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

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue, NW
Washington, D.C. 20036

DOE 1

Plaintiffs,

v.

Case No. 1:25-cv-00255

U.S. OFFICE OF PERSONNEL MANAGEMENT
1900 E Street NW
Washington, DC 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.

DEPARTMENT OF THE TREASURY
1500 Pennsylvania Avenue NW
Washington, DC 20220

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

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

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

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

Defendants.

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

INTRODUCTION

On the evening of his inauguration, President Trump signed an Executive Order "Establishing and Implementing the President's 'Department of Government Efficiency.'" The Executive Order renamed and reorganized the United States Digital Service as the U.S DOGE Service ("DOGE"), instructed agency heads to provide DOGE with extensive access to agency records and IT systems, and nominally required DOGE to adhere to strong data protection standards. DOGE quickly got its access—including to information systems containing Plaintiffs' confidential personal information.

But in the weeks since the inauguration, DOGE has disregarded the latter requirement, running roughshod over core data protections and endangering the security of vital government systems. Since Inauguration Day, DOGE personnel have sought and obtained unprecedented access to information systems across numerous federal agencies, including the Department of Treasury ("Treasury"), Office of Personnel Management ("OPM"), and at least ten others. In addition to infiltrating their information systems, DOGE personnel also played critical roles in the dismantling of USAID and ongoing concurrent efforts to largely cripple the Department of Education.

Plaintiffs are and represent individuals whose sensitive, confidential, and personally identifiable information has been unlawfully accessed and endangered by DOGE. Plaintiff Doe 1 is a career civil servant who has electronically filed her tax returns through the Bureau of the Fiscal Service ("BFS") within the last six years. Declaration of Doe 1, Exhibit A ("Doe Decl. (Ex. A)") ¶¶ 2, 5–7. Her information is stored in the informational systems Treasury and OPM maintain, namely BFS and Enterprise Human

Resources Integration ("EHRI"), and to which DOGE operatives have gained access. *Id.* ¶¶ 5, 8. She understood that in handling her data, the government would keep it private and confidential, and that it would observe all applicable laws in handling it. *Id.* ¶¶ 8, 9. Likewise, Plaintiff EPIC has members who have filed returns with and received refunds from Treasury, and expected their information to be kept private and confidential. Declaration of Alan Butler, Exhibit B ("Butler Decl. (Ex. B)") ¶¶ 7–12; Declaration of Leonard Kennedy, Exhibit C ("Kennedy Decl. (Ex. C)") ¶¶ 9–13; Declaration of David Brody, Exhibit D ("Brody Decl. (Ex. D)") ¶¶ 9–13; Declaration of Bruce Schneier, Exhibit E ("Schneier Decl. (Ex. E)") ¶¶ 9–13.

At Treasury, DOGE operatives immediately zeroed in on the Bureau of Fiscal Service payment systems, which distribute the overwhelming majority of federal payments, including payments to vendors and employees, Social Security benefits, and tax refunds. Prior to the Senate's confirmation of Secretary Bessent, employees affiliated with DOGE reportedly asked about Treasury's ability to stop payments.[1] Elon Musk, who is either the Acting Administrator for the U.S. DOGE Service or is substantially directing its work, has also been clear about his interest in the ability to use the BFS system to stop payments, posting on his social media website that DOGE operatives "discovered, among other things, that payment approval officers at Treasury were instructed always to approve payments, even to known fraudulent or terrorist groups. They literally never denied a payment in their entire career. Not even once."[2]

---

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

[2] Elon Musk (@elonmusk), X/Twitter (Feb. 1, 2025, 1:52 AM ET) https://x.com/elonmusk/status/1885582076247712229.

On January 27, Secretary Bessent authorized at least two DOGE representatives access to the BFS system. This access, and the identity of these political staffers, has only been revealed through public reporting.[3]

Meanwhile, DOGE operatives also infiltrated the Office of Personnel Management ("OPM"), moving sofa beds into the agency's headquarters and revoking civil servants' access to Enterprise Human Resources Integration system ("EHRI"), which contains millions of federal employees' Personally Identifiable Information ("PII") including social Security numbers, dates of birth, salaries, home addresses, job descriptions, and disciplinary records.[4] According to some reports, a DOGE-affiliated worker "literally walked into our building and plugged in an email server to our network" to start sending government-wide emails. Complaint, *Does v. OPM*, No. 1:25-cv-00234 (D.D.C., Jan 27, 2025), ECF No. 1. And DOGE operatives at OPM have not stopped there, combing through OPM databases "looking through all the position descriptions . . . to remove folks."[5]

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

[3] Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payments System*, The New York Times, Feb. 2, 2021, https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html.
[4] Tim Reid, *Exclusive: Musk aides lock workers out of OPM computer systems*, Reuters, Jan. 31, 2025, https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/.
[5] Hafiz Rashid, *Elon Musk Installs Illegal Server to Seize All Federal Workers' Data*, Yahoo News, Feb. 3, 2025, https://www.yahoo.com/news/elon-musk-makes-most-terrifying-183451530.html.

agencies at their will. This process moves incredibly quickly, with agencies established by Congress accessed within a matter of hours; or functionally decommissioned within a week. But federal information law bars DOGE's access to these systems, and OPM and Treasury officials were not authorized to grant that access. Because the systems access of both various unidentified DOGE officials is contrary to law and poses an ongoing threat to information security, this court should grant immediate relief terminating that access.

LEGAL STANDARD

To obtain a temporary restraining order, a plaintiff must "establish that (1) they are likely to succeed on the merits of their case; (2) they are likely to suffer irreparable harm in the absence of injunctive relief; (3) the balance of the equities tips in their favor; and (4) an injunction would be in the public interest." *Sarsour v. Trump*, 245 F. Supp. 3d 719, 728 (E.D. Va. 2017) (citing *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008) and *Manning v. Hunt*, 119 F.3d 254, 263 (4th Cir. 1997)). "The standard for granting either a TRO or a preliminary injunction is the same." *Id.* (quoting *Moore v. Kempthorne*, 464 F.Supp.2d 519, 525 (E.D. Va. 2006). The final two factors of equity and public interest "merge when the Government is the opposing party." *Miranda v. Garland*, 34 F.4th 338, 365 (4th Cir. 2022) (quoting *Nken v. Holder*, 556 U.S. 418, 435 (2009)).

FACTUAL BACKGROUND

OPM and Treasury Systems and Plaintiffs' Data

Treasury and OPM systems house enormous amounts of sensitive personal information. Specifically, the Bureau of Fiscal Service ("BFS") payment systems contain

Social Security numbers, tax return information, and other highly sensitive personal information about tens of millions of Americans, if not more. And OPM's Enterprise Human Resources Integration ("EHRI") system contains personal data on millions of federal employees, including Social Security numbers, home addresses, information about disciplinary actions, and other sensitive personal information.

Along with the robust legal protections detailed below, these systems are protected by Systems of Records Notices ("SORNs"), as required by the Privacy Act. EHRI is subject to the OPM-GOVT-1 SORN,[6] which provides that information in the system can be disclosed only for narrow, carefully defined purposes, none of which apply to the Department of Government Efficiency's access to the system. Similarly, the BFS systems are subject to SORNs[7] which permit access only in circumstances not present here. And the systems have historically been operated by career civil servants without direct involvement by political employees.

Creation of The Department of Government Efficiency

On November 12, 2024, then President-Elect Trump announced his intent to create the "Department of Government Efficiency" ("DOGE") to "provide advice and guidance from outside of Government" to "the White House and Office of Management & Budget,"

[6] OPM, *OPM GOVT-1: General Personnel Records*, accessible at https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf.

[7] BFS information related to payment and benefits for federal employees is generally subject to Treasury.001, Notice of System of Records, 89 Fed. Reg. 25688 (Apr. 11, 2024), while tax return information is covered by several SORNs, most notably FS .02 (which pertains to recipients of government payments) and FS .013 (which pertains to people who make electronic payments to the government). Notice of System of Records, 85 Fed. Reg. 11776 (Feb. 27, 2020).

to help "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[8]

Over the next several months, DOGE personnel spoke with staffers at federal agencies including the Department of Treasury, the Internal Revenue Service, the Department of Homeland Security, Veterans Affairs, and the U.S. Department of Health and Human Services.[9] These employees were directed in large part by Elon Musk, who is either the Acting USDS Administrator or otherwise exercising substantial authority within USDS.

On the day of his inauguration, January 20, 2025, President Trump signed Executive Order 14158, Establishing and Implementing the President's "Department of Government Efficiency," ("the E.O."), reorganizing and renaming the United States Digital Service as the United States DOGE Service, established in the Executive Office of the President.[10]

The E.O. established the role of U.S. DOGE Service Administrator in the Executive Office of the President, reporting to the White House Chief of Staff.[11]

The E.O. further established within the U.S. DOGE Service the "U.S. DOGE Service Temporary Organization," a temporary organization headed by the U.S. DOGE Service Administrator and tasked with advancing "the President's 18-month DOGE agenda."[12]

---

[8] *See* Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, 7:46 PM ET), https://truthsocial.com/@realDonaldTrump/posts/113472884874740859.
[9] Faiz Siddiqui, Jeff Stein and Elizabeth Dwoskin, *DOGE is dispatching agents across U.S. government*, Wash. Post (Jan. 10, 2025), https://www.washingtonpost.com/business/2025/01/10/musk-ramaswamy-doge-federal-agencies/.
[10] Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025).
[11] *Id.* § 3(b).
[12] *Id.*

The E.O. also requires each Agency Head to establish a "DOGE Team" comprising at least four employees within their respective agencies. DOGE Teams are required to "coordinate their work with [the U.S. DOGE Service] and advise their respective Agency Heads on implementing the President's DOGE agenda.[13]

The E.O. instructs the U.S. DOGE Service Administrator to "commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems."[14] 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."[15]

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."[16] The E.O. nominally directs the U.S. DOGE Service to adhere to "rigorous data protection standards."[17]

Operations of the Department of Government Efficiency

Since Inauguration Day, USDS/DOGE personnel, many of them associates of Elon Musk, have sought and obtained unprecedented access to information systems across numerous federal agencies, including: the Centers for Disease Control and Prevention, the Centers for Medicare & Medicaid Services; the Department of Education; the National Oceanographic and Atmospheric Administration; the Department of Energy; the Federal

[13] *Id.* § 3(c).
[14] *Id.* § 4(a).
[15] *Id.*
[16] *Id.* § 4(b).
[17] *Id.*

Emergency Management Agency; the Department of Labor; the U.S. Agency for International Development; the Department of Veterans Affairs; the Consumer Financial Protection Bureau; and the two agencies at issue here, Treasury and OPM.[18]

DOGE follows the same pattern across virtually every agency it enters: swooping in with new DOGE staff, demanding access to sensitive systems, often threatening employment action again employees who resist their unlawful commands, and, in many instances, beginning to reorganize the agencies. This process moves with extraordinary speed, with Congressionally created agencies fully compromised essentially overnight, or seemingly dismantled within days.

Under ordinary circumstances, the access requested and obtained by DOGE would be prevented by compliance with the rigorous scheme of legal protections detailed below. But several agencies, including Treasury and OPM, have instead acquiesced to DOGE's demands.

DOGE Access to Treasury

After President Trump's inauguration on January 20, he named a senior career Treasury official, David Lebryk, as Acting Secretary of the Treasury.[19] When DOGE

[18] Chas Danner, *All the Federal Agencies DOGE Has Broken Into*, N.Y. Mag. (Feb. 9, 2025), https://nymag.com/intelligencer/article/doge-elon-musk-what-federal-agencies-access-lawsuits.html; Mike Wendling, *Musk's Doge takes aim at US consumer protection agency*, BBC News (Feb. 8, 2025), https://www.bbc.com/news/articles/cly48101n19o.
[19] Jeff Stein, Isaac Arnsdorf & Jacqueline 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/.

personnel arrived at Treasury, they asked Lebryk about Treasury's ability to stop BFS payments, to which Lebryk replied "we don't do that."[20]

On the same day as his confirmation as Secretary of Treasury on January 27, Secretary Bessent granted system access to DOGE personnel.[21] Lebryk was subsequently placed on administrative leave for his refusal to grant system access to DOGE personnel, and he has since retired from government.[22]

Despite the expansive access granted by Secretary Bessent, career Treasury employees have consistently underscored to DOGE affiliates 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

[20] 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.

[21] 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/.

[22] Stein et al., *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, *supra* note 19; 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.

Congress."[23] According to public reporting, anyone with this level of access would have the ability to "turn off funding selectively."[24]

One person with such access was Marko Elez, a former Musk employee who had administrator-level access to BFS systems, which would have enabled him 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."[25] Elez, who has since resigned from DOGE over his connection with racist social media posts,[26] had his access downgraded to "read-only' by February 5, but not before then Secretary-Designee Bessent and the White House Press Secretary both publicly indicated that DOGE did not have administrative access to Treasury systems.[27]

DOGE access to Treasury systems was further temporarily limited by the District Court for the District of D.C., which limited DOGE-related access to "read only" access

---

[23] 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.

[24] 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.

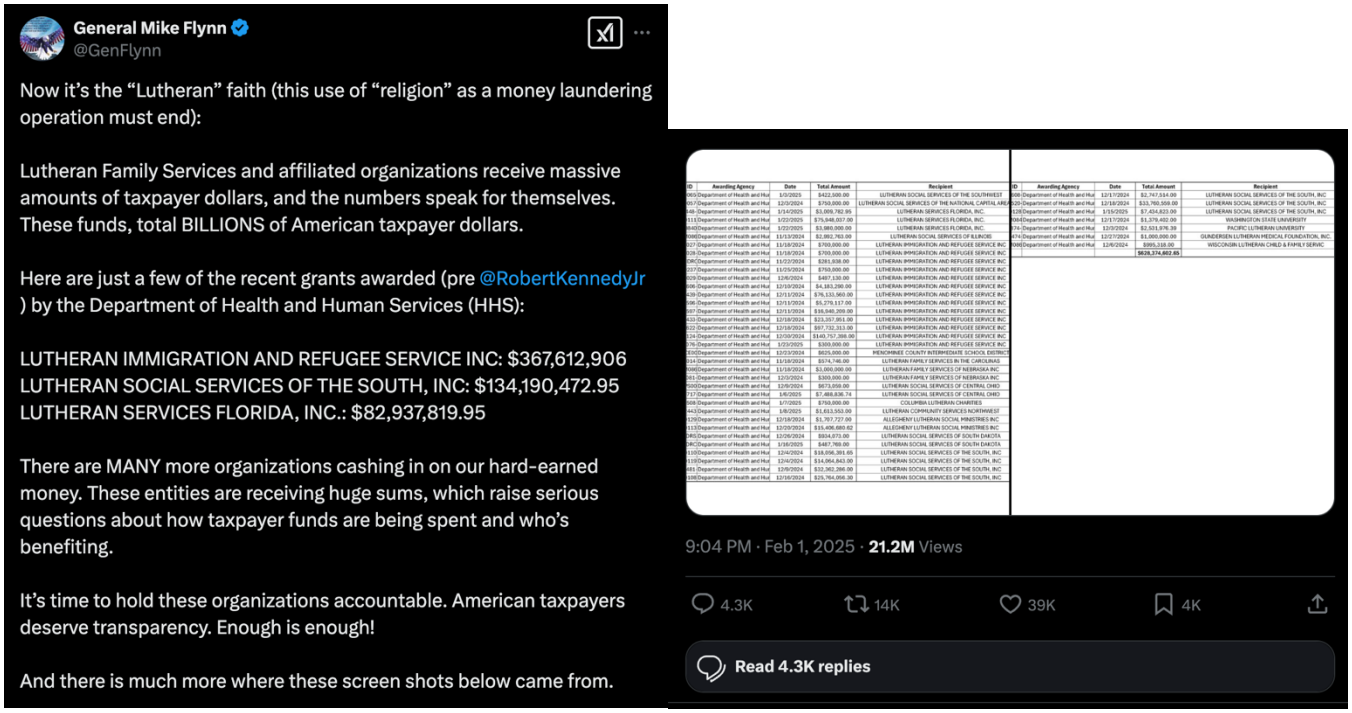
[25] *A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System*, WIRED (Feb. 4, 2025) https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/; *see also* James Lidell, *A 25-year-old Elon Musk acolyte has access to 'nearly all payments made by U.S. government'*, The Independent (Feb. 4, 2025), https://www.the-independent.com/news/world/americas/us-politics/elon-musk-marko-elez-treasury-doge-b2691932.html.

[26] Katherine Long, *DOGE Staffer Resigns Over Racist Posts*, Wall St. J. (Feb. 7, 2025), https://www.wsj.com/tech/doge-staffer-resigns-over-racist-posts-d9f11a93.

[27] *The US Treasury Claimed DOGE Technologist Didn't Have "Write Access" When He Actually Did*, WIRED (Feb. 6, 2025), https://www.wired.com/story/treasury-department-doge-marko-elez-access/.

for Elez and Tom Krause, another individual affiliated with DOGE, in a February 6 order.[28] A group of labor unions and an organization that advocates for retirees have challenged DOGE's access to Treasury systems on Privacy Act and Internal Revenue Code grounds; by agreement of the parties, Treasury temporarily limited DOGE access to its systems pending a decision on a forthcoming motion for preliminary injunction. *Alliance for Retired Americans v. Bessent*, No. 1:25-cv-00313 (D.D.C., Feb. 6, 2025).

Consistent with DOGE's approach to date, within a day of DOGE's first access to the system, information exfiltrated from the BFS payment systems was broadcast to a wide audience on X/Twitter by retired Lt. General Michael Flynn:[29]



[28] Order, *Alliance for Retired Americans v. Bessent*, No. 1:25-cv-00313 (D.D.C., Feb. 6, 2025), ECF No. 13.
[29] Mike Flynn (@GenFlynn), X/Twitter (Feb. 1, 2025, 9:04 PM ET), https://x.com/GenFlynn/status/1885872007062892568.

Elon Musk replied to the tweet, stating that "The @DOGE team is rapidly shutting down these illegal payments."[30] Indeed, after DOGE personnel gained access to Treasury payment systems, the DOGE account on Twitter claimed that it was "stopping improper payments."[31]

DOGE Access to OPM

On Inauguration Day, Musk and others affiliated with DOGE "assumed command" of OPM by taking over the agency's headquarters, which can only be accessed with a security badge or security escort. OPM employees described the move as a "hostile takeover."[32] DOGE personnel took control of computer systems, and at least six DOGE agents demanded from career staff, and were promptly given broad administrator-level access to all personnel systems, including the EHRI system.[33] DOGE personnel then locked career civil servants at OPM out of those same systems.[34]

According to two OPM staffers, these DOGE personnel now have "the ability to extract information from databases that store medical histories, personally identifiable

[30] Elon Musk (@elonmusk), X/Twitter (Feb. 2, 2025, 3:14 AM ET), https://x.com/elonmusk/status/1885964969335808217.
[31] Department of Government Efficiency (@DOGE), X/Twitter (Jan. 28, 2025, 7:20 PM ET), https://x.com/DOGE/status/1884396041786524032.
[32] Reid, *Musk Aides Lock Workers out of OPM Computer Systems*, *supra* note 4.
[33] 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/.
[34] Reid, *Musk Aides Lock Workers out of OPM Computer Systems*, *supra* note 4.

information, workplace evaluations, and other private data,"[35] including personal information for the 24.5 million people who applied for federal employment on USAJobs.[36]

Legal Responses

Plaintiffs are aware of three challenges related to DOGE activity at Treasury or OPM, specifically:

A number of states recently challenged DOGE access to Treasury systems and obtained a temporary restraining order limiting DOGE operations at the Department of Treasury until February 14, 2025. Order, *New York v. Trump*, No. 1:25-cv-01144 (S.D.N.Y., Feb. 8, 2025), ECF No. 6. In granting the order, the court expressed its "firm assessment" the plaintiffs would "face irreparable harm in the absence of injunctive relief. . . both because of the risk that the new policy presents of the disclosure of sensitive and confidential information and the heightened risk that the systems in question will be more vulnerable than before to hacking." *Id.* at 2.[37]

A group of labor unions and an organization that advocates for retirees have challenged DOGE's access to Treasury systems on Privacy Act and Internal Revenue Code grounds; by agreement of the parties, Treasury temporarily limited DOGE access to its systems pending a decision on a forthcoming motion for preliminary injunction. Order,

---

[35] 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.

[36] Stanley-Becker, et al., *Musk's DOGE agents access sensitive personnel data, supra* note 33.

[37] The substantive overlap between the *New York v. Trump* restraining order and the order Plaintiffs request does not weigh against granting Plaintiffs' requested order. *Whitman-Walker Clinic, Inc. v. U.S. Dep't of Health & Hum. Servs.*, 485 F. Supp. 3d 1, 60 (D.D.C. 2020) ("[C]ourts routinely grant follow-on injunctions against the Government, even in instances when an earlier nationwide injunction has already provided plaintiffs in the later action with their desired relief.") (collecting cases).

Alliance for Retired Americans v. Bessent, No. 1:25-cv-00313 (D.D.C., Feb. 6, 2025), ECF No. 13.

And several anonymous federal employees are currently seeking a temporary restraining order in a challenge to DOGE's reported use of an unknown email server connected to OPM systems as a violation of the E-Government Act of 2002. Amended Complaint, *Doe v. OPM*, No. 1:25-cv-00234 (D.D.C., Feb. 7, 2025), ECF No. 14.

ARGUMENT

Each of the factors for a temporary restraining order favor Plaintiffs. *See Sarsour v. Trump*, 245 F. Supp. 3d at 728. Defendants have violated the Federal Information Security Act, the Privacy Act, the Internal Revenue Code, and the Due Process Clause of the Fifth Amendment, in excess of their legal authority. Their unlawful actions have exposed and continue to expose statutorily protected PII to access by unidentified and unauthorized users for no lawful purpose. Beyond the immediate harm of disclosure, Plaintiffs face substantially elevated risk of: data errors which could interfere with their paychecks or other employment benefits, purposeful withholding of payments to which they are legally entitled, and identity theft. Defendants' acquiescence to the unlawful commandeering of government information systems serves no public interest; the seizure of those systems is nothing more than an attempted evasion of legal and regulatory safeguards by quasi-governmental actors in the course of their concerted effort to gut the federal government. This Court should issue a temporary restraining order to protect Plaintiffs from these harms and prevent further degradation of critical government systems until this Court has the opportunity to further consider the case.

I. Plaintiffs are likely to succeed on the merits.

Defendants' actions are replete with legal violations. Plaintiffs are therefore likely to prevail on the merits of their claims. First, Defendants' actions violate a variety of statutory provisions regarding the privacy and security of private information in government hands. Second, because the decision of Treasury and OPM to grant DOGE operatives access to their information systems represents final agency action taken without authorization and contrary to law, it violates the Administrative Procedure Act. Finally, this infiltration deprives Plaintiffs of their right to informational privacy under the Due Process Clause of the Fifth Amendment.

A. Defendants' decisions granting systems access to DOGE constituted disclosures in violation of both the Privacy Act of 1974 and the Internal Revenue Code

Defendants' actions violate at least two distinct laws governing information security and privacy for government data. Access to and maintenance of government information systems are carefully regulated to protect the security of information—including and especially PII. Among the comprehensive scheme of statutes which impose obligations on agencies to protect these systems are:

- The Privacy Act of 1974, 5 U.S.C. § 552a;
- The Internal Revenue Code, 26 U.S.C. § 7431.

The Privacy Act of 1974 prohibits disclosure of information from systems of records except in enumerated circumstances, 5 U.S.C. § 552a(b), and prohibits the use of such data for computer matching without an adequate written agreement, *id.* § 552a(o); FISMA requires that agencies provide information security protection "commensurate with the risk and magnitude of the harm resulting from unauthorized access [or] use" of

information or information systems maintained by the agency, 44 U.S.C. § 3554(a)(1)(A); and The Internal Revenue Code prohibits unauthorized disclosure of tax return information and unauthorized inspection of tax return information, 26 U.S.C. § 7431. The Treasury Defendants and OPM Defendants violated each of these provisions of law when they provided access to their respective systems to DOGE Defendants and other unidentified unauthorized users.

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

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

5 U.S.C. § 552a(a)(4).

Individuals under the Privacy Act are any "citizen of the United States or [] alien lawfully admitted for permanent residence." *Id.* § 552a(a)(2). As relevant for this case, the Privacy Act regulates the disclosure of records, and imposes requirements on agencies

to responsibly maintain their recordkeeping systems. With respect to disclosure, the Act provides, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, *or to another agency,* except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." *Id.* § 552a(b) (emphasis added). The Privacy Act includes a private right of action for civil remedies where, as here, the government "fails to comply with" the Privacy Act "in such a way as to have an adverse effect on an individual." 5 U.S.C. § 552a(g)(1)(D).

Additionally, the Internal Revenue Code 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 confidentiality is core to the Internal Revenue Service's "Taxpayer Bill of Rights": the

> 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) (quoting *Nat'l Treasury Empls. Union v. Fed. Labor Rels. Bd.* 791 F.2d 183, 184 (D.C. Cir. 1986). To that end, it prohibits "the making known to any person in any manner whatever a return or return information," where "return" means "any tax or information return, declaration of estimated tax, or claim for refund" filed with the Secretary of Treasury under the Internal Revenue Code. 26 U.S.C. 6103(b).

By giving DOGE operatives access to BFS and EHRI, as described above, Treasury and OPM violated all three. DOGE is not a component of the Department, so when Treasury "disclose[d] . . . record[s]" to DOGE without "the prior written consent" of the person to whom it pertains it violated the Privacy Act. 5 U.S.C. § 552a(b). OPM, too, violated the Privacy Act when it disclosed EHRI records to DOGE without "prior written consent." While § 552a(b) includes thirteen exceptions where such disclosure is permissible, none of them apply here.

BFS contained information concerning Plaintiff Doe 1's tax returns—by granting access to BFS systems to individuals outside Treasury, Secretary Bessent disclosed that return information. No exception to the Internal Revenue Code prohibition on disclosure of return information plausibly authorized this disclosure. Defendants therefore violated the Internal Revenue Code by effecting a disclosure of return information, including information regarding Plaintiff Doe 1's tax returns, by granting access to BFS without a specific statutory authorization. 26 U.S.C. § 6103. Under 26 U.S.C. § 7431, Plaintiff Doe has a private right of action for damages for this violation.

B. Granting access to sensitive information systems constituted final agency action in violation of the Federal Information Systems Modernization Act, and therefore violated the Administrative Procedure Act.

The decisions of the Treasury and OPM Defendants to grant DOGE Defendants access to their respective systems are final agency action for the purposes of the Administrative Procedure Act. Such actions "mark the consummation of the agency's decisionmaking process . . . by which rights or obligations have been determined, or from which legal consequences will flow." *U.S. Army Corps of Eng'rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177–178 (1997)). Secretary

Bessent's decision to grant DOGE access to BFS constituted "final agency action," as did OPM granting administrator-level EHRI access to DOGE. Those agency decisions were not proposed or hypothetical—they were actual and completed. Both decisions represent the "consummation of the agency's decisionmaking process" concerning the lawfulness of such access; constitute a determination as to the "rights and obligations" of the personnel granted such access; and are actions "from which legal consequences"—that is, access to sensitive personal data and systems of records—have already flowed. *Jake's Fireworks Inc. v. United States Consumer Prod. Safety Comm'n*, 105 F.4th 627, 631 (4th Cir. 2024) (quoting *Hawkes Co.*, 578 U.S. at 597).

The Administrative Procedure Act provides for judicial review of "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. Because the Federal Information Systems Modernization Act ("FISMA") lacks a private right of action, a party, like Plaintiffs, aggrieved by a final agency action contrary to FISMA has no means to obtain judicial review outside the Administrative Procedure Act. Action prohibited by FISMA, including the grants of access to DOGE, is "not in accordance with law," "contrary to constitutional right," or "in excess of statutory jurisdiction" and must be set aside. 5 U.S.C. § 706(2).

FISMA requires agencies to develop security systems and protocols to protect sensitive or confidential information in compliance with regulations and standards developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce. 44 U.S. Code § 3553(h)(2)(F), 40 U.S. Code § 11331(a).[38] Those

[38] Both the Privacy Act and FISMA generally apply to information systems maintained by the federal government. However, the Privacy Act only governs data pertaining to

requirements are found in NIST Special Publication 800-53.[39] For example, the standards require agencies to "[p]hysically control[] and securely store[]" both "digital and/or non-digital media" and "protect[] information system media until the media are destroyed."[40] Agencies must "enforce[] physical access authorizations," by "verifying individual access authorizations" and "escort visitors and control visitor activity."[41] And they must "prohibit the use of portable storage devices," including hard drives, "when such devices have no identifiable owner."[42]

It is implausible and inconsistent with public reporting that when DOGE arrived and demanded immediate access to Treasury and OPM data for its personnel that it had established any process to ensure that mandatory security controls required by FISMA were in place. Reporting indicates that at OPM, for instance, DOGE operatives simply assumed command of OPM's headquarters without observing security protocols—which required security badges and escorts, in compliance with NIST SP-800-543 PE-3, that they did not have—and subsequently took control of systems and locked OPM employees out.[43] DOGE operatives have accessed sensitive information in both BFS and OPM's EHRI

---

individuals as defined by the act, and prohibits misuse of that information, while FISMA applies broadly to all information maintained by such agencies without making specific prohibitions on the use of such information. *See, e.g.*, Office of Privacy and Open Government, *Privacy Laws, Policies, and Guidance*, U.S. Dep't of Commerce (accessed Feb. 10, 2025) https://www.commerce.gov/opog/privacy/privacy-laws-policies-and-guidance.

[39] 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 [hereinafter "NIST SP-800-53"].

[40] *Id.* at 172–73 ("MP-4: Media Storage").

[41] *Id.* at 181–83 ("PE-3: Physical Access Control").

[42] *Id.* at 176 ("MP-7: Media Use"); *id.* at 411 ("portable storage device").

[43] Reid, *Musk Aides Lock Workers out of OPM Computer Systems*, *supra* note 4.

system, reportedly connecting commercial servers to those networks,[44] and in other cases have refused to identify themselves,[45] raising serious concerns about compliance with NIST SP-800-53, which instructs, *inter alia*, that certain system actions should be attributable to an individual user.[46]

The magnitude of the harm heightened by unauthorized access to either the BFS system or OPM employment databases cannot be overstated. Both systems contain voluminous PII from millions of Americans, including Doe 1 and EPIC's individual members; unauthorized access provides ample opportunity for financial gain or retaliation against enemies. Similarly, the treasure trove of information from individual Americans—including federal employees—is of significant value and interest to foreign adversaries.[47] DOGE operatives' non-compliance with security protocols intended to safeguard those systems against malicious activities makes the systems more vulnerable to attack.[48] Providing access to these systems to individuals with neither legal authority nor any legitimate need to access them is inconsistent with even the most basic of security

---

[44] Rashid, *Elon Musk Installs Illegal Server, supra* note 5.
[45] Conrad Quilty-Harper, *Musk's DOGE Minions Refuse to Reveal Their Names When Grilling Civil Servants*, Yahoo News (Feb. 4, 2025), https://www.yahoo.com/news/musk-doge-minions-refuse-reveal-142347032.html.
[46] NIST SP-800-53, A-10 ("Non-Repudiation").
[47] *See* C.R.S., *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, (July 17, 2015), https://sgp.fas.org/crs/natsec/R44111.pdf (discussing motive for OPM cyber breaches and nothing "Theft of . . . PII may be used for identity theft and financially motivated cybercrime, such as credit card fraud. Many have speculated that the OPM data were taken for espionage . . . some have cited China as the source of the breaches.").
[48] Derek B. Johnson, *Cybersecurity, government experts are aghast at security failures in DOGE takeover*, Cyberscoop (Feb. 4, 2025) https://cyberscoop.com/musk-doge-opm-treasury-breach/ ("[DOGE] could be exposing the personal data of millions of federal employees, violating federal laws against sharing classified or sensitive information with uncleared individuals and creating new cybersecurity vulnerabilities for malicious hackers to exploit, these experts say. . . the hack and theft of OPM records by Chinese hackers in 2015 is considered among the worst federal security breaches of all time.").

protocols, let alone an elevated set of protections appropriate for such sensitive data and information.

Instead of providing the legally required and necessary security protections for systems of such significance, Treasury and OPM Defendants handed DOGE defendants and other unknown actors the keys to the kingdom, in violation of FISMA and in direct contravention of standard security practices. The BFS system has "long been run by nonpolitical career employees,"[49] and the unprecedented decision to provide access to political appointees is at odds with the system's striking history of success at administering a massive volume of payments.

C. Defendants' actions deprive Plaintiffs of their constitutional right to informational privacy.

Finally, this invasion of informational privacy violates the Constitution. Plaintiffs have a privacy right under the Fifth Amendment "to shield information from disclosure." *Cf. Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 273 (2022). "The constitutional right to privacy extends to . . . the individual interest in avoiding disclosure of personal matters." *Walls v. City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990) (quoting *Whalen v. Roe,* 429 U.S. 589, 599–600 (1997)); *see also Nat'l Aeronautics and Space Admin. v. Nelson*, 562 U.S. 134, 138 (2011).[50] This Circuit asks two questions: whether a person has a "reasonable expectation of privacy" in the relevant information and whether there is "a compelling governmental interest in disclosure [that] outweighs the individual's privacy

[49] Michael Stratford, *Trump administration gives Musk allies access to Treasury payment system*, POLITICO (Feb. 1, 2025), https://www.politico.com/news/2025/02/01/musk-claims-doge-lax-treasury-00201946.

[50] *Dobbs* expressly recognized the right to informational privacy as a discrete component of the constitutional right to privacy more generally. *Dobbs*, 597 U.S. at 273.

interest." *Payne v. Taslimi*, 998 F.3d 648, 655-56 (4th Cir. 2021). Based on the government's own representations, individuals reasonably expect that the government will protect and keep private personal information they provide for purposes of employment or paying taxes.[51] And that presumption is even stronger with regard to financial information; in *Walls*, the Court held that a municipal employee had a reasonable expectation of privacy in such information including "outstanding debts and judgments," such that the employee was entitled to constitutional protection. 895 F.2d at 194.

One the other hand, the government has no compelling interest in disclosure of individuals' private information here. Defendants have not identified what interest DOGE has in the sensitive information in Americans' tax returns or federal employees' profiles, let alone show that any such interest might qualify as compelling. Indeed, given that the DOGE Defendants lack legal authority to undertake this project in the first place, it is not clear that any interest they could articulate could suffice, because to withstand scrutiny of any rigor, the government must as a threshold matter establish that its interest is "legitimate." *See NASA v. Nelson*, 562 U.S. at 143.

II. Plaintiffs continue to suffer irreparable harm from unknown and unaccountable actors' access to their PII.

Plaintiffs' harm is irreparable because once divulged, confidential information cannot be rebottled, and because violations of constitutional rights are always irreparable, no matter how brief. As discussed, DOGE Defendants' continuing access to Treasury and

[51] *See, e.g.*, Internal Rev. Serv., *The Taxpayer Bill of Rights*, https://www.irs.gov/pub/irs-pdf/p1.pdf ("Taxpayers have the right to expect that any information they provide to the IRS will not be disclosed unless authorized by the taxpayer or by law"); OPM, *Declaration for Federal Employment, OF-306*, https://www.opm.gov/forms/pdf_fill/of0306.pdf (identifying "Routine Uses" for Privacy Act purposes).

OPM systems constitutes an ongoing violation of Plaintiffs' informational privacy rights, both statutory (under the Privacy Act and Internal Revenue Code) and constitutional (under the Fifth Amendment). The longer Defendants are permitted unauthorized access to these sensitive systems, the more likely it is that they will access or further disclose Plaintiffs' individual data, and the longer Plaintiffs' data remains at a heightened risk of exposure or exfiltration by hostile actors.[52]

Plaintiffs have standing to bring this suit. Doe 1 is a career civil servant, and OPM therefore retains her sensitive personal information on EHRI, including her Social Security number, home address, and disciplinary record. Doe Decl. (Ex. A) ¶¶ 2, 5. Likewise, both Doe 1 and many of Plaintiff EPIC's members have filed their federal tax returns electronically within the last six years, so BFS systems contain extensive financial information about them, including statutorily protected return information. Doe Decl. (Ex. A) ¶¶ 6, 7; Butler Decl. (Ex. B) ¶¶ 7, 8, 12; Kennedy Decl. (Ex. C) ¶¶ 9-11; Brody Decl. (Ex. D) ¶¶ 9-11; Schneier Decl. (Ex. E) ¶¶ 9-11. Plaintiffs reasonably expected that the information they had provided the government was subject to comprehensive protections against unlawful disclosure. Doe Decl. (Ex. A) ¶¶ 8, 9; Butler Decl. (Ex. B) ¶¶ 9–12; Kennedy Decl. (Ex. C) ¶¶ 12, 13; Brody Decl. (Ex. D) ¶¶ 12, 13; Schneier Decl. (Ex. E) ¶¶ 12, 13. Breaking those expectations in violation of statute injures Plaintiffs in a way that "creates statutory harm and confers standing." *Gaston v. LexisNexis Risk Sols., Inc.*, 483 F. Supp. 3d 318, 343 (W.D.N.C. 2020) (holding that where a "statute specifically

[52] *See* Order at 2, *New York v. Trump*, No. 1:25-cv-01144 (S.D.N.Y., Feb. 8, 2025), ECF No. 6 (describing "firm assessment" that DOGE access to Treasury systems creates "heightened risk that the systems in question will be more vulnerable than before to hacking.").

protects people from all disclosure of personal information . . . except in certain permissible instances . . . impermissible disclosure of a plaintiff's personal information in violation" of that statute gives plaintiffs standing).

Defendants' failure to abide by those protections has injured and continues to injure Plaintiffs. The disclosure of confidential and sensitive information causes substantial and irreparable harm to those to whom the information belongs, because once broken, confidentiality cannot be reestablished. *See X Corp. v. Doe*, 805 F. Supp. 1298, 1304 (E.D. Va. 1992), *aff'd sub nom*. *Under Seal v. Under Seal*, 17 F.3d 1435 (4th Cir. 1994) ("Once confidential attorney-client communications are disclosed, their confidential nature is permanently and irrevocably impaired. . . . [Movant's] right to prevent disclosures of confidential information might be forever lost absent a preliminary injunction."); *CACI, Inc.-Fed. v. United States Navy*, 674 F. Supp. 3d 257, 278 (E.D. Va. 2023) ("because a trade secret, once lost, is of course, lost forever."); *see also Plante v. Gonzalez*, 575 F.2d 1119, 1135 (5th Cir. 1978) ("When a legitimate expectation of privacy exists, violation of privacy is harmful without any concrete consequential damages."). To the extent Defendants have already accessed Plaintiffs' data, they must be immediately restrained from further access or use and required to relinquish whatever access they currently have and destroy any data retained.

Further [where] there is a likely constitutional violation, the irreparable harm factor is satisfied." *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 346 (4th Cir. 2021) (citing *Mills v. District of Columbia*, 571 F.3d 1304, 1312 (D.C. Cir. 2009). It is well established that the deprivation of constitutional rights "unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976). Here, Defendants' actions

deprive the individuals whose information is stored on these systems, including Plaintiff Doe 1 and the members of Plaintiff EPIC, of their constitutional right to determine when it is appropriate to disclose their private information.

Until unauthorized actors no longer have access to these systems, they can easily and immediately misuse PII in violation of law by arbitrarily stopping payments through access to the BFS system, as they have publicly claimed to do.[53] This improper access also creates a heightened risk that it will be used to bring adverse employment actions on the basis of information in the OPM system or use PII gathered from either system for unlawful purposes.[54] Even to the extent DOGE has been granted "read-only" access,[55] that too is unnecessary, and in any event is not permitted by the Privacy Act or the operative

[53] Department of Government Efficiency (@DOGE), X/Twitter (Jan. 28, 2025, 7:20 PM ET), https://x.com/DOGE/status/1884396041786524032 ("DOGE is saving the Federal Government approx. $1 billion/day, mostly from stopping the hiring of people into unnecessary positions, deletion of DEI and stopping improper payments to foreign organizations, all consistent with the President's Executive Orders.").

[54] *See, e.g.*, Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payments System*, The New York Times, Feb. 2, 2021, https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html (access gives administration "another mechanism to attempt to unilaterally restrict disbursement of money approved for specific purposes by Congress"); 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/ (government officials expressed "alarm about . . . abuses of [OPM] records by members of an administration . . . [that has] threatened to retaliate against federal workers accused of disloyalty.").

[55] *See, e.g.*, Order, *Alliance for Retired Americans v. Bessent*, No. 1:25-cv-00313 (D.D.C., Feb. 6, 2025), ECF No. 13.

information system security standards; DOGE employees have no lawful reason to access these systems.

Reports also indicate that operatives connected with DOGE have connected unapproved information technology to government systems.[56] In addition to violating security and privacy standards under FISMA, these unprecedented uses of government networks risk exactly what FISMA was designed to prevent, and significantly increase the vulnerability of the information in these systems: according to one OPM employee, the "access leaves federal employee data unsecured and vulnerable to hackers."[57] As long as PII or other sensitive information remains on unsecured and unmanaged information technology under the control of DOGE Defendants, that heightened risk of infiltration remains. This presents a "substantial risk" *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017) (quoting *Clapper v. Amnesty International*, 568 U.S. 398, 414 n.5 (2013)), of plaintiffs suffering future identity theft. It is "no secret" that OPM's "network is regularly subject to a strikingly large number of hacking attempts" *In re OPM Data Security Breach Litigation*, 928 F.3d 42, 51 (D.C. Cir. 2019) aimed at the theft of personal information. As a result of the increased vulnerability introduced by Defendants' actions, these attempts are now more likely to be successful.

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

The final two factors "merge when the Government is the opposing party," *Miranda*, 34 F.4th at 365 (quoting *Nken*, 556 U.S. at 435), and here, both favor plaintiffs. The government cannot suffer harm from an injunction that merely ends an

[56] Rashid, *supra* note 5.
[57] Rashid, *supra* note 5.

unlawful action because "'a state is in no way harmed by issuance of a preliminary injunction which prevents the state from enforcing restrictions likely to be found unconstitutional,'" *Leaders*, 2 F.4th at 346 (internal citations omitted), or which "merely ends an unlawful practice or reads a statute as required." *R.I.L-R v. Johnson*, 80 F. Supp. 3d 164, 191 (D.D.C. 2015) (quoting *Rodriguez v. Robbins*, 715 F.3d 1127, 1145 (9th Cir. 2013)). "If anything, the system is improved by such an injunction." *Centro Tepeyac v. Montgomery Cnty.*, 722 F.3d 184, 191 (4th Cir. 2013). "There is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016). "To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws—such as the APA, as well as regulations . . .that govern their existence and operations." *Open Communities Alliance v. Carson*, 286 F. Supp. 3d 148, 179 (D.D.C. 2017) (internal quotation marks and citations omitted). These principles should end all inquiry on the third and fourth temporary restraining order factors: plaintiffs' requested relief would impact only unlawful activities.

But even if this Court were to consider Defendants' interests as if they were private parties, the balance of equities and public interest would still overwhelmingly favor plaintiffs. Neither Defendants nor any of their associates have identified any lawful or legitimate need or reason for their seizure of government information systems. According to the E.O. creating DOGE, its purpose is to modernize government information systems.[58] But the access granted to DOGE is not necessary for that purpose, nor does the E.O. permit DOGE to violate the law.

[58] Exec. Order No. 14158 § 4(a).

Far from confining themselves to lawful justifications, Defendants and their associates have identified and threatened *unlawful* reasons: the withholding of legally obligated payments,[59] and the distribution of purported severance offers without authorizing appropriations.[60] The unlawful agenda of Defendants and their associates may suffer from the entry of a temporary restraining order, but their legally mandated operations would in fact be improved by restoration of normal order.

And plaintiffs, along with tens of millions of other Americans, including similarly situated federal employees, applicants, and taxpayers, would benefit as a result. A temporary restraining order would eliminate an active risk to taxpayer and federal employee privacy carrying real threats of identity theft or other malicious action, and would prevent both accidental and purposeful disruption of government payments.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court grant their motion and enter a temporary restraining order enjoining OPM Defendants and Treasury Defendants from allowing unauthorized or unlawful access to their information systems, and enjoining DOGE Defendants from accessing EHRI or BFS systems. Plaintiffs also request that the Court order Defendants to file a status report within twenty-four hours of the issuance of any temporary restraining order confirming that DOGE Defendants no longer have access to EHRI or BFS systems.

---

[59] *See* Elon Musk (@elonmusk), X/Twitter (Feb. 2, 2025, 3:14 AM ET), https://x.com/elonmusk/status/1885964969335808217 (claiming that DOGE is "shutting down [certain] illegal payments).

[60] *See* OPM, *Fork in the Road*, opm.gov/fork (government-wide email purporting to offer "deferred resignation program").

Dated: February 12, 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

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)

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

* pro hac vice *application forthcoming*

Counsel for Plaintiffs