UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Alliance for Retired Americans, et al., Plaintiffs, v. Scott Bessent, in his official capacity as Secretary of the Treasury, et al., Defendants.	Civil Action No. 25-313 (CKK)

MEMORANDUM IN SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT

Norman L. Eisen
(DC Bar No. 435051)
State Democracy Defenders Fund
600 Pennsylvania Avenue SE
#15180
Washington, DC 20003

Nandan M. Joshi
(DC Bar No. 456750)
Nicolas Sansone
(DC Bar No. 1686810)
Allison M. Zieve
(DC Bar No. 424786)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

April 25, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Federal Register

Other Authorities

INTRODUCTION

On his first day in office, President Trump launched an all-of-government endeavor for the stated purpose of modernizing federal technology. To achieve that goal, he established the so-called Department of Government Efficiency (DOGE) and provided that the U.S. Digital Service (USDS) in the Executive Office of the President would coordinate implementation of his "DOGE agenda" across federal agencies. DOGE Teams dispatched to multiple federal agencies gained access to federal information systems, including the sensitive personal information of millions of Americans stored in those systems.

Defendant Department of the Treasury was one of the first agencies to welcome a DOGE Team into its ranks. Within days of arriving, the Treasury Department granted the DOGE Team access to the computer systems of Defendant Bureau of the Fiscal Service (Bureau), and to the sensitive personal and financial information of millions of individuals who engage in financial transactions with federal agencies. These individuals include Social Security recipients, federal workers, and taxpayers. Plaintiffs' members are among the many whose personal information is now available to DOGE.

The Privacy Act and the Internal Revenue Code (IRC) constrain federal agencies' ability to do as they wish with personal information. And when an agency changes how it manages that information, the Administrative Procedure Act (APA) requires that the agency act in accordance with law and make decisions that are not arbitrary and capricious. In their zeal to implement the President's DOGE agenda as quickly as possible, however, Defendants brushed their legal duties aside and granted the Treasury DOGE Team unfettered access to people's most sensitive personal and financial data. This action is unlawful. This Court should grant Plaintiffs' motion for summary judgment, deny Defendants' motion to dismiss and for summary judgment, and enjoin Defendants from permitting the Treasury DOGE Team to access personal information in the Bureau's systems.

BACKGROUND

Statutory Framework

Privacy Act. Congress enacted the Privacy Act in 1974 "to protect the privacy of individuals in [federal] information systems." *Dep't of Agric. Rural Dev. Rural Housing Serv. v. Kirtz*, 601 U.S. 42, 63 (2024) (quoting Pub. L. No. 93-579, 88 Stat. 1896 § 2(a)(5)). The Privacy Act provides "safeguards for an individual against an invasion of personal privacy by requiring Federal agencies ... to ... 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 misuse of such information." *Id.* § 2(b)(4). The statute also requires agencies to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity." 5 U.S.C. § 552a(e)(10).

Under the Privacy Act, an agency must publish a notice of "the existence and character of [its] system[s] of records" in the Federal Register when such systems are established or revised. *Id*. § 552a(e)(4). Among other things, this "System of Records Notice" (SORN) must describe "each routine use of the records contained in the system, including the categories of users and the purpose of such use," and "the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records." *Id*. § 552a(e)(4)(D), (E). A "routine use" is "the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7). When an agency seeks to establish or revise its routine uses, it must provide the public with 30 days' advance notice and provide interested persons an opportunity to comment. *Id*. § 552a(e)(11). In addition, when an agency "proposes to establish or make a significant change in a system of records," the Privacy Act also requires the agency to "provide adequate advance notice of any such proposal" to designated congressional committees and the

Office of Management and Budget (OMB) "to permit evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals." *Id*. § 552a(r).

The Privacy Act provides that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency," unless the "individual to whom the record pertains" consents to the disclosure or a statutory exception applies. 5 U.S.C. § 552a(b). One exception permits disclosure "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *Id*. § 552a(b)(1). Another permits disclosure under a routine use described in a SORN. *Id*. § 552a(b)(3).

Internal Revenue Code. Congress has enacted heightened protections for information that taxpayers submit in connection with tax filings. Under 26 U.S.C. § 6103(a), "[r]eturns and return information shall be confidential." A "return" includes "any tax or information return" or "claim for refund." *Id.* § 6103(b)(1). "Return information" includes "a taxpayer's identity" and "or any other data, received by, recorded by, prepared by, furnished to, or collected" in connection with federal taxes. *Id.* § 6103(b)(2)(A). Section 6103(a) provides that "no officer or employee of the United States" may disclose return or return information unless the disclosure is expressly authorized. With respect to the Treasury Department, section 6103 permits disclosure to "officers and employees ... whose official duties require such inspection or disclosure for tax administration purposes," *id.* § 6103(h)(1), which encompasses "the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes." *Id.* § 6103(b)(4).

Privacy Standards for Bureau Systems

The Bureau's Records on Individuals. The Treasury Department is responsible for managing the finances of the U.S. Government, including collecting receipts owed to the government and making payments to recipients of public funds. 31 U.S.C. §§ 3301, 3321. The Bureau is a component within the Treasury Department charged with handling the government's receipts and disbursements. *See* Treas. Order 136-01 (Oct. 7, 2012), *published*, 78 Fed. Reg. 31629 (May 24, 2013). The Bureau's role is to "collect revenue, delinquent debt, and disburse funds to millions of Americans ensuring their timely receipt of benefit payments."[1] In fiscal year 2023, the Bureau collected "$5.47 million in federal revenue, with 99.9% of receipts settled electronically."[2] The Bureau also disbursed 87.8% of the U.S. Government's payments, totaling $5.46 trillion. Robinson Decl. ¶ 2, ECF 24-4.

To conduct payment and collection activities, the Bureau operates several systems that contain sensitive personal information about individuals. The following payment systems have been the focus of the Treasury DOGE Team's activities:

- *Payment Automation Manager (PAM)*. PAM is the primary system used by the Bureau to process payments for disbursements. Gioeli Decl. ¶ 6, ECF 24-2.
- *Secure Payment System (*SPS*)*. SPS is used by agencies to "create, certify, and submit individual payment files to Treasury" and for "one-time large dollar amount transactions." *Id*. ¶ 8.

[1] Bur. of the Fiscal Serv., Services for The General Public, https://www.fiscal.treasury.gov/public/ (Ex. A). Exhibits designated in this memorandum are exhibits to the declaration of undersigned counsel filed concurrently herewith.

[2] Bur. of the Fiscal Serv., About Us, https://www.fiscal.treasury.gov/about.html (Ex. B).

- *Automated Standard Application for Payments (ASAP)*. ASAP is a payment system that is initiated by the recipient and allows recipients to "draw down funds from an established account." *Id*. ¶ 7.
- *International Treasury Services (ITS)*. ITS is used to make international payments, including Social Security payments for Americans living abroad. *Id*. ¶ 9.
- *Central Accounting and Reporting System (CARS)*. CARS is used to record financial data on agency spending and enable agency reporting for accounting purposes. *Id*. ¶ 10.

In addition to these payment systems, the Bureau operates a Payment Information Repository System (PIRS). PIRS is a "centralized information repository for federal payments."[3] PIRS "holds information on all payments that both Treasury and Non-Treasury Disbursing Offices make."[4]

The Bureau's Privacy Documents. In accordance with the Privacy Act, the Bureau has published SORNs addressing systems that contain records on individuals. *See* 85 Fed. Reg. 11776 (Feb. 27, 2020). For instance, SORN .002 applies to records on "individuals who are the intended or actual recipients of payments disbursed by the United States Government." *Id*. at 11779. Personal information contained in this system of records includes "a payee's name, Social Security number, … date and location of birth, physical and/or electronic mailing address; telephone numbers; … financial institution information, including the routing number of his or her financial institution and the payee's account number at the financial institution." *Id*.

[3] Treas. Fin. Experience, Payment Information Repository (PIR), https://tfx.treasury.gov/taxonomy/term/10678 (Ex. C).

[4] Bur. of the Fiscal Serv., Payment Info. Repository, https://fiscal.treasury.gov/pir/ (Ex. D).

The Treasury Department has also issued a Privacy Act Handbook that further outlines the agency's "guidelines and procedures for employees who maintain, collect, use, disseminate or amend records about individuals."[5] The Handbook explains that a SORN must be published "[w]hen establishing or making significant/major alterations/modifications to a system of records." Privacy Act Handbook 20–21. For "minor changes," the Handbook requires prior internal notice to the Office of Privacy, Transparency, & Records, along with a "memorandum demonstrating that the modification is not significant." *Id*. at 21.

Consistent with 5 U.S.C. § 552a(r), the Handbook also requires the agency to report to Congress and OMB "when an alteration to an existing system … changes the purpose for which the information is used" or "changes the equipment configuration, hardware, and/or software that creates substantially greater access to the records in the system." *Id*. at 22. An "alteration" is defined broadly to include "[a]ny change to an existing system of records," including changes that "create the potential for either greater or easier access." *Id*. at 7. The report must explain "the probable or potential effect of the proposed new or altered/modified system of records on the privacy or other personal rights of individuals," "the personnel who will have access," and a "description of the steps taken by the agency to minimize the risk of unauthorized access." *Id*. at 23–24. As the Handbook recognizes, this report "provide[s] an opportunity for U.S. citizens and legal permanent residents to examine the effect the new system of records might have on them." *Id*. at 22.

The Treasury Department has also published a Privacy Program Plan to implement OMB's Circular A-130 guidance "for effectively managing Personally Identifiable Information (PII) as a

[5] U.S. Dep't of Treas., Off. of Deputy Ass't Sec. for Privacy, Transparency, & Records, Privacy Act Handbook, TD P 25-04, at 6 (Ex. E).

strategic resource."[6] The Plan identifies privacy controls based on "the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act." Privacy Program Plan 15. These include the principles that "Treasury will be transparent and provide notice to the public regarding its collection, use, sharing, and maintenance of PII," "Treasury will use PII solely for the purposes specified in required notices," any external sharing "will be done in a manner compatible with the purpose for which the PII was originally collected," and "Treasury will protect PII (in all media) through appropriate security safeguards." *Id*.

The safeguards established by the Privacy Program Plan are derived from guidance developed by the National Institute of Standards and Technology (NIST).[7] NIST guidelines incorporate principles such as "separation of duties" and "least privilege" to protect information systems. Separation of duties protects against abuse by "dividing mission or business functions and support functions among different individuals or roles." NIST SP 800-53, at 36. Least privilege "allow[s] only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks." *Id*. The principle of least privilege ensures that personnel "are only given the minimum privileges necessary for satisfying organizational mission/business needs." NIST SP 800-53, at 24.

DOGE Activities at the Bureau

The DOGE Executive Order. President Trump established DOGE by executive order on January 20, 2025. Exec. Order 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025) (DOGE Executive Order). The DOGE Executive Order did not create DOGE as a single entity with a fixed structure or

[6] U.S. Dep't of Treas., Privacy Program Plan (ver. 1.1 Sept. 18, 2024), https://home.treasury.gov/system/files/236/Department-of-the-Treasury-Privacy-Program-Plan.pdf (Ex. F).

[7] NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Fed. Info. Sys. and Orgs. (NIST SP 800-53) (Ex. G) (last updated Dec. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

leadership. Under the executive order, the United States Digital Service was "publicly renamed" the "United States DOGE Service (USDS)" and "established" in the Executive Office of the President. *Id*. § 3(a), 90 Fed. Reg. at 8441. The order also "established" a "USDS Administrator," who reports to White House Chief of Staff Susan Wiles and is within the Executive Office of the President. *Id*. § 3(b). "[W]ithin USDS," the executive order establishes "the U.S. DOGE Service Temporary Organization" pursuant to 5 U.S.C. § 3161, which is to be led by the USDS Administrator and "dedicated to advancing the President's 18-month DOGE agenda." *Id*.

Executive Order 14158 directs agency heads to establish "a DOGE Team of at least four employees" at each agency. *Id*. § 3(c). Agency heads must consult with the USDS Administrator when selecting DOGE Team members and must "ensure that DOGE Team Leads coordinate their work with USDS and advise their respective Agency Heads on implementing the President's DOGE Agenda." *Id.*

The Executive Order does not define the "DOGE Agenda," except to note that it is to be achieved "by modernizing Federal technology and software to maximize governmental efficiency and productivity." *Id*. § 1. To that end, the Executive Order directs 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" and directs the USDS Administrator to "work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization." *Id*. § 4(a). Agency heads, in turn, must "take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS

has full and prompt access to all unclassified agency records, software systems, and IT systems." *Id*. § 4(b).[8]

The Treasury DOGE Team. DOGE moved rapidly to establish a Treasury DOGE Team. Almost two weeks before the inauguration, the transition team named Thomas Krause to the "day 1 team" at the Treasury Department. Supp. AR 1.[9] A second Treasury DOGE Team Member, Special Advisor Marko Elez, was also assigned to the Treasury Department in advance of the inauguration. *See* AR 28. Mr. Elez formally began work at the Treasury Department on January 21, 2025, and Mr. Krause began two days later on January 23, 2025. *See* AR (Elez); Krause Decl. ¶ 11, ECF 24-1.

Mr. Krause has not had a consistent or clearly defined role at the Treasury Department.[10] Appointed as a consultant, Mr. Krause's initial job description called on him to "lead[] IT modernization efforts by implementing emerging technologies such as AI, blockchain, and cloud

[8] Other executive orders delegate additional responsibilities to DOGE or its components. *See* Exec. Order 14270, 90 Fed. Reg. 15643 (Apr. 15, 2025) (requiring agencies to coordinate with DOGE Team Leads on sunsetting regulations); Exec. Order 14269, 90 Fed. Reg. 15635 (Apr. 15, 2025) (requiring DOGE to provide recommendations on maritime matters); Exec. Order 14248, 90 Fed. Reg. 14005 (Mar. 28, 2025) (requiring Department of Homeland Security and DOGE Administrator to review state voter registration databases); Exec. Order 14222, 90 Fed. Reg. 11095 (Mar. 3, 2025) (directing DOGE Team Leads to provide the USDS Administrator reports on agency contracting and travel); Exec. Order 14219, 90 Fed. Reg. 10583 (Feb. 25, 2025) (directing agency heads to coordinate with DOGE Team Leads on review of existing regulations); Exec. Order 14218, 90 Fed. Reg. 10581 (Feb. 25, 2025) (requiring OMB and USDS to identify sources of federal funding for individuals present without authorization); Exec. Order 14210, 90 Fed. Reg. 9669 (Feb. 14, 2025) (addressing "Workforce Optimization"); Exec. Order 14170, 90 Fed. Reg. 8621 (Jan. 30, 2025) (delegating to the "Administrator of the Department of Government Efficiency" (an undefined position) the duty to advise on a "hiring plan"); Hiring Freeze, Memorandum, 90 Fed. Reg. 8247 (Jan. 28, 2025) (requiring consultation with USDS Administrator on a workforce reduction plan).

[9] "AR" refers to the administrative record docketed at ECF 44-1. "Supp. AR" refers to the supplemental administrative record docketed at ECF 48-1. The pages identified by the Bates stamp on the AR and Supp. AR are used for page numbering.

[10] Mr. Elez's role was to serve as a confidential advisor to Mr. Krause. *See* AR 22.

computing while ensuring compliance with federal IT policies," to "oversee[] the modernization of legacy systems, integrating real-time analytics, automation, and enhanced data sharing capabilities across agencies," to "strengthen cybersecurity protocols," and to "foster[] public-private partnerships with financial institutions, technology firms, and regulatory agencies." AR 15.

Other hiring paperwork describes Mr. Krause's job duties differently: "to execute [the Bureau's] mission of promoting the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services," with focus areas "including but not limited to (1) Operational Resiliency; (2) Advancing Governmentwide Payment Integrity; (3) Critical Modernization Programs; (4) Improving the Payment Experience; and (5) TreasuryDirect User Credential Costs." AR 21; *see also* Wenzler Decl. ¶ 6, ECF 24-3.

Mr. Krause himself uses other formulations to describe his role. He states that his position was "created to help effectuate [DOGE's] mission" and that, as the team lead of the Treasury DOGE Team, he is responsible "for reducing and eliminating improper and fraudulent payments; waste, fraud, and abuse; and improving the accuracy of financial reporting" by "improving the controls, processes, and systems that facilitate payments and enable consolidated financial reporting." Krause Decl. ¶ 2. He also "find[s] ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of this Administration." *Id*. ¶ 4; *see also* Defs.' Response to Interrog. #1, at 6, ECF 61-2. To that end, he "coordinate[s] with officials at USDS/DOGE, provide[s] them with regular updates on the team's progress, and receive[s] high-level policy direction from them." Krause Decl. ¶ 4.

The DOGE Team's Initial Work. The Treasury DOGE Team's initial work focused on two projects: the payment processing engagement plan and implementation of Executive Order

14169, 90 Fed. Reg. 8619 (Jan. 30, 2025) (Foreign Aid Executive Order), which directed agencies to pause certain foreign aid payments. Defs.' Response to Interrog. #2, at 7.

Payment processing engagement plan. According to Mr. Krause, "an important aspect of the President's DOGE efforts [was] to quickly place [him] into the Treasury Department so [he could] understand how BFS's end-to-end payment systems and financial report tools work." Krause Decl. ¶ 11; *see also* AR 60 (reproducing Mr. Krause's preliminary work plan for IT access). On January 24, 2025, the day after Mr. Krause's official start date, the Bureau developed an "engagement plan" to support "the USDS/DOGE team during their 4–6-week engagement to understand payment processes and opportunities." AR 57. The engagement plan sought to "engage in a way that is secure and minimizes the likelihood of disruptions" and avoids "catastrophic consequences" to U.S. financial interests and "the delivery of lifeline payments to millions of constituents." *Id*. With respect to data protection, USDS/DOGE also had to attest "at the end of the engagement" that Bureau "information has been properly destroyed and that "no known or suspicious unauthorized access" had occurred. *Id*. at 59. The engagement plan was "initiated" on January 26, 2025. Krause Decl. ¶ 13.

On January 28, 2025, Defendant Scott Bessent was sworn in as Treasury Secretary. Between January 28 and January 30, Mr. Elez and Mr. Krause were in Kansas City, where the Federal Reserve Bank of Kansas City hosts and maintains several Bureau payment systems, to do a "deep dive" into the Bureau's systems. AR 56; Krause Feb. 10 Decl. ¶ 7, ECF 15-1.

Between January 29 and January 31, the Treasury DOGE Team requested that Mr. Elez receive access to the PAM, SPS, ASAP, CARS, and ITS.gov databases. AR 62; Defs.' Response to Interrog. #5, at 13; Supp. AR 7. On January 31, Secretary Bessent reportedly placed the then-

head of the Bureau on administrative leave after disputes arose about the Treasury DOGE Team's access to Bureau systems.[11]

The following Monday, February 3, the Treasury Department gave Mr. Elez access to Bureau systems. AR 61; Defs.' Response to Interrog. #5, at 13**.** Although Mr. Elez's access was supposed to be "read only," he received a level of access—"a single individual with access to multiple systems and data records"—that "was broader in scope than what has occurred in the past." Gioeli Decl. ¶ 13. "This broad access presented risks, which included potential operational disruptions to Fiscal Service's payment systems, access to sensitive data elements, insider threat risk, and other risks that are inherent to any user access to sensitive IT systems." *Id*. ¶ 12. The Bureau accordingly "developed mitigation strategies that sought to reduce these risks. *Id*. ¶ 11. The record does not indicate, however, that any limits were placed on Mr. Elez's ability to "view and query" sensitive personal information. *Id.* ¶ 17. On February 3, "Mr. Elez was provided read-only access to PAM, and on February 4 and 5, Mr. Elez accessed the PAM database and SPS. *Id.* ¶¶ 18–19.[12]

Mr. Elez resigned from the Treasury DOGE Team on February 6. *Id*. ¶ 22. He has not provided an "attestation statement" that "any copies of Treasury information made would be properly destroyed" and that "no suspicious or unauthorized access to Bureau information or data had occurred during the engagement," as required by the Bureau's risk-mitigation measures. Gioeli Decl. ¶ 14; Defs.' Response to Req. for Admis. #3, at 5 (Ex. H).

---

[11] Jeff Stein et al., *Senior U.S. official to exit after rift with Musk allies over payment system*, Wash. Post, Jan. 31, 2025; *See* Andrew Duehren et al., *Treasury Official Quits After Resisting Musk's Requests on Payments*, N.Y. Times, Jan. 31, 2025.

[12] Mr. Elez also had access to the CARS Application "leveraging a read-only auditor role." Gioeli NY Decl. ¶ 16, *New York v. U.S. Dep't of the Treasury*, No. 1:25-cv-1144-JAV (S.D.N.Y. Mar. 5, 2025), ECF 98-2.

Throughout this period, Mr. Krause was granted "over the shoulder" access to the Bureau's payment systems and source code. Gioeli Decl. ¶ 4. Over-the-shoulder access provides an individual with authority "to view a computer system while in physical proximity (or virtual proximity, such as through screen-sharing) with another person who has logical access and permissions." Gioeli NY Decl. ¶ 9. Despite this access limitation, Mr. Krause received "updates" from Mr. Elez, including "screenshots of payment systems data or records." Gioeli Decl. ¶ 4. In addition, between January 28 and February 5, 2025, Mr. Krause and Mr. Elez made several requests for payment data, which Bureau staff retrieved from PIRS. Defs.' Response to Interrog. #1, at 6.

Flagging foreign aid payments. Although the Foreign Aid Executive Order did not mention DOGE, the Treasury DOGE Team worked to "implement[] a system to assist payor agencies in identifying payments that may be improper" under that executive order. Defs.' Response to Interrog. #2, at 7; Krause Decl. ¶¶ 17–20; Robinson Decl. ¶¶ 7–16. That effort began on January 26, 2025, and was paused on February 10. Robinson Decl. ¶¶ 8, 15.

On January 28, Mr. Krause received an email that he requested containing a spreadsheet entitled "USAID Payment request payment dates 1.21 through 1.24 updated." This file contained payment data about USAID payments, including the name of the payee. Defs.' Response to Interrog. #6, at 14; *see* Elez Email to GSA (Ex. I). Two days later, Mr. Krause emailed the information to Mr. Elez, who then emailed it to two individuals at the U.S. General Services Administration (GSA). Response to Interrog. #6, at 14–15; Ambrose Decl. ¶ 12, ECF 48-2.

Separately, on February 4 and 5, Mr. Elez copied USAID records directly from the PAM database to his [Bureau] laptop. *See* Gioeli Decl. ¶ 18. These records also contained personal information of the recipients of federal funds. *See* Defs.' Response to Interrog. #6, at 14–15.

LEGAL STANDARD

In evaluating Defendants' motion to dismiss under Rules 12(b)(1) and 12(b)(6), the Court must accept the complaint's allegations as true and draw all reasonable inferences in Plaintiffs' favor. *See Ho v. Garland*, 106 F.4th 47, 50 (D.C. Cir. 2024). As for the Rule 12(b)(1) motion, the Court has "an affirmative obligation … to ensure that it is acting within the scope of its jurisdictional authority" so that the Court may also "consider matters outside the pleadings" without converting the motion to a motion for summary judgment. *Forrester v. U.S. Parole Comm'n*, 310 F. Supp. 2d 162, 167 (D.D.C. 2004) (citation omitted). Accordingly, to the extent that Defendants have "challenged the factual basis of the court's jurisdiction, … the court must go beyond the pleadings and resolve any disputed issues of fact the resolution of which is necessary to a ruling upon the motion to dismiss." *Phoenix Consulting Inc. v. Republic of Angola*, 216 F.3d 36, 40 (D.C. Cir. 2000).

As for the Rule 12(b)(6) motion, this Court must ask whether Plaintiffs' complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). This standard is satisfied where the complaint contains "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* The plausibility standard "is not akin to a 'probability requirement.'" *Id.* (quoting *Twombly*, 550 U.S. at 556). In other words, if "there are two alternative explanations" for the facts alleged, "one advanced by [the] defendant and the other advanced by [the] plaintiff, both of which are plausible," dismissal is inappropriate. *Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1129 (D.C. Cir. 2015) (alterations in original; quoting *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011)). Finally, while "the pleadings must 'give the defendants fair notice of what the claim is and the grounds upon which it rests,'" *Jones v. Kirchner*, 835 F.3d 74, 79 (D.C. Cir. 2016) (quoting

Twombly, 550 U.S. at 555), they need not contain "detailed factual allegations" to survive a Rule 12(b)(6) motion, *id.* (quoting *Iqbal*, 556 U.S. at 678).

The parties' summary judgment motions are governed by Federal Rule of Civil Procedure 56, which requires a court to grant summary judgment "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). In APA cases, however, "the summary judgment standard functions slightly differently." *Ashtari v. Pompeo*, 496 F. Supp. 3d 462, 467 (D.D.C. 2020) (citation omitted). Because "the reviewing court generally ... reviews the agency's decision as an appellate court addressing issues of law," limiting its review "to the administrative record and the facts and reasons contained therein to determine whether the agency's action was consistent with the relevant APA standard of review," the "entire case on review is a question of law, and only a question of law." *Id.* (omission in original; citation omitted).

ARGUMENT

I. THE COURT SHOULD REACH THE MERITS OF PLAINTIFFS' CLAIMS.

A. Plaintiffs have standing.

Article III's standing requirement ensures that a plaintiff bringing a federal lawsuit "has 'such a personal stake in the outcome of the controversy as to warrant [the] invocation of federal-court jurisdiction.'" *Murthy v. Missouri*, 603 U.S. 43, 57 (2024) (quoting *Summers v. Earth Island Inst.*, 555 U.S. 488, 492 (2009)). Where the plaintiff is an organization that asserts standing "solely as the representative of its members," standing is established if the members, "or any one of them, are suffering immediate or threatened injury as a result of the [defendant's] challenged action of the sort that would make out a justiciable case had the members themselves brought suit," *Warth v. Seldin*, 422 U.S. 490, 511 (1975), provided that "the interests [the organization] seeks to protect are germane to the organization's purpose" and "neither the claim asserted nor the relief requested

requires the participation of individual members in the lawsuit," *Hunt v. Wash. State Apple Advertising Comm'n*, 432 U.S. 333, 344 (1977).

Here, Defendants do not challenge this Court's preliminary determination that these latter two requirements are satisfied. *See* Prelim. Inj. Mem. Op. 24–25, ECF 42. Defendants challenge only whether Plaintiffs' members "would … have standing to sue in their own right." *Hunt*, 432 U.S. at 344. Plaintiffs meet this requirement as well. They have submitted declarations from members whose personal information Defendants wish to expose to DOGE and who are "disturbed, anxious, and frustrated" as a result of this threatened breach of their privacy. *See, e.g.*, Decl. of Carol Rosenblatt ¶ 10, ECF 16-2. The imminent injury to Plaintiffs' members' privacy interests (or "substantial risk" thereof) is concrete and particularized, causally connected to Defendants' challenged actions, and redressable through prospective relief barring Defendants from giving DOGE unlawful access to the personal data stored in Defendants' records. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). As this Court has preliminarily concluded, then, *see* Prelim. Inj. Mem. Op. 33, Plaintiffs' members would have standing to pursue the claims that Plaintiffs raise here.

The only aspect of the foregoing analysis that Defendants dispute is the showing of injury. According to Defendants, the privacy harms that Plaintiffs' members will suffer if Defendants give DOGE unlawful access to their personal data are insufficiently concrete to support standing. The common law, however, has long recognized that "an intentional interference with [one's] interest in solitude or seclusion, … as to [one's] affairs or private concerns, of a kind that would be highly offensive to a reasonable person" is a legally redressable injury. Restatement (Second) of Torts § 652B, cmt. a (1977). Because the privacy injuries asserted here bear "a 'close relationship'" to that "'traditionally' recognized" injury of an intrusion upon seclusion, Plaintiffs' members'

injuries are "concrete for purposes of Article III" standing. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021) (quoting *Spokeo v. Robins*, 578 U.S. 330, 341 (2016)).

Nonetheless, Defendants fault Plaintiffs for failing to show that DOGE's anticipated "*uses* of [their members'] confidential information … [will] result in concrete injury" such as defamation or the disclosure of their private affairs. Defs.' Mem. 14. Defendants, though, disregard that Defendants' intrusion into Plaintiffs' members' "affairs or private concerns," Restatement (Second) of Torts § 652B, cmt. a, is *itself* a legally cognizable harm, even absent some additional injurious follow-on consequence. *See id.* § 652B, cmt. b ("The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the … information [accessed]."). Where an individual has a statutory right to keep certain information private, courts have accordingly recognized that the individual has standing to sue when that information is shared in alleged violation of the law. *See, e.g.*, *Salazar v. Paramount Global*, — F.4th —, 2025 WL 1000139, at *2–3 (6th Cir. Apr. 3, 2025); *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 540–44 (2d Cir. 2024), *cert. petition filed*, No. 24-994 (U.S. Mar. 14, 2025); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 272–74 (3d Cir. 2016); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019); *Feldman v. Star Trib. Media Co.*, 659 F. Supp. 3d 1006, 1013–16 (D. Minn. 2023).

Defendants miss the point when they emphasize that Plaintiffs have not alleged that "any member of the Treasury DOGE Team has ever actually accessed any of their members' data." Defs.' Mem. 14. Plaintiffs' suit for declaratory and injunctive relief aims to *prevent* unlawful access, which Defendants admit could occur without the knowledge of Plaintiffs' members. *See id.* at 17 ("Plaintiffs' members would have no reason to know that a particular employee has accessed their information in the normal course of that employee['s] duties."). And to the extent

that Defendants suggest (without squarely arguing) that the risk of DOGE personnel accessing personal data is speculative, Defendants themselves represent that the DOGE Team's work "requires a thorough review of payment transactions, payment information, and payee information databases" that contain personal data such as Social Security numbers and banking information. Defs.' Statement of Undisputed Material Facts 10, ECF 61-3; *see* Defs.' Mem. 28 (discussing DOGE's interest in tax payments); Defs.' Response to Interrog. #3, at 10 (discussing personal data implicated by DOGE's "end-to-end system review" of "payment transactions, payment information, and payee information databases").

Ultimately, Defendants devote the bulk of their argument to contending that the threatened privacy violation does not resemble a common-law intrusion upon seclusion. First, Defendants argue that allowing DOGE to access Treasury records would create "no … intrusion into Plaintiffs' members' private space," and they contrast Plaintiffs' claims with cases where a defendant has disrupted "the tranquility of the plaintiffs' use of their personal property," as by sending unwanted text messages or other communications. Defs.' Mem. 15–16. But even setting aside that courts have recognized that individuals "have a property interest in their personal information," *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (collecting cases), the government draws no principled line between the annoyance of receiving an unwanted text message—which it appears to accept is sufficient to support standing, *see* Defs.' Mem. 15—and being made "disturbed, anxious, and frustrated" by having one's personal information exposed to those who should not have it. *See, e.g.*, Rosenblatt Decl. ¶ 10. And again, courts have recognized that unlawful access to private information is sufficiently analogous to a traditional intrusion upon seclusion to create an Article III injury. *See supra* at 16–17.

Although Defendants rely heavily on Judge Richardson's concurrence in the grant of a stay pending the government's appeal in *American Federation of Teachers v. Bessent*, 2025 WL 1023638 (4th Cir. Apr. 7, 2025), that concurrence also recognizes that "intrusion upon seclusion can occur beyond the confines of the home" and that "[p]rying eyes and probing fingers can be as disquieting when aimed at one's private affairs as when aimed at one's private bedroom." *Id.* at *5 (Richardson, J., concurring). To be sure, the concurrence opines that harm arising from an unauthorized individual viewing "information [in] one row in various databases" is "different in kind, not just in degree, from the harm inflicted by reporters, detectives, and paparazzi." *Id.* But another court in this District and a district court within the Fourth Circuit have recently declined to follow Judge Richardson's reasoning, and this Court should do the same. *See Am. Fed. of State, Cnty. & Mun. Emps., AFL-CIO v. Soc. Sec. Admin.*, — F. Supp. 3d —, 2025 WL 1141737, at *27–42 (D. Md. Apr. 17, 2025) (*AFSCME*), appeal filed, No. 25-1411 (4th Cir.); *Am. Fed'n of Labor & Congress of Indus. Orgs. v. Dep't of Labor*, 2025 WL 1129227, at *6–10 (D.D.C. Apr. 16, 2025) (*AFL-CIO*). As Judge Bates explained, Congress, in passing legislation like the Privacy Act, "in effect created a new sphere in which individuals not only *expect* privacy, but have a right to it—*i.e.*, a sphere of seclusion." *AFL-CIO*, 2025 WL 1129227, at *8. Because "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law,'" *Spokeo,* 578 U.S. at 341 (alteration in original; quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992)), an "intrusion upon [a] sphere" that Congress has designated as private—"even if the sphere literally encompasses only one row of millions in a dataset—amounts to an injury similar to the intrusion upon other private spheres, such as one's home." *AFL-CIO*, 2025 WL 1129227, at *8; *see also Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021) (holding that "whether [plaintiff] would prevail in a lawsuit for common law

invasion of privacy is irrelevant" in the case of the violation of a statutory privacy right so long as "the harm alleged in her complaint resembles the harm associated with intrusion upon seclusion").

In addition, Defendants emphasize that an intrusion upon seclusion under the common law is not actionable unless it is "highly offensive" to a reasonable person, and argue that the disclosures threatened here do not satisfy that requirement because Plaintiffs' members' personal information can "lawfully be accessed by employees of the [Treasury Department]" for any number of authorized purposes. Defs.' Mem. 17. This argument disregards that this Court "must 'assume [Plaintiffs] will prevail on the merits of their' claims when evaluating their standing to sue." Prelim. Inj. Mem. Op. 26 (alteration in original; quoting *LaRoque v. Holder*, 650 F.3d 777, 785 (D.C. Cir. 2011)). That Plaintiffs might not suffer a cognizable injury from the *lawful* disclosure of their personal information has no bearing on the question whether Plaintiffs suffer concrete injury where—as is claimed here—their personal information is disclosed unlawfully. And as this Court has noted, in the District of Columbia, "conduct giving rise to *unauthorized* viewing of personal information such as a plaintiff's Social Security number and other identifying information can constitute an intrusion that is highly offensive to any reasonable person." *Id.* at 31 (emphasis added; quoting *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009)).

Moreover, Defendants' argument conflates Plaintiffs' members' degree of injury with the type of injury Plaintiffs have alleged. *See Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (explaining that when courts "analogize" statutory violations to "harms recognized by the common law" to assess standing, courts "are meant to look for a 'close relationship' in kind, not degree"); *cf. AFSCME*, 2025 WL 1141737, at *34 ("At least seven circuits … 'have held that receiving either one or two unwanted texts or phone calls resembles the

kind of harm associated with intrusion upon seclusion,' for purposes of standing, even though that harm would not rise to the '*degree* of offensiveness required to state a claim for intrusion upon seclusion at common law'" (quoting *Drazen v. Pinto*, 74 F.4th 1336, 1344 (11th Cir. 2023) (en banc))). Congress has made the determination that certain government records may be disclosed only in certain expressly delineated circumstances, and "[c]ourts must afford due respect to Congress's decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory prohibition or obligation." *TransUnion*, 594 U.S. at 425. Particularly on an issue such as the level of offensiveness that certain conduct must reach before it is actionable—which is "largely a matter of social conventions and expectations," Prelim. Inj. Mem. Op. 31 (quoting J. Thomas McCarthy, *The Rights of Publicity and Privacy* § 5.1(A)(2) (1993))—Congress is particularly "well positioned to identify intangible harms that meet minimum Article III requirements" when assessed against the backdrop of contemporary norms and evolving societal realities. *Spokeo*, 578 U.S. at 341.

This Court should thus confirm its preliminary conclusion that the statutory violations alleged are sufficiently analogous to a common-law intrusion upon seclusion to support standing. What is more, Defendants' intrusion into Plaintiffs' members' private concerns—while sufficient to establish injury—is not the only cognizable injury that creates standing. For one thing, Defendants have breached the "relationship of trust" created when Plaintiffs' members placed sensitive information in their hands. *Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1064 (D.C. Cir. 2019). And as Judge Bates recently explained, "[t]he D.C. Circuit has … recognized that the tort of 'breach of confidence' can serve as a common-law analogue for a harm inflicted by a statutory violation." *AFL-CIO*, 2025 WL 1129227, at *9 (citing *Jeffries*, 928 F.3d at 1064). Defendants claim that Plaintiffs' members' trust derives from "subjective expectations" that "their

information [would] be handled in a certain way," Defs.' Mem. 18, but those expectations derive from statutory guarantees that this Court, in assessing standing, must assume have been violated. As this Court has stated, "[i]t is entirely reasonable for [Plaintiffs'] members to rely on the explicit statutory protections provided by the Privacy Act and the Internal Revenue Code." Prelim. Inj. Mem. Op. 30.

Defendants' actions further create a substantial risk that Plaintiffs' members' private information will be disseminated to additional unauthorized parties. "A person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435. Citing "the extensive security mitigation measures Treasury has employed," Defendants claim that the risk of further dissemination of Plaintiffs' members' data is too "speculative" to support standing, Defs.' Mem. 18, but this Court has noted Defendants' "own admission" that "Treasury's security measures limiting access to [Bureau] records by the Treasury DOGE Team have proven imperfect," Prelim. Inj. Mem. Op. 32 (citing Gioeli Decl. ¶ 20), and Treasury's own internal threat watchdog has advised that "U.S. DOGE Service access to a sensitive payment network represent[s] an 'unprecedented insider threat risk,'" Joseph Menn et al., *Treasury was warned DOGE access to payments marked an 'insider threat'*, Wash. Post (Feb. 7, 2025). Indeed, since this Court's preliminary injunction decision, Defendants have revealed that Mr. Krause obtained a spreadsheet containing personal information of USAID funding recipients, and that Mr. Elez emailed that information to two individuals at GSA without following proper procedures. *See supra* at 13. Thus, the threat of unauthorized disclosure is very real.

Finally, Plaintiffs' members have attested to experiencing the additional concrete injury of emotional distress as a result of Defendants' actions. *See, e.g.*, Rosenblatt Decl. ¶ 10; McElhaney

Decl. ¶ 10, ECF 16-3; Casey Decl. ¶ 10, ECF 16-4. Defendants are wrong to assert that such distress is not a cognizable harm. *See* Defs.' Mem. 18. In *Doe v. Chao*, 540 U.S. 614 (2004), the Supreme Court addressed the Privacy Act claim of an individual whose sole claim of injury rested on his testimony that he was concerned and worried by the disclosure of his Social Security number. *See id.* at 617–18. Although the Court held that this "adverse consequence" was insufficient to allow him to recover a statutory damages award because the Court interpreted the relevant statutory provision to permit recovery only upon a showing of "actual damages," *id.* at 620, the Court recognized that the plaintiff's emotional distress was sufficient to avoid "dismissal for want of standing" and was "injury enough to open the courthouse door." *Id.* at 624–25; *see Mulhern v. Gates*, 525 F. Supp. 2d 174, 184 n.13 (D.D.C. 2007) (holding that allegations that a disclosure caused an individual to "experience emotional distress" were "sufficient to establish an 'adverse effect' of the sort required to confer standing").

Defendants' citation to *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014), *cited at* Defs.' Mem. 18, likewise does not support the proposition that Plaintiffs' members' distress in this case is not a cognizable injury. In *SAIC*, "it was highly unlikely" that an unauthorized third party "understood what the [exposed records] were, let alone had the wherewithal to access them." 45 F. Supp. 3d at 29. Here, it is clear that DOGE knows what it is doing with the personal information it has been collecting from the Bureau. Under such circumstances, the distress of Plaintiffs' members is reasonable, genuine, and sufficiently concrete to establish jurisdiction over their challenge to Defendants' practices.

B. Plaintiffs challenge final agency action.

The APA authorizes judicial review of "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. Reviewable agency action is defined to "include[] the whole or part of an agency rule, order, license, sanction, relief, or the equivalent," *id.* § 551(13),

and the D.C. Circuit has held that "[a]dopting a policy of permitting employees to disclose confidential information without notice" satisfies this definition. *Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008); *see also Chrysler Corp. v. Brown*, 441 U.S. 281, 318–19 (1979) (holding that a "decision to disclose" reports under the Freedom of Information Act "is reviewable agency action" under the APA). Applying this holding, courts have determined that an agency's policy of allowing DOGE access to agency records constitutes final agency action. *See AFSCME*, 2025 WL 1141737, at *51–52; *AFL-CIO*, 2025 WL 1129227, at *12–13; *Am. Fed'n of Teachers v. Bessent*, 2025 WL 895326, at *13–17 (D. Md. Mar. 24, 2025) (*AFT*), *stayed pending appeal*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025); *New York v. Trump*, 2025 WL 573771, at *18–21 (S.D.N.Y. Feb. 21, 2025); *Am. Fed'n of Gov't Emps. v. U.S. Off. of Pers. Mgmt.*, 2025 WL 996542, at *17 (S.D.N.Y. Apr. 3 2025). This Court should do the same.

Arguing otherwise, Defendants recast Plaintiffs' claim as challenging "a loosely defined series of personnel decisions related to granting individual employees access to agency systems." Defs.' Mem. 20. This characterization is not accurate. Plaintiffs challenge a discrete agency decision taken to "effectuate the mission" of the DOGE Executive Order, Krause Decl. ¶ 2, which necessarily involved granting DOGE members access to agency records so that they can carry out the objectives of the DOGE Executive Order, *id*. ¶¶ 11, 15 (asserting that access to sensitive data was needed to carry out DOGE activities); Gioeli Decl. ¶¶ 11–15 (discussing measures implemented to mitigate risks associated with broad access to Bureau systems). Under *Venetian Casino Resort*, this case "presents a live and focused dispute emanating from agency action." 530 F.3d at 931.

Although Defendants invoke *Lujan*'s statement that the APA does not provide for "general judicial review" of an agency's "day-to-day operations," Defs.' Mem. 19 (quoting *Lujan v. Nat'l*

Wildlife Fed'n, 497 U.S. 871, 899 (1992)), that statement has no application here. In *Lujan*, the Supreme Court held that an affidavit challenging an agency's failure to "provide adequate information and opportunities for public participation" in connection with a particular project was insufficiently specific to identify an agency action subject to review. *Lujan*, 497 U.S. at 899. Because no "particular … decision could be identified as the source of the grievance," the Court held that the affidavit failed to "set forth the specific facts necessary" to survive summary judgment. *Id.* Contrary to Defendants' suggestion, then, *Lujan* does not hold that final agency action is unreviewable if it affects an agency's day-to-day operations; rather, *Lujan* holds that an APA challenge must target "an identifiable action or event." *Id*.

Norton v. Southern Utah Wilderness Alliance, 542 U.S. 55 (2004), on which Defendants also rely, is similar. Citing *Lujan*, the Court observed that "[t]he limitation" of the APA's judicial-review provision "to discrete agency action precludes [a] … broad programmatic attack" against an agency's general operations. *Id.* at 64. *Norton* then went on to hold that an APA claim asserting that an agency had failed to manage certain wilderness areas "in a manner so as not to impair the suitability of such areas for preservation as wilderness," *id.* at 65 (quoting 43 U.S.C. § 1782(c)), challenged "[g]eneral deficiencies in [the agency's] compliance" with its statutory mandate, which "lack[ed] the specificity requisite for agency action," *id.* at 66.

Here, unlike in *Lujan* and *Norton*, Plaintiffs "challenge … discrete agency decisions"—the decision "to grant DOGE affiliates access to systems that contain [personal] records"— and they "ask the Court to stop the agencies from taking a specific action that they believe is contrary to law." *AFT*, 2025 WL 895326, at *15; *see New York*, 2025 WL 573771, at *21 (explaining that a challenge to a grant of access to agency records "is not an amorphous component of a large set of 'continuing (and thus constantly changing) [agency] operations,' as was the case in *Lujan*"

(quoting *Lujan*, 497 U.S. at 875)). An agency's "decision to allow [a] DOGE Team access to the [personal data] of millions of Americans[] is a sea change that falls within the ambit of a final agency action." *AFSCME*, 2025 WL 1141737, at *52.

Defendants next argue that even if Defendants' decision is an "agency action," it is not "final" within the meaning of the APA. Agency action is final when it "mark[s] the 'consummation' of the agency's decisionmaking process," that is, it is not "of a merely tentative or interlocutory nature," and the action is one "by which 'rights or obligations have been determined,' or from which 'legal consequences will flow.'" *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (quoting *Port of Bos. Marine Terminal Ass'n v. Rederiaktiebolaget Transatlantic*, 400 U.S. 62, 71 (1970)). Defendants correctly do not dispute that the first prong is satisfied: The decision to grant access to DOGE has been made and implemented. *See U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 598 (2016) (holding that the first finality prong is met when the agency "has ruled definitively"). Defendants argue, though, that no legal consequences flow from their decision to grant DOGE access to Treasury records. Defs.' Mem. 20–22.

Defendants are wrong. An agency's decision has legal consequences when it "alter[s] the legal regime to which the agency action is subject." *Bennett*, 520 U.S. at 178. Before Defendants implemented the DOGE Executive Order, they maintained and enforced privacy policies that would have protected personally identifiable information from the type of unfettered access that the Treasury DOGE Team has been granted. *See supra* at 5–7. Defendants' "decision to provide such broad access to the DOGE Team upended the longstanding policy and practice that has governed [at the Bureau] with respect to access to PII." *AFSCME*, 2025 WL 1141737, at *46 (finding that policy change regarding "guarding the confidentiality and privacy of PII" constituted final agency action).

Defendants concede—as they must—that "unauthorized third-party disclosures" are sufficiently final to be reviewable under the APA because they have "direct and immediate consequences for litigants." Defs.' Mem. 21 (citing *Venetian Casino Resort*, 530 F.3d at 925). But they argue that intragovernmental disclosures are distinct because they "do[ ] not threaten the same immediate harms." *Id.* That distinction does not hold up. Even allowing Defendants' dubious assumption that intragovernmental disclosure is somehow less harmful than third-party disclosure—notwithstanding Congress's explicit choice to provide statutory protections against intragovernmental disclosures of the sort challenged here—the degree of harm caused by an agency action is distinct from the question whether that action is final. And here, the legal effect of Defendants' decision to grant DOGE access to Plaintiffs' members' personal information is just as final as if Defendants had chosen to post that information publicly on their website.

Selectively quoting from *Sierra Club v. EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020), Defendants suggest that their action does not trigger legal consequences because it "imposed no obligations, prohibitions or restrictions on regulated entities" and "did not subject them to new penalties or enforcement risks." Defs.' Mem. 20 (quoting *Sierra Club*, 955 F.3d at 63). In *Sierra Club*, the plaintiffs challenged a guidance document setting forth how the agency would exercise its discretion with respect to permitting decisions. The court held that, "[g]iven the specific nature of the statutory regime, and because the guidance was "*not sufficient* to support a permitting decision" and "also *not necessary* for a permitting decision—permitting authorities are free to completely ignore it," it did not have the legal consequences necessary to show final agency action under the APA. *Sierra Club*, 955 F.3d at 63–64. Here, Defendants have decided that DOGE shall be granted

access to agency records, leaving the decision to the DOGE Team rather than to the individuals affected whether the information will be further disclosed.[13]

Defendants argue that agency action is not final unless it holds "'direct and appreciable legal consequences' for plaintiffs." Defs.' Mem. 21 (quoting *Cal. Cmtys. Against Toxics v. EPA*, 934 F.3d 627, 640 (D.C. Cir. 2019)). To start, as Judge Bates recently concluded, an agency decision of authorizing DOGE's access to personal information *does* "determine the rights of those whose information is being disclosed," as well as "the obligations of the agency." *AFL-CIO*, 2025 WL 1129227, at *13. Accordingly, "just like … in *Venetian Casino* [*Resort*]," Defendants' "policies of unlawfully disclosing information without consent" are final agency action subject to APA review. *Id.*

In any event, the case that Defendants cite in support of this position recognizes that agency action "may be legally consequential because it binds *agency staff* and affected parties have no means (outside of judicial review) by which to challenge it." *Cal. Cmtys. Against Toxics*, 934 F.3d at 638 (emphasis added). Holding otherwise would create an incongruous regime in which a particular agency action could be final as to some plaintiffs but not as to others. Defendants cite no case that has adopted this counterintuitive approach, and courts regularly resolve APA challenges from parties who have suffered injury as a result of a final agency action that does not regulate them directly. *See, e.g.*, *Corner Post, Inc. v. Bd. of Governors of Fed. Reserve Sys.*, 603 U.S. 799, 824 n.9 (2024) (entertaining an APA challenge where the plaintiff had "no other way to

[13] To be sure, Defendants dispute that they have made such a decision. Defs.' Mem. 21. That issue, though, goes to the merits of Plaintiffs' claims and not to their justiciability. In any event, the record belies Defendants' effort to disavow their decision with respect to DOGE's access. *See infra* at 33–36.

obtain meaningful review" of a given regulation because it "d[id] not directly regulate" the plaintiff).

C. Plaintiffs have no adequate alternative remedy to APA relief.

As Defendants note, the APA provides a remedy only where an adequate alternative remedy is unavailable. *See* 5 U.S.C. § 704; Defs.' Mem. 22–25. To determine "whether an alternative remedy is 'adequate' and therefore preclusive of APA review, [courts] look for 'clear and convincing evidence' of 'legislative intent' to create a special, alternative remedy and thereby bar APA review." *Citizens for Responsibility & Ethics in Wash. v. U.S. Dep't of Justice*, 846 F.3d 1235, 1244 (D.C. Cir. 2017) (*CREW*) (quoting *Garcia v. Vilsack*, 563 F.3d 519, 523 (D.C. Cir. 2009)). While "[a]n alternative that provides for *de novo* district-court review of the challenged agency action offers … evidence of Congress' will" to displace an APA remedy, *id.* at 1245, the potency of this evidence is fatally diminished where there is a significant "gap between the *relief* [the alternative] provides and the relief … [sought] under the APA," *id.* at 1246 (emphasis added). For example, the availability of "a naked money judgment against the United States" under an alternative statutory scheme is not necessarily "an adequate substitute for prospective relief" under the APA where a plaintiff seeks "entry of declaratory or injunctive relief that requires the [government] to modify future practices." *Bowen v. Massachusetts*, 487 U.S. 879, 905 (1988); *cf. Garcia*, 563 F.3d at 525 (holding that an alternative remedial scheme was adequate where a successful plaintiff could "obtain declaratory and injunctive relief against [an] agency itself, in addition to money damages, and such remedies would presumably deter [the agency] to the same extent as a successful APA claim").

Here, the primary APA relief that Plaintiffs seek is an injunction barring Defendants from unlawfully granting access to private personal and financial information and requiring Defendants to ensure that no further unlawful disclosure occurs. *See* Compl., ¶ 18, ECF 1. Neither the Privacy

Act nor the IRC offers such relief. *Cf. Bowen*, 487 U.S. at 903 (noting that Congress withheld APA remedies when an adequate alternative remedy already existed so as not to "duplicate existing procedures for review of agency action").

As for the Privacy Act, numerous decisions hold that its remedial scheme does not provide for equitable relief of the sort that Plaintiffs seek here. *See AFSCME*, 2025 WL 1141737, at *52–53 ("The injunctive relief sought by plaintiffs here is not available under the privacy Act."); *AFL-CIO*, 2025 WL 1129227, at *14–16 ("[P]laintiffs' reliance on the Privacy Act does not rob them of an APA cause of action"); *Am. Fed'n of Teachers v. Bessent*, — F. Supp. 3d —, 2025 WL 582063, at *8 (D. Md. Feb. 24, 2025) ("The Privacy Act provides a cause of action for damages when an agency improperly discloses records; it does not provide a cause of action for injunctive relief in these circumstances."); *Am. Fed'n of Gov't Emps.*, 2025 WL 996542, at *15 ("plaintiffs may not obtain declaratory or injunctive relief under the Privacy Act for the violations they have alleged here."); *see also Radack v. U.S. Dep't of Justice*, 402 F. Supp. 2d 99, 104 (D.D.C. 2005) ("Because [plaintiff] seeks declaratory and injunctive relief in addition to damages, the Privacy Act does not provide an 'adequate remedy.'"). As the Supreme Court has observed, the Privacy Act's silence on "standards of proof governing equitable relief" may be "explained by the general provisions for equitable relief within the" APA." *Chao*, 540 U.S. at 619 n.1.

This wall of authority rests on solid ground. After all, the Privacy Act authorizes individuals to seek monetary relief under certain circumstances and provides for injunctive relief directing an agency to amend the individual's records or to produce those records to the individual. 5 U.S.C. § 552a(g)(2)–(4). These forms of relief are entirely distinct from the relief that Plaintiffs seek here. As the Supreme Court has recognized, money damages against the government are not an adequate substitute for "the general equitable powers of a district court" to craft injunctive relief

that preemptively averts the harmful effects of unlawful official conduct before they come to pass. *Bowen*, 487 U.S. at 905; *see AFL-CIO*, 2025 WL 1129227, at *14 ("Damages and injunctions belong to different genres: one compensates for harm while the other prevents it."). And as for the injunctive relief available under the Privacy Act, the difference between an injunction to have one's records corrected or produced on request and an injunction to prevent one's records from being unlawfully disseminated to unauthorized and unaccountable third parties is not merely "some mismatch," but a "yawning gap." *CREW*, 846 F.3d at 1246. The two genres of injunction are wholly different in kind. *See AFL-CIO*, 2025 WL 1129227, at *14 (explaining that injunctive relief under the Privacy Act is available only in situations "involving an agency's *failure* to disclose records whose disclosure the Act compels").

Defendants do not explain why Privacy Act remedies resemble the remedies sought here or why they would "deter [Defendants]" from granting unauthorized third-party access to confidential records "to the same extent [that] a successful APA claim" would. *Garcia*, 563 F.3d at 525. Instead, they quote *Wilson v. Libby*, 535 F.3d 697 (D.C. Cir. 2008), for the proposition that the Privacy Act "provides a 'comprehensive remedial scheme'" and infer from this stray language that Congress intended to preclude all other remedies for Privacy Act violations. Defs.' Mem. 22 (quoting *Wilson*, 535 F.3d at 703). This Court, though, has already explained that the Supreme Court's recent decision in *Kirtz*, 601 U.S. 42, "suggests that the Privacy Act is not the kind of comprehensive and 'exclusive' remedial scheme that impliedly displaces remedies under other statutes." Prelim. Inj. Mem. Op. 35; *see also AFL-CIO*, 2025 WL 1129227, at *15 (citing this Court's analysis with approval). Defendants do not even cite *Kirtz*, let alone identify any flaw in this Court's earlier reasoning.

As for the IRC, Defendants acknowledge that "[c]ivil damages … [are] the sole remedy" available under the statute for a violation of section 6103, and that the relevant remedial provision "does not authorize injunctive relief." Defs.' Mem. 24. The lone case that Defendants cite for the idea that damages under the Code are an adequate substitute for injunctive relief under the APA is a 1988 case from the District of Arizona that did not mention the APA, let alone address an APA claim. *See Agbanc Ltd. v. Berry*, 678 F. Supp. 804, 806–08 (D. Ariz. 1988). The case also predates the Supreme Court's recognition in *Bowen* that the availability of an alternative damages remedy does *not* preclude an APA claim for injunctive relief. *See Bowen*, 487 U.S. at 905. The prospect of retrospective compensation for the injury that Defendants' challenged policy will inflict on Plaintiffs' members absent an injunction is not an adequate substitute for an equitable judicial order enjoining Defendants from inflicting those injuries in the first place.

D. Plaintiffs may pursue injunctive relief to ensure Defendants' compliance with federal law.

In addition to seeking relief under the APA, Plaintiffs bring a nonstatutory cause of action to halt Defendants' unlawful action in enabling DOGE to access sensitive personal information. The Court need not address Plaintiffs' nonstatutory cause of action if the Court addresses the merits of Plaintiffs' APA claims. Contrary to Defendants' contention, however, *see* Defs.' Mem. 30–31, nonstatutory relief is available apart from the APA because federal courts have inherent authority to "grant injunctive relief" against federal officers "who are violating, or planning to violate, federal law." *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 326–27 (2015); *see also Chamber of Commerce v. Reich*, 74 F.3d 1322, 1328 (D.C. Cir. 1996) ("When an executive acts ultra vires, courts are normally available to reestablish the limits on his authority," quoting *Dart v. United States*, 848 F.2d 217, 224 (D.C. Cir. 1988)). The "enactment of the APA did not repeal the review of *ultra vires* action recognized long before." *Id*. (quoting *Dart*, 848 F.2d at 224).

And while Defendants again emphasize the damages remedy available under the Privacy Act and the IRC, the "[m]ere existence of a remedy at law has not sufficed to warrant denial of equitable intervention." *Council of & for the Blind of Delaware Cnty. Valley, Inc. v. Regan*, 709 F.2d 1521, 1550 n.76 (D.C. Cir. 1983). Although Plaintiffs have properly alleged claims under the APA, if the Court concludes that APA review is unavailable, it should grant injunctive relief to prevent Defendants from violating their legal obligations to protect the privacy of the sensitive personal information of Plaintiffs' members.

II. DEFENDANTS ACTED UNLAWFULLY IN GRANTING DOGE UNFETTERED ACCCESS TO PERSONAL INFORMATION ON THE BUREAU'S SYSTEMS.

A. Defendants' action is contrary to law and in excess of their statutory authority.

To avoid the conclusion that they acted inconsistently with their legal obligation to protect individual privacy, Defendants characterize the DOGE initiative and its implementation at the Bureau as a routine personnel matter that concerns nothing more than the "day-to-day operations" of the Bureau's systems. Defs.' Mem. 1. But there is nothing routine or ordinary about the DOGE initiative. By its terms, it seeks to rework the privacy expectations of millions of individuals whose personal information is housed in federal information systems, including those of the Bureau. And in their rush to implement the DOGE Executive Order, Defendants failed to take the steps necessary to comply with the Privacy Act and the IRC to ensure that personal information remains protected.

1. The Privacy Act and Defendants' own privacy policies outline the steps that Defendants must take before implementing a new initiative that affects the privacy of individuals' personal information on the agency's systems. *See* Defs.' Mem. 25 (recognizing that the DOGE Executive Order "creat[ed] a framework for agency DOGE Teams and USDS collaboration"). First, Defendants must publish a SORN that describes the changes that the agency seeks to make to its

system of records and "new use or intended use of the information," including a new routine use. 5 U.S.C. § 552a(e)(4), (11). As the Privacy Act Handbook recognizes, a SORN is needed when "making significant/major alterations/modifications to a system of records." Privacy Act Handbook 20–21, which includes "changing the purpose for which the information is used" or "the equipment configuration (i.e., hardware, software, or both) on which the system is operated so as to create the potential for either greater or easier access," *id*. at 7.

Second, a "significant change in a system of records" requires advance notice to Congress and OMB "to permit evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals." 5 U.S.C. § 552a(r). As the Privacy Handbook explains, this includes changes to system security, including "such things as the "personnel who will have access" to the system and "the steps taken by the agency to minimize the risk of unauthorized access to the system of records." Privacy Act Handbook 24. The report must also evaluate how the change will "impact an individual's privacy," even if "no adverse effect is anticipated." *Id*. at 23–24.

Third, changes to systems of records that are "minor" still must be documented in a notice to the Office of Privacy, Transparency, & Records. Privacy Act Handbook 21. That notice must be accompanied by a "memorandum demonstrating that the modification is not significant" and does not require a SORN or a report to Congress and OMB. *Id*.

Defendants recognized that the President's DOGE initiative—and the access to personal information it required—was not a run-of-the-mill agency operation. The initial Treasury DOGE Team was not named by the agency; it was selected by the presidential transition team before the inauguration. As team lead, Mr. Krause appears to have no fixed job responsibility, *see supra* at 9–10, but instead acts as a jack-of-all-trades "in service of the President's DOGE mission." Krause Decl. ¶ 6; *see* Defs.' Response to Interrog. #2, at 7–8 (listing the four DOGE projects that involve

access to personal information). To that end, he "coordinate[s]" his work with USDS and "receive[s] high-level policy direction from them." Krause Decl. ¶ 4; *see* Defs. Mem. 25 (recognizing that the DOGE Executive Order "creat[ed] a framework for agency DOGE Teams and USDS collaboration"). The Treasury DOGE Team is not integrated into the agency workforce; it is a discrete group of individuals dedicated to implementing the DOGE Executive Order. Defs.' Response to Interrog. #1, at 6. And DOGE itself is a flexible entity to which the President has delegated a disparate set of responsibilities that go well beyond modernizing technology. *See supra* n.8. Giving DOGE unprecedented access to the Bureau's systems was not the type of "day-to-day" decisions that agencies routinely make. It was a decision that profoundly affects individuals' privacy rights, therefore triggering Defendants' obligations under the Privacy Act.

2. Defendants seek to excuse their failure to follow the Privacy Act by invoking 5 U.S.C. § 552a(b)(1), which authorizes an agency to disclose records "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." *See* Defs.' Mem. 25. Section 552a(b)(1), however, does not grant agency employees carte blanche to obtain any record within the agency's files. Rather, the "need to know" exception permits an employee to examine a record "in connection with the performance of duties assigned to him" if "he had to do so in order to perform those duties properly." *Bigelow v. Dep't of Def.*, 217 F.3d 875, 877 (D.C. Cir. 2000). This inquiry must be conducted for "each employee" to whom the information has been disclosed. *Dick v. Holder*, 67 F. Supp. 3d 167, 178 (D.D.C. 2014). Defendants recognize that personal information on the Bureau's systems may be accessed only on a need-to-know basis.[14]

[14] *See* Bur. of the Fiscal Serv., Privacy and Civil Liberties Impact Assessments for PAM, SPS, ASAP, ITS, CARS, and PIRS, https://www.fiscal.treasury.gov/pia.html (Ex. J).

Contrary to Defendants' suggestion, Defs.' Mem. 26, DOGE's charge "to modernize technology" does not automatically indicate that team members have a need for unfettered access to any and all personal information housed in a government system. For instance, information security guidelines include principles such as "separation of duties" and "least privilege" designed specifically to protect systems and the information stored on them from being compromised by granting excessive access permissions to a single person or cadre of individuals. *See AFSCME*, 2025 WL 1141737, at *47–*48 (discussing these principles). Here, Defendants recognized that their decision to grant the DOGE Team unprecedented access to the Bureau's systems risked "[d]isruptive impacts to technical operations" that threatened "U.S. economic security" and the delivery of lifeline payments to millions of constituents." AR 57. But while Defendants developed "mitigation strategies" to reduce the risk of disruptions, Gioeli Decl. ¶¶ 11, 13; *see* AR, 61–62, it took no action to give teeth to the need-to-know limitation of the Privacy Act. There is no evidence in the record that any personal information was off limits to DOGE.

Defendants' ability to enforce the need-to-know limitation was further eroded by their failure to provide Mr. Krause with a consistent set of job duties. *See supra* at 9–10. Mr. Krause himself sees his role "is to find ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of this Administration." Krause Decl. ¶ 4. Such a vaguely defined role does not act as a limitation at all. *Cf. Hill v. Dep't of Def.*, 981 F. Supp. 2d 1, 13 (D.D.C. 2013) (relying on job responsibilities set out in federal regulations to assess an employee's need to know).

The Treasury DOGE Team's activities underscore that the need-to-know requirement has no teeth at the Bureau. With respect to the payment processing engagement plan, Mr. Krause initially proposed the project to "understand how [the Bureau's] end-to-end payment systems and

financial report tools work." Krause Decl. ¶ 11; AR 60. In his declaration, he asserted without explanation that this project required "the ability to review sensitive payment data." Krause Decl. ¶ 15. When pressed in discovery to elaborate, Defendants referred to the "need to … query the payment data sources, which include PII, to understand the extent of the system failures and improper payments." Defs.' Response to Interrog. #3, at 10. But while Defendants argue that this "need" flows "directly from the mandates" of the DOGE Executive Order, Defs' Mem. 26, nothing in that Executive Order refers to halting improper payments. And even assuming that some data analysis may aid the DOGE Team in carrying out a legitimate, well-defined objective, Defendants have failed to demonstrate why personal information itself must be disclosed to DOGE if the goal is to understand the "extent" of "information mismatches" for purposes of "recommend[ing] new technology solutions." Defs.' Response to Interrog. #3, at 10–11.

The DOGE Team's efforts to implement the Foreign Aid Executive Order further demonstrate the absence of meaningful privacy safeguards: Although Mr. Krause was supposedly granted only "over the shoulder" access to the Bureau's systems, Gioeli Decl. ¶ 4; Krause Decl. ¶ 16, he and Mr. Elez apparently had the authority to obtain payment data upon request. *See* Defs.' Response to Interrog. #1, at 6. Defendants have not disclosed the nature of these requests, but during the Kansas City site visit, the record shows that Mr. Krause obtained personal information on USAID funding recipients, which he forwarded to Mr. Elez, who then emailed the information to two individuals at GSA. *Id*. Defendants do not contend that these actions are tied to the goal of modernizing technology. Rather, Defendants argue that the President may designate payments "improper," which in turn "likely" justifies dissemination of personal information to *GSA*. Defs.' Mem. 27–28. As this incident confirms, the Treasury DOGE Team is not meaningfully bound by any need-to-know condition when it comes to their ability to access sensitive personal information.

Lastly, Defendants' argument that the DOGE Team needs access to tax records subject to the IRC's heightened confidentiality protections also relies on DOGE's roving mission to stamp out "improper" payments. *See* Defs.' Mem. 28–29. Of course, *any* payment might be viewed as "improper" until an investigation occurs and it is shown not to be, indicating that no effective constraints limit DOGE's access to sensitive data. And while Defendants assert that the DOGE is no different from "all of the other Treasury employees, contractors, and others who work every day to maintain and improve the operation of these critical payment systems," they offer no examples of other employees or contractors who can rummage through personal information on the Bureau's systems at will the way that the DOGE Team can. *See* Gioeli Decl. ¶ 13. Such unfettered access to "immense amounts of very sensitive information" is exactly the type of threat to Americans' personal affairs that the Privacy Act prohibits.[15]

B. Defendants' action is arbitrary and capricious.

The APA authorizes reviewing courts to set aside agency action that is "arbitrary" or "capricious." 5 U.S.C. § 706(2)(A). "An agency action qualifies as 'arbitrary' or 'capricious' if it is not 'reasonable and reasonably explained.'" *Ohio v. EPA*, 603 U.S. 279, 292 (2024) (quoting *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021)). To satisfy that obligation, an agency must act "within a zone of reasonableness and, in particular, [must have] reasonably considered the relevant issues and reasonably explained the decision." *Prometheus Radio Project*, 592 U.S. at 423. Agency action is unreasonable where the agency has ignored "an important aspect of the problem." *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

[15] Legislative History of the Privacy Act 5 (1976) (introductory remarks of Sen. Ervin), https://tile.loc.gov/storage-services/service/ll/llmlp/LH_privacy_act-1974/LH_privacy_act-1974.pdf.

Here, the record shows that Defendants ignored the privacy risks associated with granting DOGE unfettered access to sensitive personal information. Rather, their overriding objective was to place Mr. Krause at the agency "quickly"—even before Secretary Bessent was sworn in—so he and Mr. Elez could begin implementing the President's DOGE agenda. Krause Decl. ¶ 11. Defendants apparently believed that they could implement the President's DOGE agenda by portraying their actions as routine housekeeping matters and thereby avoid their duty to engage in reasoned decisionmaking. That belief is wrong. Adherence to APA standards ensures that "federal agencies are accountable to the public and their actions subject to review by the courts." *DHS v. Regents of the Univ. of Cal.*, 591 U.S. 1, 16 (2020) (quoting *Franklin v. Massachusetts*, 505 U.S. 788, 796 (1992). Defendants' decisions about implementation of the DOGE Executive Order are no exception to that rule.

Defendants argue that they "thoughtfully considered the risk of granting access to [Bureau] systems and put in place risk mitigation measures as a result." Defs.' Mem. 30. But none of the mitigation measures that Defendants adopted constrained the DOGE Team's authority to view and process any sensitive personal information they wished to access. *See* AR 58–62; Gioeli Decl. ¶¶ 11–17. Even those mitigation measures were not wholly effective for that purpose. For instance, Mr. Elez was permitted to resign without providing an attestation statement, Defs.' Admis. at 5, he was permitted to email personal information to GSA without obtaining proper authorization, Ambrose Decl. ¶ 12, ECF 48-2, and the agency still "has not yet completed its forensic analysis of [Mr. Elez's] laptop" to evaluate whether his actions compromised the Bureau's systems, Defs.' Response to Interrog. #7, at 16. Moreover, those mitigation measures applied only to the DOGE Team's payment processing engagement plan. For other initiatives, the record indicates that Mr. Krause and Mr. Elez (and presumably newer DOGE Team members) have been granted the

authority to obtain any data from Bureau personnel that they wish. Defs.' Response to Interrog. #1, at 6. Defendants acted arbitrarily by failing to consider the privacy implications of their actions in their zeal to implement the DOGE Executive Order.

CONCLUSION

For the foregoing reasons, the Court should grant Plaintiffs' motion for summary judgment and deny Defendants' motion to dismiss or, in the alternative, for summary judgment.

April 25, 2025

Respectfully submitted,

/s/ Nandan M. Joshi
Nandan M. Joshi (DC Bar No. 456750)
Nicolas Sansone (DC Bar No. 1686810)
Allison M. Zieve (DC Bar No. 424786)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Norman L. Eisen (DC Bar No. 435051)
State Democracy Defenders Fund
600 Pennsylvania Avenue SE
#15180
Washington, DC 20003