IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

ELECTRONIC PRIVACY INFORMATION CENTER;
1519 New Hampshire Avenue, N.W.
Washington, D.C. 20036

DOE 1

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT
1900 E Street NW
Washington, D.C. 20415

CHARLES EZELL, in his official capacity as Acting Director of the Office of Personnel Management
1900 E Street NW
Washington, D.C. 20415

U.S. OFFICE OF PERSONNEL MANAGEMENT DOGE TEAM
1900 E Street NW
Washington, D.C. 20415

U.S. DEPARTMENT OF THE TREASURY
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

SCOTT BESSENT, in his official capacity as Secretary of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

U.S. DEPARTMENT OF THE TREASURY DOGE TEAM
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

U.S. DOGE SERVICE
736 Jackson Place NW
Washington, D.C. 20503

No. 1:25-cv-00255-RDA-WBP

U.S. DOGE SERVICE TEMPORARY ORGANIZATION
736 Jackson Place NW
Washington, D.C. 20503

AMY GLEASON, in her purported official capacity as Acting Administrator of the U.S. DOGE Service and U.S. DOGE Service Temporary Organization
736 Jackson Place NW
Washington, D.C. 20503

ELON MUSK, in his official capacity as leader of DOGE
1650 17th Street NW
Washington, DC 20006

STEVE DAVIS, in his official capacity as Chief Operating Officer of DOGE
736 Jackson Place NW
Washington, D.C. 20503

GENERAL SERVICES ADMINISTRATION
1800 F Street NW
Washington, D.C. 20405

STEPHEN EHIKIAN, in his official capacity as Acting Administrator of the General Services Administration
1800 F Street NW
Washington, D.C. 20405

Defendants.

**AMENDED COMPLAINT FOR DAMAGES,
INJUNCTIVE RELIEF, AND DECLARATORY RELIEF**

1. This action arises from the largest and most consequential data breach in U.S. history, currently ongoing at numerous federal agencies, including the U.S. Department of the Treasury and U.S. Office of Personnel Management. This unprecedented breach of privacy and security implicates the personally identifiable information ("PII") of tens of millions of people, including nearly all federal employees and millions of members of the American public.

2. Treasury and OPM are the legal custodians of these extraordinarily sensitive records —records that should only be accessed for specific and limited purposes, by only those agency employees whose roles require such access and who are appropriately trained. For decades, these agencies have upheld the law and worked to safeguard American's privacy.

3. Since January 20 of this year, however, Treasury and OPM have turned Americans' data over to a network of outsiders with very different priorities. To that network, DOGE, privacy obligations are meaningless; accordingly, federal agencies' protections come a distant second to the enactment of DOGE's Agenda throughout the government.

4. Yet Treasury and OPM have deliberately provided DOGE with unlawful access to sensitive and protected data and have allowed those data to be used for legally prohibited purposes. These basic security failures have resulted in the unlawful disclosure of personal data—including social security numbers and tax information—belonging to tens of millions of individuals stored in Bureau of Fiscal Service ("BFS") systems and the unlawful disclosure of personal data belonging to millions of federal employees and others stored in Enterprise Human Resources Integration ("EHRI").

5. Treasury and OPM's decisions to welcome DOGE into American's data are and were unlawful. These agencies have decided not to abide by legally required safeguards to

protect the information within their systems, to the detriment of the millions of Americans who rely on these agencies to keep their data safe.

6. DOGE has, through agency DOGE Teams and otherwise, exceeded the scope of its legal authority by accessing and controlling OPM and Treasury systems. These *ultra vires* actions have resulted in unlawful disclosure and use of the PII contained within these systems, violated Plaintiffs' constitutional right to informational privacy and endangered the security of the information they contain.

7. Plaintiffs seek injunctive relief curing Government Defendants' unlawful failure to secure PII contained in the EHRI system and BFS payment systems; halting all Defendants' unlawful use of such systems for impermissible purposes or without required information security safeguards; and halting the unlawful disclosure and computer matching of sensitive PII. Plaintiffs seek injunctive and/or mandamus relief halting the DOGE Teams' unlawful, *ultra vires* direction of the use and administration of the EHRI, USAJobs, USA Staffing, USA Performance – Office of the Director, and eOPF systems at OPM; and BFS payment systems at Treasury.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, 5 U.S.C. § 704, 5 U.S.C. § 552a(g)(5), 26 U.S.C. § 7431(a)(1), and 28 U.S.C. § 1361.

9. Venue is proper in this district because Plaintiff Doe 1 resides in this District. 28 U.S.C. § 1391(e)(1).

10. Venue is proper in the Alexandria division because Plaintiff Doe 1 resides within the Alexandria division as described in Local Rule 3(B)(1).

PARTIES

11. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities that impact individual privacy. EPIC is a membership organization. An individual member of EPIC is any person who contributes to the advancement of the mission of EPIC, who acts in accordance with the core values and policies of EPIC, and who has been recognized and registered as a member by EPIC, by virtue of payment of annual dues or having been granted a dues waiver. This includes members of EPIC's Advisory Board, who are distinguished experts in law, technology, and public policy.

12. Doe 1 is a current federal employee of an agency subject to U.S. Code Title 5.

13. Defendant U.S. Office of Personnel Management is an agency within the meaning of 5 U.S.C. § 701(b)(1), 5 U.S.C. § 552a(a)(1), and 5 U.S.C. § 552(f). It serves as the "home" agency for a number of DOGE Affiliates and regularly details these individuals to other federal agencies in order to carry out the DOGE Agenda.

14. Defendant Charles Ezell is the Acting Director of the U.S. Office of Personnel Management and an officer or employee of the United States within the meaning of 26 U.S.C. § 7431. He is sued in his official capacity.

15. Defendant OPM DOGE Team is the group of employees identified by Defendant Ezell pursuant to Executive Order 14158 § 3(c). They are sued as an entity.

16. Defendant U.S. Department of the Treasury is an agency within the meaning of 5 U.S.C. § 701(b)(1), 5 U.S.C. § 552a(a)(1), and 5 U.S.C. § 552(f).

17. Defendant Scott Bessent is the Secretary of the Treasury and an officer or employee of the United States within the meaning of 26 U.S.C. § 7431. He is sued in his official capacity.[1]

18. Defendant Treasury DOGE Team is the group of employees identified by Defendant Bessent pursuant to Executive Order 14158 § 3(c). They are sued as an entity.

19. 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).

20. Defendant U.S. DOGE Service Temporary Organization is a subcomponent of the USDS, a subcomponent of the Executive Office of the President, and an agency within the meaning of 5 U.S.C. § 701(b)(1).

21. Defendant Amy Gleason is purported to be the Acting U.S. Digital Service Administrator (for both USDS and the USDSTO).

22. Defendant Elon Musk is putatively a Special Government Employee, serving as Senior Advisor to the President in the Executive Office of the President, and is the *de facto* head of DOGE.

23. Defendant Steve Davis is a Senior Advisor in the United States Digital Service, and is the *de facto* Chief Operating Officer and second-in-command of DOGE.

24. Defendant General Services Administration is an agency within the meaning of 5 U.S.C. § 701(b)(1), 5 U.S.C. § 552a(a)(1), and 5 U.S.C. § 552(f). It serves as the "home" agency

[1] Defendants OPM, Director Ezell, Treasury, and Secretary Bessent are collectively referred to as "Defendant Agencies."

for a number of DOGE Affiliates and regularly details these individuals to other federal agencies in order to carry out the DOGE Agenda.

25. Defendant Stephen Ehikian is the Acting Administrator of the General Services Administration and an officer or employee of the United States within the meaning of 26 U.S.C. § 7431. He is sued in his official capacity.

Legal Framework

Laws Governing Federal Information Privacy

26. Government information systems are subject to comprehensive privacy and information security protections.

27. 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, *id*. § 3554(a)(1)(A).

28. The Privacy Act of 1974, 5 U.S.C. § 552a, prohibits disclosure of information from systems of records except in enumerated circumstances.

29. The Privacy Act further requires that, when an agency establishes or revises a system of records, it must issue a System of Records Notice (SORN), which discloses information about the records in the system, the manners in which those records may assertedly be used, and storage and access policies. 5 U.S.C. § 552a(e)(4).

30. The E-Government Act of 2002, Pub. L. 107-347, requires that agencies conduct a privacy impact assessment for new or substantially changed information technology which contains certain records. Privacy act assessments are intended to "demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a

system." *E-Government Act of 2002*, Department of Justice: Office of Privacy and Civil Liberties, https://www.justice.gov/opcl/e-government-act-2002.

31. Federal agencies are also subject to standards and guidance developed by the National Institute of Standards and Technology ("NIST"). NIST develops and implements "standards to be used by all agencies to categorize all information and information systems" in order to "provid[e] appropriate levels of information security according to a range of risk levels" and "minimum information security requirements for information and information systems." 15 U.S.C. § 278g–3(b)(1). The Secretary of Commerce is further empowered to make those standards "compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems." 40 U.S.C. § 11331.

32. Those mandatory standards for Federal information systems can be found in NIST Special Publication 800-53. NIST SP-800-53, *Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce: National Institute of Standards and Technology (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. The standards require that when federal agencies process personally identifiable information, they must abide by information security and privacy programs designed to manage the security risks for the PII in the system. *Id.* at 13.

33. The Internal Revenue Code, 26 U.S.C. § 6103, provides that "[r]eturns and return information shall be confidential" and prohibits the disclosure and use of this information by United States employees and other defined persons, except as specifically authorized by statute. This protection is an essential component of the due process granted to taxpayers by the Government. Indeed, the IRS has made the right of confidentiality core to its "The Taxpayer Bill

of Rights." This "general ban on disclosure provides essential protection for the taxpayer; it guarantees that the sometimes sensitive or otherwise personal information in a return will be guarded from persons not directly engaged in processing or inspecting the return for tax administration purposes. The assurance of privacy secured by § 6103 is fundamental to a tax system that relies upon self-reporting." *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000).

34. Taxpayers have a private right of action to seek damages under 26 U.S.C. § 7431 for the knowing or negligent unauthorized inspection or disclosure of returns or return information in violation of 26 U.S.C. § 6103.

35. The term "disclosure" means "the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8).

36. The term "return" is broadly defined to include "any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed." 26 U.S.C. 6103(b)(1).

37. Records of tax payments and tax deposits are tax return information under 26 U.S.C. § 6103.

The Administrative Procedure Act

38. 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).

FACTS

The "Department of Government Efficiency"

39. On November 12, 2024, then-President-Elect Trump announced the creation of the "Department of Government Efficiency" ("DOGE"). At the time, President-Elect Trump said that DOGE would not be a formal part of the government. Instead, DOGE was to be created to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget," to "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[2]

40. 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 ("USDS"), established in the Executive Office of the President.[3]

41. The E.O. established the role of USDS Administrator in the Executive Office of the President, reporting to the White House Chief of Staff.[4]

42. The E.O. further established within USDS a temporary organization known as "the U.S. DOGE Service Temporary Organization." The U.S. DOGE Service Temporary

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

Organization is headed by the USDS Administrator and is tasked with advancing "the President's 18-month DOGE agenda."[5]

43. The E.O. also requires each Agency Head to establish a "DOGE Team" comprised of at least four employees within their respective agencies. DOGE Teams are required to "coordinate their work with [U.S. DOGE Service] and advise their respective Agency Heads on implementing the President's DOGE Agenda."[6]

44. The E.O. instructed the USDS Administrator to "commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems."[7] The Administrator must work with Agency Heads to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization."[8]

45. The E.O. further requires 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."[9] The E.O. nominally directs USDS (but not DOGE or DOGE Teams more generally) to adhere to "rigorous data protection standards."[10]

The Current Structure of DOGE

46. As currently constituted, DOGE is a network of individuals located at GSA, OPM, and USDSTO and embedded at agencies throughout the federal government. Although the group is spread across multiple agencies, and some DOGE employees hold concurrent positions

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

at more than one agency, the network remains centrally controlled and its work remains directed by DOGE leadership.

47. Of the USDS Defendants, USDS is largely made up of legacy United States Digital Service employees, who are still carrying out the original United States Digital Service mission.

48. The putative Acting Administrator of USDS, Amy Gleason, oversees the work of those legacy employees.

49. The legacy USDS employees are not primarily responsible for implementation of the President's "DOGE Agenda"—the rapid dismantling of federal agencies, evisceration of the federal workforce, and consolidation of sensitive data.

50. Instead, the individuals who are known publicly and within federal agencies as "DOGE," and tasked with implementing the DOGE Agenda, are formally spread across a number of different government entities.

51. First, the other half of the USDS Defendants—the USDSTO—is largely made up of individuals new to government since January 20, 2025, and who are either employed by or detailed to USDSTO. Unlike the legacy USDS entity, USDSTO hosts individuals who play a meaningful role in supporting or carrying out the DOGE Agenda across federal agencies.

52. The two other "home bases" for DOGE are Defendants GSA and OPM, who formally employ most of the individuals responsible for carrying out the President's "DOGE Agenda" government-wide. Many of these individuals are concurrently detailed to or dual-employed by other federal agencies as members of those agencies' DOGE Teams.

53. In addition to the employees at USDSTO, GSA, and OPM, a small number of individuals who are primarily responsible for carrying out the President's DOGE Agenda are directly employed by host agencies.

54. This network of personnel tasked with carrying out the President's DOGE Agenda, with partially overlapping employment by USDSTO, OPM, GSA, and host agencies, can collectively be referred to as "DOGE" or "DOGE Affiliates." They are responsible for unlawful system seizures, unlawful agency closures or partial closures, and unlawful grant and contract terminations. On information and belief, all members of DOGE take instruction from and coordinate their work through central DOGE leadership.

55. Small groups of DOGE Affiliates within federal agencies operate as DOGE Teams—DOGE personnel on the ground within agencies to effectuate the DOGE Agenda.

56. DOGE receives overall direction and leadership from Elon Musk, a Senior Advisor within the White House.

57. Day-to-day leadership and oversight of DOGE Teams is undertaken by Steve Davis, who is both a Senior Advisor in the USDTO and a detailee from USDSTO to Defendant GSA.

58. DOGE Team members formally assume titles as employees of or detailees to those agencies; however, DOGE Team members do not serve as normal agency employees or detailees. They are there to carry out an externally imposed agenda coordinated by DOGE leaders outside their host agencies.

59. DOGE Team members work for DOGE and functionally are DOGE employees, even when their formal employment relationships are with their host agencies or other non-USDS entities.

60. On information and belief, the following individuals are, or have been, among the members of the Treasury DOGE Team since Inauguration: Baris Akis, Sam Corcos, Marko Elez, Thomas Krause, Aram Moghaddassi, and Ryan Wunderly.

61. On information and belief, the following individuals are, or have been, among the members of the OPM DOGE Team since Inauguration: Riccardo Biasini, Akash Bobba, Edward Coristine, Gavin Kliger, Nikhil Rajpal, and Amanda Scales.[11]

The Seizure, Breach, and Misuse of Key Federal Information Systems

62. Beginning on Inauguration Day, DOGE sought and obtained unprecedented access to information systems across numerous federal agencies, including the Department of Treasury and the Office of Personnel Management.[12]

63. Under normal circumstances, these systems and the information contained therein are carefully protected by, *inter alia*, rigorous information security protocols mandated by FISMA, robust privacy protections established by the Privacy Act of 1974, and careful supervision by trained agency personnel.

64. Yet at the direction and insistence of DOGE, Defendant Agencies have abandoned these safeguards, relinquishing control of systems and, without legal basis, disclosing vast stores of PII to individuals unauthorized by law to access them, including but not limited to USDS/DOGE personnel.

---

[11] Numerous other individuals known or believed to be working for DOGE are formally affiliated with OPM in some capacity, but, on information and belief, may not have performed DOGE work internally at OPM. In addition to Defendant Steve Davis, those individuals include: Jacob Altik, Baris Akis, Anthony Armstrong, Brian Bjelde, Stephen Duarte, Joe Gebbia, Christiana Hanna, Stephanie Holmes, Scott Kupor, Jeremy Lewin, Tarak Makecha, Bryanne-Michelle Mlodzianowski, Justin Monroe, Noah Peters, Austin Raynor, and Christopher Young.

[12] 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/.

65. Individuals affiliated with or acting at the urging of DOGE connected hard drives and at least one server to these critical systems. On information and belief, these devices were not compliant with FISMA or other applicable privacy and security requirements, introducing substantial vulnerabilities to these systems.

Treasury Department/Bureau of the Fiscal Service Payment Systems

66. Treasury houses the Bureau of the Fiscal Service ("BFS"), which controls a federal payment system that distributes nearly 90% of all federal payments, including Social Security benefits, tax refunds, and vendor payments.[13] BFS payment systems process more than $6 trillion in annual payments and are responsible for more than a billion payments annually.[14]

67. BFS payment systems contain vast amounts of sensitive personal data of tens of millions of individuals. As one example, the BFS's Integrated Document Management System ("IDMS") contains personally identifying information for "10,000,000–99,999,999" individuals, including Social Security Numbers, personal taxpayer identification numbers, personal financial information, taxpayer information/return information, dates of birth, addresses, zip codes, phone numbers, email addresses, marital statuses, spouse information, information on children, mother's maiden names, military service information, employee identification numbers, health plan beneficiary numbers, patient ID numbers, file/case ID numbers, medical/health information,

[13] Katelyn Polantz, Phil Mattingly & Tierney Sneed, *How an Arcane Treasury Department Office Is Now 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] Letter from U.S. Sen. Ron Wyden to Treasury Secretary Scott Bessent (Jan. 31, 2025), https://www.finance.senate.gov/imo/media/doc/letter_from_senator_wyden_to_secretary_bessent_on_payment_systemspdf.pdf.

mental health information, worker's compensation information, disability information, and emergency contact information.[15]

68. Across presidential administrations of both parties, including President Trump's first administration, BFS systems have historically—and successfully—been operated by career civil servants without direct involvement by political employees.

69. Individuals' full Social Security Numbers—among the most sensitive and carefully guarded categories of personal data—are housed across numerous BFS systems, including the IDMS,[16] the Disbursement And Debt Management Analytics Platform,[17] Do Not Pay,[18] the Electronic Check Processing System,[19] the Electronic Federal Tax Payments System,[20] FedDebt,[21] the Fiscal Data Hub,[22] the Invoice Processing Platform,[23] the Payment Information

[15] BSF, Privacy and Civil Liberties Impact Assessment, *Integrated Document Management System-Records Management (IDMS-RM*), 11 (Oct. 8, 2019), https://www.fiscal.treasury.gov/files/pia/IDMS-pia.pdf [https://perma.cc/Q3V5-AVYE].
[16] *Id.*
[17] Privacy and Civil Liberties Impact Assessment, *Disbursement And Debt Management Analytics Platform (DDMAP)*, BSF, 7 (Mar. 17, 2023), https://www.fiscal.treasury.gov/files/pia/ddmap-pclia.pdf.
[18] Privacy and Civil Liberties Impact Assessment*, Do Not Pay,* BSF, 7 (July 14, 2024), *https://www.fiscal.treasury.gov/files/pia/dnp-pclia.pdf*.
[19] Privacy and Civil Liberties Impact Assessment, *Electronic Check Processing (ECP) System*, BSF, 6 (Aug. 23, 2024), https://www.fiscal.treasury.gov/files/pia/ecp-pclia.pdf.
[20] Privacy and Civil Liberties Impact Assessment, *Electronic Federal Tax Payments System (EFTPS)*, BSF, 7 (June 6, 2024), https://www.fiscal.treasury.gov/files/pia/eftps-pia.pdf.
[21] Privacy and Civil Liberties Impact Assessment, *FedDebt*, BSF, 7 (June 6, 2023) https://www.fiscal.treasury.gov/files/pia/feddebt-pclia.pdf.
[22] Privacy and Civil Liberties Impact Assessment, *Fiscal Data Hub (DH)*, BSF, 7 (Sept. 19, 2023) https://www.fiscal.treasury.gov/files/pia/fiscal-data-hub-pclia.pdf.
[23] Privacy and Civil Liberties Impact Assessment, *Invoice Processing Platform (IPP)*, BSF, 7 (Feb. 15, 2024), https://www.fiscal.treasury.gov/files/pia/IPP-pclia.pdf.

Repository,[24] Payment Information & View of Transactions,[25] the Secure Payment System,[26] the Treasury Check Information System,[27] and Treasury Direct.[28] Pursuant to the Federal Information Security Modernization Act, at least some of these systems are designated high security,[29] meaning that unauthorized disclosures, modifications, or disruptions to access of the systems could have "severe or catastrophic adverse effect[s] on organizational operations, organizational assets, or individuals."[30]

70. Along with the other robust protections that ensure the security of this information, the data on BFS systems are subject to Privacy Act system of records notices (SORNs). These SORNs establish that PII contained in BFS systems is to be disclosed only for narrow, carefully defined purposes relating or incident to the accounting, payment processing, and public debt responsibilities of the BFS.[31]

71. These purposes do not include dismantling, slashing, and restructuring federal programs.

---

[24] Privacy and Civil Liberties Impact Assessment, *Payment Information Repository (PIR)*, BSF, 11 (Apr. 6, 2020), https://www.fiscal.treasury.gov/files/pia/pir-pclia.pdf.
[25] Privacy and Civil Liberties Impact Assessment, *Payment Information & View of Transactions (PIVOT)*, BSF, 7 (May 4, 2022), https://www.fiscal.treasury.gov/files/pia/pivot-pclia.pdf.
[26] Privacy and Civil Liberties Impact Assessment, *Secure Payment System (SPS)*, BSF, 7 (Mar. 22, 2021), https://www.fiscal.treasury.gov/files/pia/spspclia.pdf.
[27] Privacy and Civil Liberties Impact Assessment, *Treasury Check Information System (TCIS)*, BSF, 12 (Apr. 16, 2020), https://www.fiscal.treasury.gov/files/pia/tcis-pclia.pdf.
[28] Privacy and Civil Liberties Impact Assessment, *TreasuryDirect (TD)*, BSF, 7 (Dec. 19, 2023), https://www.fiscal.treasury.gov/files/pia/treasurydirect-pclia.pdf.
[29] *See*, *e.g.*, GovTribe.com, *Secure Payment System O & M Support Services* (May 11, 2022), https://govtribe.com/opportunity/federal-contract-opportunity/secure-payment-system-o-m-support-services-rfifsa23001.
[30] *Standards for Security Categorization of Federal Information and Information Systems*, U.S. Dep't of Comm., FIPS PUB 199 1, 6 (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf.
[31] System of Records, 85 Fed. Reg. 11,776 (Feb. 27, 2020), https://www.federalregister.gov/documents/2020/02/27/2020-03969/privacy-act-of-1974-system-of-records.

72. Since Inauguration, the Treasury Department has flagrantly violated these safeguards at the direction and insistence of DOGE.

73. On Inauguration Day, January 20, 2025, Trump named David Lebryk, a nonpolitical career civil servant who has spent 35 years in government service,[32] as acting Secretary of the Treasury.[33]

74. Treasury DOGE Team Members asked Lebryk about Treasury's ability to stop payments, to which Lebryk responded, "We don't do that."[34]

75. A week later, on January 27, 2025, Defendant Scott Bessent was confirmed as Secretary of the Treasury.[35]

76. Sometime between January 27 and January 31, Lebryk was placed on administrative leave because he had resisted requests to access BFS payment systems from the Treasury DOGE Team.[36]

---

[32] *David Lebryk*, U.S. Dept. of the Treasury, https://home.treasury.gov/about/general-information/officials/david-lebryk; Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/.

[33] Press Release, *President Trump Announces Acting Cabinet and Cabinet-Level Positions*, The White House (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/designation-of-acting-leaders/.

[34] Katelyn Polantz, Phil Mattingly & Tierney Sneed, *How an Arcane Treasury Department Office Is Now 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.

[35] Fatima Hussein, *Scott Bressent Confirmed as Treasury Secretary, Giving Him a Key Role in Extending Trump's Tax Cuts*, AP (Jan. 27, 2025), https://apnews.com/article/bessent-confirmed-treasury-secretary-2ca8eb1c882d094b032584adf1a95c48.

[36] Jeff Stein, Isaac Arnsdorf & Jaqueline Alemany, *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, Wash. Post (Jan. 31, 2025), https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems/; Andrew Duehren et al., *Treasury Official Quits After Resisting Musk's Requests on Payments*, N.Y. Times (Jan. 31, 2025), https://www.nytimes.com/2025/01/31/us/politics/david-lebryk-treasury-resigns-musk.html.

77. Lebryk subsequently announced his retirement in a January 31, 2025, email to Treasury colleagues.[37]

78. Career Treasury employees have consistently underscored to the Treasury DOGE Team that it is not the role of Treasury or BFS to approve or deny payments because "the decision about whether to approve or deny payments belongs to individual agencies based on funds appropriated by Congress."[38]

79. Late on January 27, 2025, Secretary Bessent granted the Treasury DOGE Team access to the BFS's payment systems.[39]

80. Specifically, on information and belief, Treasury has adopted a policy of granting members of the Treasury DOGE Team access to any system to which they request access.

81. On information and belief, Treasury grants Treasury DOGE Team employees access to systems without requiring or reviewing any individualized justification for access or indication that a given employee needs access to that system.

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

[38] Gregory Korte & Viktoria Dendrinou, *Musk Says DOGE Halting Treasury Payments to US Contractors*, Bloomberg (Feb. 2, 2025), https://www.bloomberg.com/news/articles/2025-02-02/musk-says-doge-is-rapidly-shutting-down-treasury-payments.

[39] 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; Jeff Stein, *Musk Aides Gain Access to Sensitive Treasury Department Payment System,* Wash. Post (Feb. 1, 2025), https://www.washingtonpost.com/business/2025/02/01/elon-musk-treasury-payments-system/.

82. Anyone with access to these Treasury payment systems—which, at least at one time, included DOGE Team Members—can stop payments from the federal government, including the ability to "turn off funding selectively."[40]

83. By granting BFS payment system access to the Treasury DOGE Team, Secretary Bessent and the Treasury Department disclosed vast stores of PII contained in those systems to individuals not authorized by law to access them.

84. At least one former employee of Elon Musk and member of the Treasury DOGE Team, Marko Elez, was granted administrator-level privileges over BFS payment systems, including but not limited to the Payment Automation Manager, the Secure Payment System (SPS), and the Electronic Federal Tax Payments System.[41]

85. Administrative privileges granted Elez power to "navigate an entire file system, change user permissions, . . . delete or modify critical files . . . bypass the security measures of, and potentially cause irreversible changes to, the very systems they have access to."[42]

86. Federal information technology experts have stated that nobody would need these privileges to hunt down fraudulent payments or to analyze the disbursement of funds.[43] A source

[40] Greg Sargent, *Trump and Elon Musk Just Pulled off Another Purge – And It's a Scary One*, The New Republic (Jan. 31, 2025), https://newrepublic.com/article/191014/trump-elon-musk-treasury-purge.
[41] James Lidell, *A 25-year-old Elon Musk acolyte has access to 'nearly all payments made by U.S. government'*, The Independent (Feb. 4, 2025), https://www.the-independent.com/news/world/americas/us-politics/elon-musk-marko-elez-treasury-doge-b2691932.html
[42] *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/
[43] *Id.*

reported they were concerned that data could be passed from the Payment Automation Management and Secure Payment System to DOGE Affiliates embedded in other agencies.[44]

87. Elez's access was unlawful under the Privacy Act and in violation of established security policies and requirements. On information and belief, Elez lacked requisite training in the handling of sensitive personal data.

88. That access was also unnecessary; Elez had no lawful reason to have access to these systems.

89. Elez since resigned from the federal government and was later re-hired into the federal government to perform DOGE work.[45] He is an employee of at least one agency (the Department of Labor) and detailed to at least two other federal entities (USDSTO and the Department of Health and Human Services).

90. On information and belief, Treasury DOGE Team members are unlawfully exfiltrating identifying information from BFS payment systems, impermissibly matching this information with other data sets, and using and redisclosing such information for impermissible purposes.

91. For example, the privacy impact assessments for SPS and other BFS payment systems state that PII maintained within the systems will not be used as part of a matching program.[46]

92. On information and belief, Treasury DOGE Team members have used PII from these systems to conduct computer matching of PII.

---

[44] *Id.*
[45] *The US Treasury Claimed DOGE Technologist Didn't Have "Write Access" When He Actually Did*, WIRED (Feb. 6, 2025).
[46] *See e.g.*, Privacy and Civil Liberties Impact Assessment, Secure Payment System (SPS), Mar. 22, 2021, https://www.fiscal.treasury.gov/files/pia/spspclia.pdf 13.

93. The privacy impact assessments for SPS and other accessed BFS payment systems state that PII maintained in the system is not shared with agencies, organizations, or individuals external to the Treasury.[47]

94. On information and belief, Treasury has shared PII with individuals not employed at Treasury, including DOGE Affiliates outside the agency.

95. The privacy impact assessments for multiple Treasury payment systems designed to facilitate payments and deliver government benefits and services state the PII in such systems shall not be "used to make adverse determinations about an individual's rights, benefits, and privileges under federal programs."[48]

96. On information and belief, the Treasury, at the direction of its DOGE Team has moved to stop approved payments to federal contractors, charities that provide social services, and other federal departments. DOGE Team members have further indicated that DOGE is likely to target vital public benefits programs.

The Office of Personnel Management's EHRI System

97. OPM hosts and administers the Enterprise Human Resources Integration, which is "responsible for maintaining the integrity of the electronic Official Personnel Folder (eOPF), which protects information rights, benefits, and entitlements of federal employees."

98. The EHRI Data Warehouse, a component of the EHRI, "is the Federal government's source for integrated Federal workforce information and includes career lifecycle information that encompasses human resource data, training data, and payroll data."[49]

---

[47] *Id*. at 14.
[48] *See e.g.*, *id.* at 11.
[49] *Privacy Impact Assessment for Enterprise Human Resources Integration Data Warehouse*, U.S. Office of Personnel Management (July 11, 2019) https://www.opm.gov/information-management/privacy-policy/privacy-policy/ehridw.pdf

99. The "system currently collects, integrates, and publishes data for 2.0 million Executive Branch employees on a bi-weekly basis, supporting agency and governmentwide analytics."[50]

100. "Contained within the EHRI are the Social Security numbers, dates of birth, salaries, home addresses, and job descriptions of all civil government workers, along with any disciplinary actions they have faced."[51]

101. Pursuant to FISMA, EHRI is categorized as a high risk information system, for which "the unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals," and "[t]he disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals."[52]

102. Like the BFS systems, information in EHRI is protected by a robust set of legal safeguards, including SORNs.

103. The principal SORN applicable to EHRI makes clear that PII contained in EHRI is to be disclosed only for narrow, carefully defined purposes relating or incident to the provision

[50] *Enterprise Human Resources Integration: Data Warehouse*, U.S. Office of Personnel Management, https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human-resources-integration/#url=Data-Warehouse.
[51] Caleb Ecarma and Judd Legum, *Musk associates given unfettered access to private data of government employees*, MuskWatch (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered.
[52] *See Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse*, U.S. Office of Personnel Management Office of the Inspector General, Rep. No. 4A-CI-00-19-006 1, 6 (2019), https://www.oversight.gov/sites/default/files/documents/reports/2022-01/4a-ci-00-19-006.pdf; FIPS PUB 199 at 6, *supra* note 30.

of human resource services. These purposes do not include dismantling, slashing, and restructuring federal programs.

104. Since Inauguration, OPM has flagrantly violated these safeguards at the direction and insistence of DOGE.

105. On January 20, 2025, Inauguration Day, DOGE "assumed command" of OPM by taking over the agency's headquarters, which can only be accessed with a security badge or security escort.[53] OPM employees described the move as a "hostile takeover."[54]

106. DOGE took control of computer systems, and at least six DOGE Affiliates were appointed to OPM and given broad access to all personnel systems, including the EHRI system.[55] The OPM DOGE Team then locked career civil servants at OPM out of those same systems.[56]

107. OPM has since adopted a policy of granting members of the OPM DOGE Team and other DOGE personnel access to any system to which they request access.

108. On information and belief, OPM grants DOGE personnel, including OPM DOGE Team members access to systems without requiring or reviewing any individualized justification for access or indication that a given employee needs access to that system, or needs access that is as broad as what is granted.

---

[53] 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/.
[54] *Id.*
[55] Isaac Stanley-Becker, et al., *Musk's DOGE agents access sensitive personnel data, alarming security officials*, Wash. Post (Feb. 6, 2025), https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/.
[56] Reid, *Exclusive: Musk Aides Lock Workers out of OPM Computer Systems*, https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.

109. An additional ten DOGE affiliates were given access to OPM records without being appointed to OPM.[57] Of the seventeen DOGE affiliates that currently have access to OPM databases, six perform work at two or more agencies in addition to OPM.[58]

110. According to two OPM staffers, the DOGE Team Members now have "the ability to extract information from databases that store medical histories, personally identifiable information, workplace evaluations, and other private data."[59] That includes PII for the 24.5 million people who applied for federal employment on USAJobs.[60]

111. DOGE Team Members emailed an OPM staffer, directing the staffer to give a DOGE Team Member access "as an admin user" to the system and "code read and write permissions."[61] The staffer said that level of permission would allow DOGE to "make updates to anything that they want."[62]

112. DOGE Team Members have also been caught installing "hard drives" and a "new server being used to control" EHRI and other databases at OPM.[63]

---

[57] Notice of Filing of Admin. Record at OPM-000089– 90, OPM-000098, OPM-000103, *Am. Fed. of Gov. Emps. v. U.S. Office of Personnel Mgmt.*, No. 1:25-cv-01237 (S.D.N.Y. April 23, 2025), ECF No. 78.
[58] Mem. ISO Prelim. Inj. at 5, *Am. Fed. of Gov. Emps. v. U.S. Office of Personnel Mgmt.*, No. 1:25-cv-01237 (S.D.N.Y. April 25, 2025), ECF No. 84.
[59] Caleb Ecarma & Judd Legum, *Musk Associates Given Unfettered Access to Private Data of Government Employees*, Musk Watch (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered.
[60] Isaac Stanley-Becker, et al., *Musk's DOGE agents access sensitive personnel data, alarming security officials*, Wash. Post (Feb. 6, 2025) https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/.
[61] *Id.*
[62] *Id.*
[63] Alt National Park Service (@altnps.bsky.social), Bluesky (Jan. 31, 2025, 8:14 PM ET), https://bsky.app/profile/altnps.bsky.social/post/3lh3dl3rkgc2u.

113. In addition to EHRI, OPM DOGE Team Members also have access to other OPM systems.[64] These systems include: USAJOBS, the federal government's hiring site that contains PII, including Social Security Numbers, home addresses, and employment records, of anyone who has applied for a federal job or internship; USA Staffing, an onboarding system; USA Performance, a job performance review site; and HI, a system for managing employee health care that contains sensitive health information protected by the Health Insurance Portability and Accountability Act ("HIPAA").[65]

114. Between January 24 and February 7, 2025, ten OPM DOGE Team Members obtained access to USA Performance – Office of the Director.[66]

115. The DOGE Affiliates who have access to Treasury and OPM systems and to whom sensitive information have not been comprehensively identified by the government, and, on information and belief, some of them individuals lack training in applicable security safeguards for PII, do not have relevant Treasury or OPM experience, and may not have necessary security clearances.

116. By granting EHRI system access to DOGE Team Members, OPM disclosed vast stores of PII contained in those systems to individuals not authorized by law to access them; for purposes impermissible under the Privacy Act and the applicable systems of records notice and privacy impact assessments; and in violation of established security policies and requirements.

Harms to Plaintiffs

117. Plaintiffs have a constitutional right to the privacy of their information; Treasury and OPM Defendants have violated and continue to violate that right by unlawfully disclosing

[64] *Id.*
[65] *Id.*
[66] Notice of Filing of Admin. Record at OPM-000103, *Am. Fed. of Gov. Emps. v. U.S. Office of Personnel Mgmt.*, No. 1:25-cv-01237, ECF No. 78.

extremely personal information about Plaintiffs and millions of others to unchecked actors in violation of law.

118. The ongoing breach of Treasury and OPM systems puts Plaintiffs at severe continuous risk of further data disclosure.

119. DOGE has made clear their disregard for legal controls or restraints, and in light of their past willingness to disclose information publicly or use it for other unlawful purposes, their continued access to sensitive information presents a near certainty that they will continue to misuse that information.

120. The use of unauthorized and unsecured information technology to access, view, store, or disseminate sensitive information creates increased vulnerability to illegal exfiltration by actors unaffiliated with the federal government.

121. Specifically, OPM and Treasury data are rich targets for cyberattacks both by criminals and by foreign adversaries.

122. The PII contained in the BFS and EHRI systems can enable identity theft and other financial crimes which have devastating effects on their victims. Plaintiffs' information is at significantly elevated risk of being stolen and used by cybercriminals for these purposes.

123. OPM data have already likely been targeted in prior breaches by foreign adversary actors to gain intelligence or other advantage over the United States, specifically to the detriment of the individuals whose information was stolen.

124. Foreign adversaries regularly target United States government information systems, and increasing the vulnerability of desirable data creates an elevated risk that they will successfully access those data.

125. The unlawful breach, disclosure, and accessing of the personal information of multiple EPIC members and Plaintiff Doe 1 has intruded upon their otherwise private concerns and caused them unease and offense.

126. The unlawful breach, disclosure, and accessing of the personal information of multiple EPIC members and Plaintiff Doe 1 has caused them, and continues to cause them, significant fear about the misuse of their personal information by those who have accessed it, significant fear about the increased vulnerability of their personal information to further theft, and significant fear about the increased risk of identity theft.

CLAIMS FOR RELIEF

Count I
Violation of the Privacy Act
Defendant Agencies

127. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

128. Treasury Defendants and OPM Defendants have disclosed Plaintiffs' personal data contained in systems of records controlled by Defendants in violation of the Privacy Act, 5 U.S.C. § 552a(b) and wrongfully used such data for computer matching without an adequate written agreement in violation of the Privacy Act, 5 U.S.C. § 552a(o).

129. DOGE and its affiliates are non-agency employees with no need for the records to which OPM and Treasury have granted them access.

130. No condition of disclosure in 5 U.S.C. § 552a(b) allows Treasury or OPM to grant DOGE or its affiliates to agency systems of records.

131. Plaintiffs are entitled to civil remedies under 5 U.S.C. § 552a(g).

Count II
Violation of 26 U.S.C. § 6103
(Willful or Grossly Negligent Unauthorized Disclosure)
Defendants Scott Bessent, Treasury

132. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

133. The Treasury Department maintains records of direct payments and direct deposits for tax payments and refunds for up to six years from the date of the direct deposit. IRM 12.4.2.1.2.1.2.

134. Plaintiff Doe 1's return information has been used by BFS systems to process tax payments in the last 6 years. Information about those transactions is included in BFS systems.

135. Treasury and Secretary Bessent have knowingly or grossly negligently violated Section 6103 by disclosing and inspecting confidential return information contained in the BFS system, which includes tax return information (including the amount of tax refunds), including Doe 1's.

136. Pursuant to 26 U.S.C. § 7431, Plaintiff Doe 1 is entitled to statutory damages in the amount of $1,000 per each act of unauthorized inspection and disclosure.

137. Plaintiff Doe 1 is also entitled to punitive damages pursuant to 26 U.S.C. § 7431(c)(1)(B)(ii) because the Treasury Department's unlawful disclosure of their confidential return information was either willful or a result of gross negligence.

Count III
Violation of the Fifth Amendment (Right to Informational Privacy)
Defendant Agencies

138. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

139. Defendants, by providing access to confidential PII, including financial information, in which individuals have a reasonable expectation of privacy, without lawful authorization, have deprived EPIC's members and Doe 1 of their liberty interest in avoiding

disclosure of personal matters under the Due Process Clause of the Fifth Amendment. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Payne v. Taslimi*, 998 F.3d 648, 656 (4th Cir. 2021).

140. Defendants have done so without legal authorization, without providing notice to the individuals whose data has been accessed, including EPIC's members and Doe 1, and without providing them an opportunity to challenge the disclosure of their data before a neutral decisionmaker.

141. Defendants have violated the Fifth Amendment rights to due process of law of Plaintiff EPIC's members and of Plaintiff Doe 1. U.S. Const. amend. V.

Count IV
Violation of the APA: Contrary to law
Defendant Agencies

142. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

143. Defendants Treasury and OPM have adopted system access policies that grant DOGE unfettered, unauthorized access to a number of highly sensitive record systems managed by Defendants.

144. These system access policies ignore, alter, or effectively nullify existing system access rules, regulations, policies and/or procedures at Defendant Agencies.

145. These system access policies constitute final agency actions that injure Plaintiffs and have no other adequate remedy in court. Accordingly, relief is available under the Administrative Procedure Act. 5 U.S.C. §§ 702, 704.

146. As described above, these system access policies violate a number of legal requirements, including the Privacy Act, FISMA, 26 U.S.C. § 6103, and the Fifth Amendment of the U.S. Constitution.

147. For these reasons, Treasury's and OPM's system access policies are "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). They should, accordingly, be held unlawful and "set aside." *Id.* § 706(2).

Count V
Violation of the APA: Arbitrary and Capricious
Defendant Agencies

148. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

149. Defendants Treasury and OPM have adopted system access policies that effectively revoke and replace existing system access policies to allow DOGE unfettered access to Defendants' sensitive systems.

150. These system access policies ignore, alter, or effectively nullify existing system access rules, regulations, policies and/or procedures at Defendant Agencies.

151. These system access policies constitute final agency actions that injure Plaintiffs and have no other adequate remedy in court. Accordingly, relief is available under the Administrative Procedure Act. 5 U.S.C. §§ 702, 704.

152. These policies were hasty, ill-considered, unsupported, and destructive to the interests that government privacy laws are intended to advance.

153. For these reasons, Treasury's and OPM's system access policies are "arbitrary" and "capricious," and should be held unlawful and "set aside." *Id.* § 706(2).

Count VI
Violation of the APA: Notice and Comment
Defendant Agencies

154. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

155. Defendants Treasury and OPM are agencies subject to the requirements of the APA. 5 U.S.C. § 701(b)(1).

156. Defendants' decisions to adopt new system access policies that effectively revoke pre-existing system access policies constitute the promulgation of a new substantive rule because they affirmatively change the rights and obligations of USDS personnel with regards to access to sensitive information systems.

157. Under the APA, substantive rules promulgated by an agency must undergo notice and comment procedures to allow the public and affected parties the opportunity to weigh in on changes to agency policy. 5 U.S.C. § 553.

158. Neither Treasury nor OPM complied with the notice-and-comment rulemaking procedures prescribed by the APA, and thus impermissibly promulgated a new rule in violation of the APA.

159. Plaintiffs were and continue to be harmed by this unlawful act.

Count VII
Actions *Ultra Vires*
Defendants DOGE Teams, USDS, USDSTO, OPM, GSA, Davis, Musk

160. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

161. In directing and controlling the use and administration of Defendant OPM's EHRI system and Defendant Treasury Department's BFS payment systems, the OPM and Treasury DOGE Teams (and, to the extent the DOGE Teams are functionally controlled by Defendants USDS, USDSTO, OPM, GSA, Musk, and Davis, those Defendants as well), have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of people.

162. The DOGE Teams may not take actions which are not authorized by law.

163. No law or other authority authorizes or permits the DOGE Teams to access or administer these systems.

164. Through such conduct, Defendants have engaged (and continue to engage) in *ultra vires* actions which injure plaintiffs by violating their constitutional rights, exposing their private information, and increasing the risk of further disclosure of their information.

165. Plaintiffs have a non-statutory right to relief directing the DOGE Teams, and, as necessary to obtain relief, the Acting USDS Administrator, GSA Administrator, OPM Director, and DOGE heads Musk and Davis, to remedy these violations.

Count VIII
Violation of Separation of Powers
Defendants DOGE Teams, USDS, USDSTO, OPM, GSA, Davis, Musk

166. Plaintiffs assert and incorporate by reference the foregoing paragraphs.

167. Defendants have violated and are continuing to violate Separation of Powers principles by repeatedly acting in contravention of congressional authority.

168. Congress exercised its Article I authority to create both Treasury and OPM; each is a creature of statute which possesses only the authority with which Congress provided it.

169. Congress neither created nor provided any authority to the agency DOGE Teams, USDS, USDSTO, nor the positions held by Davis and Musk.

170. The OPM and Treasury DOGE Teams (and, to the extent the DOGE Teams are functionally controlled by Defendants USDS, USDSTO, OPM, GSA, Musk, and Davis, those Defendants as well), are exercising powers imbued in OPM and Treasury by Congress.

171. Defendants' actions unlawfully usurp Congress's legislative authority and override congressional mandates.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that this Court:

1. Enjoin Defendants' wrongful provision of access to and disclosure of systems of records containing PII;

2. Declare unlawful and halt Defendants' use of OPM and Treasury systems for purposes in excess of System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), and the Federal Information Security Modernization Act (FISMA);

3. Declare unlawful and halt OPM Defendants and Treasury Defendants from sharing data from OPM systems and Treasury systems with non-agency employees for non-routine and non-permitted purposes;

4. Order Treasury Defendants and OPM Defendants to revoke access to PII by the respective DOGE Teams;

5. Declare unlawful and halt the DOGE Teams' direction or control of use of OPM and BFS systems;

6. Declare unlawful and halt the DOGE Teams' access to or disclosure of personal or other protected information;

7. Order the DOGE Teams, and any people or entities with whom they shared data which they lacked legal authority obtain to disgorge or delete all unlawfully obtained, disclosed, or accessed PII from systems or devices on which they were not present on January 19, 2025;

8. Prohibit DOGE Affiliates from collecting, accessing, disclosing, or retaining PII in OPM systems and Treasury systems;

9. Award statutory and punitive damages to Plaintiff Doe;

10. Award costs and reasonable attorneys' fees incurred in this action; and

11. Grant such other relief as the Court may deem just and proper.

Dated: May 6, 2025

Respectfully Submitted,

/s/ Matthew B. Kaplan
Matthew B. Kaplan, VSB # 51027
THE KAPLAN LAW FIRM
1100 N. Glebe Rd., Suite 1010
Arlington, VA 22201
Telephone: (703) 665-9529
mbkaplan@thekaplanlawfirm.com

Mark B. Samburg*
Aman T. George*
Orlando Economos*
Robin F. Thurston*
Skye Perryman*
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
oeconomos@democracyforward.org
rthurston@democracyforward.org
sperryman@democracyforward.org

Alan Butler*
EPIC Executive Director
John L. Davisson*
EPIC Director of Litigation
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (fax)

**admitted* pro hac vice

Counsel for Plaintiffs