, rigorous national-security vetting. As the *Washington Post* reported, that level of access gives DOGE Defendants "sweeping authority to install and modify software on government-supplied equipment and, according to two OPM officials, to alter internal documentation of their own

[2] https://www.nytimes.com/2025/02/03/us/politics/musk-federal-government.html
[3] https://www.nytimes.com/2025/02/07/us/politics/musk-doge-aides.html

activities."[4]

10. The Privacy Act makes it unlawful for OPM Defendants to hand over access to OPM's millions of personnel records to DOGE Defendants, who lack a lawful and legitimate need for such access. No exception to the Privacy Act covers DOGE Defendants' access to records held by OPM. OPM Defendants' action granting DOGE Defendants full, continuing, and ongoing access to OPM's systems and files for an unspecified period means that tens of millions of federal-government employees, retirees, contractors, job applicants, and impacted family members and other third parties have no assurance that their information will receive the protection that federal law affords.

11. DOGE Defendants have exceeded the scope of their legal authority by accessing and controlling OPM systems. These *ultra vires* actions have resulted in unlawful disclosure of the contents of these systems and endangered the security of the information they contain.

12. Plaintiffs bring this action to put an immediate stop to Defendants' systematic, continuous, ongoing, wholesale violation of federal laws that protect the privacy of the highly sensitive personal information contained in OPM's systems about tens of millions of American public servants, job applicants, their family members, and other third parties.

JURISDICTION AND VENUE

13. This Court has statutory jurisdiction over this action under 28 U.S.C. § 1331 because this action arises under the laws of the United States, namely, the Privacy Act, 5 U.S.C. § 552a, and the Administrative Procedure Act (APA), 5 U.S.C. §§ 702, 706.

14. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b)(2) and (e)(1).

[4] https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/

Plaintiffs are or act on behalf of residents of this judicial district, and a substantial part of the events or omissions giving rise to this complaint occurred and are continuing to occur within the Southern District of New York.

PARTIES

15. Plaintiffs American Federation of Government Employees, AFL-CIO ("AFGE") and Association of Administrative Law Judges, International Federation of Professional and Technical Engineers Judicial Council 1, AFL-CIO ("AALJ") represent current employees and contractors of the U.S. government whose sensitive personal and employment information was included in the OPM data that Defendant OPM disclosed and continues to disclose.

16. Plaintiff AFGE is a labor organization and unincorporated association that represents approximately 800,000 federal civilian employees through its affiliated councils and locals who reside in every state in the United States, including in New York and in this judicial district. AFGE members include nurses caring for our nation's veterans, border patrol agents securing our borders, correctional officers maintaining safety in federal facilities, scientists conducting critical research, health care workers serving on military bases, civilian employees in the Department of Defense supporting our military personnel and their families, and employees of the Social Security Administration making sure retirees receive the benefits they have earned.

17. Plaintiff AALJ is a labor organization and unincorporated association that represents approximately 910 Administrative Law Judges engaged in adjudication at the Social Security Administration. AALJ's headquarters are located in Purchase, New York, and AALJ represents members residing throughout the United States, including in this judicial district.

18. Plaintiff Vanessa Barrow is an employee of the Brooklyn Veterans Affairs Medical Center who resides in Nassau County, New York. As a federal employee since

September 2008, Ms. Barrow's sensitive personal and employment information was included in the OPM records that Defendants disclosed and continue to disclose.

19. Plaintiff George Jones is President of AFGE Local 2094 and a former employee of VA New York Harbor Healthcare who resides in Bronx County, New York. As a former federal employee, Mr. Jones' sensitive personal and employment information was included in the OPM records that Defendants disclosed and continue to disclose.

20. Plaintiff Deborah Toussant is a former federal employee who resides in New York County, New York. As a former federal employee, Ms. Toussant's sensitive personal and employment information was included in the OPM records that Defendants disclosed and continue to disclose.

21. Plaintiffs Does 1–100 are, like the named plaintiffs, current and former employees or contractors of the United States government.

22. Defendant U.S. Office of Personnel Management (OPM) is an agency of the United States, headquartered in Washington, D.C.

23. Defendant Charles Ezell is the Acting Director of OPM.

24. Defendant U.S. Digital Service, also known as the United States DOGE Service, is a subcomponent of the Executive Office of the President and an agency within the meaning of 5 U.S.C. § 701(b)(1).

25. Defendant Acting U.S. DOGE Service Administrator is the head of the USDS.

26. Defendant U.S. DOGE Service Temporary Organization is a subcomponent of the USDS and a subcomponent of the Executive Office of the President.

27. Defendant Elon Musk is the apparent director of the U.S. DOGE Service Temporary Organization.

FACTUAL ALLEGATIONS

28. Plaintiffs and their members are current and former federal employees who work in a wide variety of positions in every state and the District of Columbia as well as overseas. Plaintiffs and their members who are actively working must have their highly sensitive personal and employment information stored by Defendant OPM to receive their salaries and wages from their federal employment, while retirees must do so to receive their pension benefits.

29. On January 20, 2025, OPM Defendants gave at least six DOGE agents broad access to all personnel systems at OPM, and access to others a week later, according to the *Washington Post*, which further reported, "The DOGE team's demand for access to OPM files and networks came as Musk deputies arrived at the agency promising to wipe out 70 percent of its staff."[5]

30. Systems to which DOGE Defendants gained access include the Enterprise Human Resources Integration; Electronic Official Personnel Folder; USAJOBS; USA Staffing; USA Performance; and Health Insurance (which houses information about the Federal Employee Health Benefits (FEHB) program and the Postal Service Health Benefit (PSHB) program), according to the newsletter Musk Watch.[6]

31. As the *Washington Post* has reported, OPM Defendants' illegal disclosure of personnel records to DOGE is vast:

> The data that the DOGE team can access includes a massive trove of personal information for millions of federal employees, included in systems called Enterprise Human Resources Integration and Electronic Official Personnel Folder. It also includes personal information for anyone who applied to a federal job through the site USAJobs, the people said. Last year alone, the people said, there were 24.5 million such applicants.

[5] https://wapo.st/3WNsOik
[6] https://www.muskwatch.com/p/musk-associates-given-unfettered

> The two OPM officials said the level of access granted to DOGE agents means they could copy the Social Security numbers, phone numbers and personnel files for millions of federal employees.
>
> "They could put a new file in someone's record; they could modify an existing record," one said. "They could delete that record out of the database. They could export all that data about people who are currently or formerly employed by the government, they could export it to some nongovernment server, or to their own PC, or to a Google Drive. Or to a foreign country."[7]

32. The *Washington Post* reported on February 6, 2025, that the "disruptions [by DOGE] at the OPM, Treasury and other agencies have raised concerns among U.S. security officials and experts that Russia, China, Iran and other adversaries could seek to exploit the chaos by launching new cyber intrusions or targeting the devices and communications of Musk's team."[8] Those concerns are well founded: a previous cyberattack on OPM databases was attributed to hackers working for the Chinese government.[9]

33. Concerns about unauthorized parties seeking access to OPM data are exacerbated by the facts that DOGE agents have not received security clearance through a normal process, and that at least one of those agents has previously been fired from private employment in connection with disclosure of his employer's secrets (which means he would not have passed a normal security-clearance vetting). Indeed, as the *Washington Post* has reported, although the Trump administration "has suggested that members of the DOGE team have the authority to review sensitive government files," the administration has also "refused to provide details about whether security clearances have been issued." [10]

---

[7] https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/
[8] *Id.*
[9] https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html
[10] https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/

34. While a report suggests that OPM Defendants might have recently issued directives that DOGE agents should be withdrawn from two OPM systems,[11] those directives are not public, have not been confirmed by OPM itself, and it is unclear if any such directives were followed. Moreover, DOGE Defendants' access to other systems with personal data has not been revoked, and DOGE Defendants might retain personal data from the reportedly revoked systems.

35. The Privacy Act strictly protects personal information from improper disclosure and misuse, including by barring disclosure to other agencies within the federal government and individuals who lack a lawful and legitimate need for it. OPM Defendants are not permitted to give access to that information to other persons or agencies unless granting that access fits within one of the Privacy Act's enumerated exceptions.

36. OPM Defendants have given DOGE Defendants access to OPM data without obtaining or asking for the consent of affected individuals.

37. DOGE Defendants have no lawful need under the Privacy Act for the records that OPM Defendants have released to them.

38. While the Privacy Act lists other exceptions justifying disclosure, such as for law-enforcement purposes, none apply here.

39. Plaintiffs and their members reasonably fear that, unless Defendants are enjoined, Plaintiffs' and their members' information may be further disclosed to or used by DOGE Defendants and other unauthorized parties.

40. Plaintiffs and their members also reasonably fear harmful consequences of the disclosure and use of that information. President Trump, DOGE director Elon Musk, and others

[11] https://www.washingtonpost.com/nation/2025/02/08/doge-opm-musk/

have repeatedly threatened to fire government employees they view as disloyal. They have repeatedly and unlawfully purported to fire government employees and shutter entire departments. And they have affirmatively put in place policies that seek to terminate government employees based on their gender identity.[12] OPM Defendants' unlawful disclosure of Plaintiffs' personal information to DOGE Defendants puts Plaintiffs' and their members' job security at risk.

41. OPM Defendants' unlawful disclosure of Plaintiffs' and their members' personal information to DOGE Defendants also puts Plaintiffs' and their members' health and safety at risk. For example, some Plaintiffs or their members work or worked in fields where public disclosure of their identifying and other information could lead to retaliation from people who oppose their agency's work. Other Plaintiffs or their members regularly work abroad in countries where knowledge of their identifying information could be used to harm them or to threaten or extort them.

42. Finally, OPM Defendants' unlawful disclosure of Plaintiffs' and their members' personal information to DOGE Defendants puts Plaintiffs' and their members' financial security at risk. Any new and untested protocols, technologies, and personnel, especially without sufficient security safeguards, expose Plaintiffs' and their members' personal identifying information to new threats of hacking by criminals and foreign governments.

43. Given the sensitivity of the information improperly disclosed to DOGE Defendants, which could be used for identity theft, intimidation, harassment, or physical harm, some Plaintiffs or their members have purchased credit-monitoring services and web-monitoring

[12] https://www.military.com/daily-news/2025/01/28/trump-orders-pentagon-policy-saying-transgender-troops-are-not-consistent-military-ideals.html

services to protect themselves. Their concerns are not without precedent. The OPM data breach disclosed in 2015 affected 22.1 million people, leading to identity theft and fraud.

44. OPM Defendants' disclosure of Plaintiffs' and their members' information to DOGE Defendants was not an accident but was deliberate and willful.

45. OPM Defendants' violations of the Privacy Act also give rise to this case under the Administrative Procedure Act, which directs courts to hold unlawful and set aside agency actions that are not in accordance with law. 5 U.S.C. § 706(2)(A).

46. On information and belief, OPM Defendants continue to disclose Plaintiffs' and their members' personal information to DOGE Defendants in ongoing violation of the Privacy Act. On information and belief, DOGE Defendants continue to possess and use Plaintiffs' confidential information in ongoing violation of the Privacy Act.

FIRST CLAIM FOR RELIEF
(Violations of the Privacy Act of 1974, 5 U.S.C. § 552a(b))

47. Plaintiffs incorporate by reference the allegations in each of the preceding paragraphs as if fully set forth in this paragraph.

48. OPM Defendants have disclosed and are disclosing Plaintiffs' and their members' records to DOGE Defendants without consent from Plaintiffs or their members. Through their actions, OPM Defendants have intentionally and willfully violated the Privacy Act.

49. OPM Defendants have disclosed and are disclosing records on Plaintiffs and their members to DOGE Defendants, who do not have a need for the records in the performance of any lawful duty they may have at OPM or elsewhere in the federal government.

50. On information and belief, OPM Defendants have done so with full awareness that DOGE Defendants did not have a lawful basis to access that information.

51. On information and belief, DOGE Defendants have caused or induced the

unlawful disclosure of Plaintiffs' and their members' data to DOGE Defendants and are acting in concert with OPM Defendants to cause them to violate the Privacy Act.

52. Defendants' intentional and willful disclosures are ongoing and continuous.

53. Plaintiffs and their members have sustained and will continue to sustain actual damages and pecuniary losses directly traceable to Defendants' violations set forth above. Plaintiffs and their members are entitled to damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

54. Plaintiffs and their members will be irreparably injured by continuing disclosure of their information and by the use and disclosure of their information outside lawful channels in the absence of an injunction prohibiting further disclosure of their information, prohibiting use of information already obtained unlawfully, and requiring return or destruction of any copies of their personal information maintained by DOGE Defendants.

SECOND CLAIM FOR RELIEF
(Violation of the Privacy Act, 5 U.S.C. § 552a(e)(10))

55. Plaintiffs incorporate by reference the allegations in each of the preceding paragraphs as if fully set forth in this paragraph.

56. Section 552a(e)(10) of the Privacy Act, 5 U.S.C. § 552a(e)(10), requires any agency of the federal government that maintains records containing individuals' personal data to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

57. OPM Defendants have not established appropriate "administrative, technical, and physical safeguards" to ensure the security and confidentiality of the records that they have allowed DOGE Defendants to access and/or collect from OPM.

58. DOGE Defendants do not maintain public security policies; neither OPM Defendants nor DOGE Defendants provided security training to DOGE's agents before OPM gave them access to OPM's records; and neither OPM Defendants nor DOGE Defendants properly vetted DOGE agents before OPM Defendants gave them access to OPM's Records. It was and continues to be unlawful for OPM Defendants to permit DOGE Defendants to have access to OPM data.

59. Defendants' intentional and willful violations of federal law continue. Defendants have failed to undertake compulsory security precautions to safeguard Plaintiffs' and their members' sensitive information.

THIRD CLAIM FOR RELIEF
(Under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), for Violations of the Privacy Act)

60. Plaintiffs incorporate by reference the allegations in each of the preceding paragraphs as if fully set forth in this paragraph.

61. The Administrative Procedure Act directs courts to hold unlawful and set aside agency actions that are found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. 5 U.S.C. § 706(2)(A).

62. OPM Defendants have disclosed and are disclosing Plaintiffs' and their members' records to DOGE Defendants in violation of the Privacy Act, 5 U.S.C. § 552a(b).

63. OPM Defendants have allowed DOGE Defendants to access, collect, and maintain records from OPM that are not "relevant and necessary" to accomplish any lawful purpose, in violation of the Privacy Act, 5 U.S.C. § 552a(e)(1).

64. OPM Defendants have not established appropriate "administrative, technical, and physical safeguards" for the records they have allowed DOGE Defendants to access and/or

collect from OPM, in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10).

65. OPM Defendants' actions violate the prohibitions in the Privacy Act and are thus contrary to law. OPM Defendants' actions are "final agency action[s] for which there is no other adequate remedy in a court." 5 U.S.C. § 704. OPM Defendants' actions therefore are "subject to judicial review." *Id*. § 702.

66. The Federal Information Security Management Act (FISMA) makes the head of each agency, including Defendant Ezell, responsible for providing information security protections and ensuring that agency officials take steps to reduce the risk of unauthorized use of information in the agency's possession. 44 U.S.C. § 3554. FISMA further provides that each agency head, including Defendant Ezell, is responsible for complying with the requirements of the statute and pertinent information technology policies, procedures, standards, and guidelines established by appropriate authorities, such as executive orders on cybersecurity and standards promulgated by the National Institute of Standards and Technology (NIST). 44 U.S.C. § 3554(a)(1)(B). Defendant Ezell did not comply with the statutory requirements or the policies, procedures, and guidelines established by the relevant authorities.

67. On information and belief, DOGE Defendants and those acting under their purported authority have caused or induced the unlawful disclosure of Plaintiffs' and their members' data to DOGE Defendants and are acting in concert with OPM Defendants to cause it to violate the Privacy Act.

68. Defendants' intentional and willful violations of federal law are ongoing and continuous.

69. Plaintiffs and their members have sustained and will continue to sustain actual damages and pecuniary losses directly traceable to Defendants' violations set forth above.

70. Plaintiffs and their members will be irreparably injured by continuing disclosure of their information and by the continued use and disclosure of their information outside lawful channels in the absence of an injunction prohibiting further disclosure of their information, prohibiting use of information already obtained unlawfully, and requiring return or destruction of any copies of their personal information maintained by DOGE Defendants.

FOURTH CLAIM FOR RELIEF
(Against OPM Defendants Under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), for Arbitrary and Capricious Action)

71. Plaintiffs incorporate by reference the allegations in each of the preceding paragraphs as if fully set forth in this paragraph.

72. The Administrative Procedure Act directs courts to hold unlawful and set aside agency actions that are found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. 5 U.S.C. § 706(2)(A).

73. Agency action is arbitrary and capricious when an agency fails to engage in reasoned decision-making when it adopts or alters its policies.

74. OPM Defendants failed to engage in reasoned decision-making when they implemented a system under which DOGE Defendants could access OPM's records for purposes other than those authorized by the Privacy Act. In particular, OPM Defendants failed to consider their legal obligations under federal law, the harm that their actions would cause to the objectives that those statutes sought to achieve, or the harm caused to Plaintiffs and their members.

75. OPM Defendant's actions are final agency action for which there is no other adequate remedy in a court and therefore are subject to judicial review. *Id*. § 704; *see id*. § 702.

FIFTH CLAIM FOR RELIEF
(*Ultra Vires* Actions by DOGE Defendants)

76. Plaintiffs incorporate by reference the allegations in each of the preceding

paragraphs as if fully set forth in this paragraph.

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

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

79. DOGE has no authority in law to direct operations or decisions at government agencies.

80. In directing and controlling the use and administration of Defendant OPM's systems, as alleged above, DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of Americans.

81. DOGE Defendants may not take actions that are not authorized by law.

82. No law or other authority authorizes or permits DOGE Defendants to access or administer OPM systems.

83. Through such conduct, DOGE Defendants have engaged and continue to engage in *ultra vires* actions that violate federal laws and injure Plaintiffs and their members by violating their constitutional rights, exposing their private information, and increasing the risk of further disclosure of their information.

84. Plaintiffs and their members will be irreparably injured by DOGE Defendants' *ultra vires* actions in the absence of an injunction prohibiting further accessing of their information, prohibiting use of information already unlawfully obtained, and requiring return or destruction of any copies of their personal information maintained by DOGE Defendants.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

A. Declare to be unlawful OPM Defendants' decision to implement a system by which DOGE Defendants may access OPM's records and obtain personal information about individuals contained therein;

B. Enjoin Defendants from continuing to permit such access or obtain such personal information or to make any use of the information they have illegally obtained;

C. Enjoin Defendants to ensure that future disclosure of individual records will occur only in accordance with the Privacy Act and the Administrative Procedure Act;

D. Grant any temporary, preliminary, or permanent injunctive relief necessary to protect the privacy of individuals whose information is contained within OPM's system of records;

E. Order the impoundment and destruction of all copies of individuals' personal information that has been unlawfully disclosed;

F. Award Plaintiffs their costs and attorneys' fees for this action, as mandated by statute, 5 U.S.C. §552a(g)(4)(B); and

G. Grant such other and further relief as the Court deems just and proper.

Dated: February 11, 2025

Respectfully submitted,

/s/ Rhett O. Millsaps II

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

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

Norman L. Eisen*
STATE DEMOCRACY DEFENDERS FUND
600 Pennsylvania Avenue SE #15180
Washington, DC 20003

Subodh Chandra*
THE CHANDRA LAW FIRM LLC
The Chandra Law Building
1265 W. 6th Street, Suite 400
Cleveland, OH 44113

*pro hac vice application forthcoming

Counsel for Plaintiffs