

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

**AMERICAN FEDERATION OF
TEACHERS, *et al.*,**

Plaintiffs,

v.

SCOTT BESSENT, *et al.*,

Defendants.

*

*

*

Civ. No. DLB-25-0430

*

*

*

MEMORANDUM OPINION

On the first day of President Donald J. Trump’s second term in office, he issued an Executive Order that created the Department of Government Efficiency (“DOGE”) and renamed the United States Digital Service as the United States DOGE Service (“USDS”). Exec. Order No. 14,158, 90 Fed. Reg. 8441 (Jan. 29, 2025) (“DOGE Executive Order”). The stated purpose of DOGE is “to implement the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.” *Id.* at § 1. The DOGE Executive Order commands federal agency heads to “take all necessary steps . . . 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). Almost immediately after the DOGE Executive Order was issued, federal government agencies hired or accepted as detailees individuals whose mission is to implement the DOGE Executive Order. Among those agencies were the U.S. Department of Education (“Education”), the U.S. Office of Personnel Management (“OPM”), and the U.S. Department of the Treasury (“Treasury”). Pursuant to the DOGE Executive Order, Education, OPM, and Treasury gave individuals affiliated with DOGE access to agency systems that hold records with the personally identifiable information (“PII”) of millions of Americans.

This lawsuit is one of several filed by plaintiffs who seek to enjoin federal government agencies from disclosing records with their sensitive personal information to government personnel implementing the DOGE Executive Order. In this case, the plaintiffs are unions and membership organizations representing current and former federal employees and federal student aid recipients and six military veterans who have received federal benefits or student loans. In their amended complaint, filed on February 12, 2025, the plaintiffs assert claims under the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.* (“APA”) against Education, OPM, and Treasury; Denise L. Carter, the Acting Secretary of Education; Charles Ezell, the Acting Director of OPM; and Scott Bessent, the Secretary of the Treasury (collectively, “the government” or “the agencies”). The plaintiffs allege that the agencies unlawfully granted access to records that contain their PII to DOGE representatives.

On February 24, 2025, the Court granted in part and denied in part the plaintiffs’ motion for a temporary restraining order (“TRO”), enjoining Education and OPM from granting access to the plaintiffs’ sensitive personal information to individuals who are implementing the President’s DOGE agenda. *See* ECF 38. Since then, the government has produced the administrative records for each agency, and the plaintiffs have filed a motion for a preliminary injunction. Having considered the administrative records, the parties’ TRO and preliminary injunction briefing, their exhibits, and oral argument by counsel, the Court grants the plaintiffs’ motion for a preliminary injunction. They have shown a likelihood that they will succeed on their claim that the defendants violated the APA by not acting in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a; that they will suffer irreparable harm if the defendants are not enjoined; and that the balance of the equities and public interest weigh favor of preliminary injunctive relief.

I. Background

A. DOGE Executive Order

On January 20, 2025, President Donald J. Trump signed the DOGE Executive Order. It established the Department of Government Efficiency “to implement the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.” DOGE Executive Order § 1. The order establishes “the U.S. DOGE Service Temporary Organization” to be “dedicated to advancing the President’s 18-month DOGE agenda.” *Id.* § 3(b). It directs each agency head to establish “a DOGE Team of at least four employees, which may include Special Government Employees, hired or assigned within thirty days of the date of this Order.” *Id.* § 3(c). “Each DOGE Team will typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney.” *Id.* DOGE Team Leads will “coordinate their work with USDS and advise their respective Agency Heads on implementing the President’s DOGE Agenda.” *Id.*

The DOGE 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,” which includes “work[ing] 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). The DOGE Executive Order commands agency heads to “take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems.” *Id.* § 4(b). It also directs that “USDS shall adhere to rigorous data protection standards.” *Id.*

B. Agency Defendants

The defendants include Education, OPM, Treasury, and the respective agency heads in their official capacities. Members of the DOGE team or “DOGE affiliates” are working at each of these agencies.¹

1. Education

Education manages the federal student loan system. ECF 13, ¶ 94. Within this system, the Federal Student Aid Office maintains the National Student Loan Data System (“NSLDS”), the Common Origination and Disbursement System (“CODS”), the FUTURE Act System (“FAS”), and the Financial Management System (“FMS”). *See id.* ¶¶ 95, 98, 100, 102. These systems house records that contain the PII of individuals who receive federal student aid, such as Social Security numbers and taxpayer identification numbers, names, dates of birth, mailing and email addresses, driver’s license information, income and asset information, federal tax information, demographic information including marital and citizenship status, and family members’ personal and financial information. *See, e.g., id.* ¶¶ 95–102; Privacy Act of 1974; System of Records, 89 Fed. Reg. 44652, 44656–57 (May 21, 2024) (listing categories of records in the NSLDS); Privacy Act of 1974; System of Records, 88 Fed. Reg. 41942, 41947–48 (June 28, 2023) (listing categories of records

¹ Unless otherwise noted, the Court uses the term “DOGE affiliates” throughout the opinion to refer to the personnel at Education, OPM, and Treasury whose principal role is to implement the DOGE agenda as described in the DOGE Executive Order and who were granted access to agency record systems for the principal purpose of implementing that agenda. The administrative records refer to these personnel as “employees implementing [the DOGE Executive Order].” *See* ECF 51-1, at 2; ECF 64-1, at 2; ECF 51-3, at 2; ECF 58, at 1; ECF 51-2, at 2. The government has redacted the names of DOGE affiliates at Education and OPM and refers to them by the agency initials and a number (*e.g.*, ED-1, OPM-1). Because the government produced three separate administrative records—one for each agency—citations to the administrative records also begin with the agency initials, followed by a four- or six-digit number (*e.g.*, ED-000001, OPM-000001, TR-0001).

in the CODS); Privacy Act of 1974; System of Records, 88 Fed. Reg. 42200, 42222 (June 29, 2023) (listing categories of records in the FAS); Privacy Act of 1974; System of Records—Financial Management System (FMS), 73 Fed. Reg. 177, 178 (Jan. 2, 2008) (listing categories of records in the FMS).

The government represents that there are six DOGE affiliates at Education.² ECF 62, at 7 (citing ECF 27-6, ¶¶ 4–6 (A. Ramada Suppl. Decl.)). Several of the DOGE affiliates at Education are detailed from other agencies. The administrative record shows that Education executed two memoranda of understanding with the DOGE affiliates’ home agencies on February 12, 2025, “formaliz[ing] . . . prior oral agreement[s].” *See* ED-000005–07, ED-000013–16. One detailee, ED-1, is a Senior Advisor in the Office of the Secretary. ED-000005. Another detailee, ED-3, is a special government employee detailed from their position as a “Software Engineer (Consultant)” at the General Services Administration (“GSA”) to the Office of the Secretary. ED-000013. Two other DOGE affiliates, ED-2 and ED-4, were appointed to Education on January 31, 2025 and February 4, 2025 as a Senior Advisor and a Consultant, respectively, in the Office of the Secretary. ED-000009–10, ED-000017.

In a February 5, 2025 memorandum, Thomas Flagg, the Chief Information Officer (“CIO”) at Education, authorized IT system access to “USDS personnel onboarded to the Department of Education DOGE team”:

President Trump signed an Executive Order (EO) “Establishing and Implementing the President’s “Department of Government Efficiency”” to implement the

² The government has consistently represented to the Court that “[t]here are six employees at the Department of Education whose principal role is to help advance the goals of [the DOGE Executive Order],” and submitted declarations to that effect. *See* ECF 62, at 7; ECF 27, at 9; ECF 27-5, ¶¶ 4–7 (A. Ramada Decl.); ECF 27-6, ¶ 2 (A. Ramada Suppl. Decl.). However, the administrative record only identifies four DOGE affiliates—two detailees and two appointees. *See* ED-000005–7, ED-000009, ED-000013–19, ED-000021.

President's DOGE Agenda by modernizing Federal technology and software to maximize governmental efficiency and productivity. The EO also tasked Agencies to establish an internal DOGE team and allow full access to the DOGE Administrator to all unclassified agency records, software systems and IT systems. This is to support the USDS Administrator Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems. All ED Information System Owners (ISO) shall work with the USDS Administrator and internal DOGE Team members to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.

This memorandum documents the need to know and authorizes USDS personnel onboarded to the Department of Education DOGE team full and prompt access to all unclassified IT systems and data. These new requirements support the implementation of the EO "Establishing and Implementing the President's [']Department of Government Efficiency[.']"

ED-000025.

One week later, Education and USDS executed "Terms and Conditions for Reimbursable Work" that "formalize[d] and supersede[d] [a] prior oral agreement, written interim assignment agreement, and supporting documentation between USDS and ED." ED-000001. These terms and conditions state that "ED will provide USDS detailees with access to all ED systems on USDS employees' EOP devices to the maximum extent allowable by law." ED-000002.

2. OPM

OPM acts as the "chief human resources agency and personnel policy manager for the Federal Government." ECF 13, ¶ 71 (quoting *About Us*, OPM, <https://www.opm.gov/about-us> [<https://perma.cc/CQ7X-LLYA>] (last visited Mar. 20, 2025)). OPM maintains a host of systems with information about federal government personnel. *See id.* ¶ 72. For example, OPM maintains the Electronic Official Personnel Folder ("eOPF"), which contains digital versions of federal employees' personnel files that cover their entire period of federal civilian service. *See* OPM, *Privacy Impact Assessment for Electronic Official Personnel Folder System (eOPF)* 1 (2020), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/eopf-pia.pdf>

[<https://perma.cc/T6KM-RGHU>]. The eOPF contains current and former federal employees' PII such as Social Security numbers, bank account numbers, names and addresses, dates of birth, health and life insurance policy numbers, civil and criminal history information, and personnel actions such as promotions and suspensions. *Id.* at 5, 11–12. OPM also maintains the Enterprise Human Resources Integration Data Warehouse (“EHRI”), USA Performance, USA Staffing, and USAJOBS. ECF 13, ¶ 78. These systems also contain PII, including names, Social Security numbers, dates of birth, and citizenship status. *See* ECF 13, ¶¶ 78, 81–83; OPM, *Privacy Impact Assessment for Enterprise Human Resources Integration Data Warehouse (EHRI DW)* 3 (2019), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/ehridw.pdf> [<https://perma.cc/5UCS-N5V8>]; OPM, *Privacy Impact Assessment for USA Staffing*® 6–7 (2021), https://www.fhfa.gov/sites/default/files/2023-12/OPM%20USA%20Staffing_pia.pdf [<https://perma.cc/W3ER-CAWS>]; OPM, *Privacy Impact Assessment for USA Performance (USAP)* 4 (2020), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/usap-pia.pdf> [<https://perma.cc/NR3C-WGMS>].

At OPM, there are several DOGE affiliates.³ *See* ECF 64-1, at 2; ECF 64, at 1; OPM-000103. The record contains employment documents for some of them. OPM-2, OPM-3, OPM-4, OPM-6, and OPM-7 are “Expert[s]” hired to work in the Office of the Director. OPM-000008, OPM-000010–11, OPM-000014, OPM-000021–22, OPM-000111–12. OPM-2 is also listed as a “Senior Advisor.” OPM-000006. OPM-5 is a “Senior Advisor to the Director for Information Technology” in the Office of the Director, and OPM-8 is a “Senior Advisor to the Director.” OPM-

³ “DOGE affiliates” does not include OPM’s CIO Greg Hogan, OPM Acting Director Charles Ezell, or OPM Chief of Staff Amanda Scales, because these individuals, by virtue of their positions at OPM, would otherwise have access to OPM systems and were not granted access for the principal purpose of implementing the President’s DOGE agenda.

000016–17, OPM-000019, OPM-000114–15. All of these DOGE affiliates were appointed to OPM on either January 20, 2025 or January 24, 2025. OPM-000006, OPM-000010, OPM-000014, OPM-000016, OPM-000021, OPM-000112, OPM-000116. Most of them are developers, engineers, or “political tech staff.” *See* OPM-000027–29, OPM-0000107–08.

On January 20, 2025, OPM Acting Director Ezell requested that several “[i]ndividuals from the [p]olitical [t]eam,” including OPM-3, OPM-5, and OPM-7, be added to OPM systems as “admins.” OPM-000107. That same day, these individuals were given “super user permissions” for USAJOBS administrative systems. OPM-000104. On January 27, 2025, Ezell sent an email with the subject line “Getting DoGE Engineers access.” OPM-000028. The email told an OPM employee, MC Price, that “[w]e are rapidly ramping up some engineers here,” and “[t]o accomplish this goal, these engineers”—OPM-2, OPM-3, OPM-4, OPM-5, and OPM-6—“need[ed] the following items urgently,” including “a short list of all the systems OPM operates and manages” and a range of access permissions “for each computer system.” OPM-000027–29. The access requested was “[c]ode read and write permissions,” the “[a]bility to access the system as a regular user (e.g. hiring manager and onboarding user for USA Staffing),” and the “[a]bility to access the system as an admin user,” with the instruction to “[p]rioritize USA Staffing, USAJOBS, and EHRI.” OPM-000029. On January 28, 2025, Price stated in an email that “[w]e have already given several of the political devs/engineers comprehensive access to USAJOBS and USA Staffing” and that “[n]ow we have 3 more individuals with the same requirement,” listing OPM-2, OPM-4, and OPM-6. OPM-000108–09. Price explained that this access would “start with USAJOBS, USA Staffing, and eOPF/EHRI,” and “USAP will be next, so might as well go ahead there.” OPM-000108. He noted that the individuals “need to have access today.” *Id.* On February 3, 2025, Price was forwarded a request from OPM Chief of Staff Amanda Scales for OPM-8 to

have “account creation info” with “admin access” for USA Staffing, “[s]imilar to . . . [OPM-6].” OPM-000110.

Other OPM DOGE affiliates were granted access to OPM systems, including USA Performance, the Federal Employee Health Benefits system, and the Postal Service Health Benefits Data Platform, between January 24, 2025 and February 7, 2025. OPM-000103.

3. Treasury

The Treasury Department’s Bureau of the Fiscal Service (“Fiscal Service”) maintains systems for disbursement of payments for federal programs such as Social Security benefits, federal income tax refunds, and veterans’ pay. ECF 13, ¶¶ 46, 48. Fiscal Service payment systems include the Payment Automation Manager (“PAM”), the Automated Standard Application for Payments (“ASAP”), and the Secure Payment System (“SPS”). *See* ECF 27-3, ¶ 5 (J. Gioeli Decl.). These payment systems contain PII including names, Social Security numbers, and bank information. *See* Fiscal Service, *Privacy and Civil Liberties Impact Assessment: Payment Automation Manager* 5 (2019), <https://www.fiscal.treasury.gov/files/pia/pampclia.pdf> [<https://perma.cc/5JW9-S42K>]; Fiscal Service, *Privacy and Civil Liberties Impact Assessment Secure Payment System (SPS)* 7 (2021), <https://fiscal.treasury.gov/files/pia/spspclia.pdf> [<https://perma.cc/U6HS-AJE5>]; Fiscal Service, *Privacy and Civil Liberties Impact Assessment: Automated Standard Application for Payments (ASAP)* 6–7 (2019), <https://fiscal.treasury.gov/files/pia/spspclia.pdf> [<https://perma.cc/XA33-TRXC>].

There are two DOGE affiliates at Treasury: Thomas Krause and Ryan Wunderly. Krause was appointed as the Senior Advisor for Technology and Modernization on January 23, 2025. *See* TR-0024, TR-0007, TR-0015, TR-0024. On February 5, 2025, Krause was delegated the duties of the Fiscal Assistant Secretary. *See* TR-0002–03. Wunderly took over a role previously held by

Marko Elez, who was hired by Treasury as a Special Advisor for Information Technology and Modernization on January 21, 2025 and resigned on February 6, 2025. TR-0004; *see* TR-0022–23; ECF 27-4, ¶ 8 (M. Wenzler Decl.); ECF 35-1, ¶ 2 (J. York Decl.).⁴

On January 24, 2025, Treasury Administrative Services set forth an “[e]ngagement [p]lan” for “supporting the USDS/DOGE team during their 4–6 week engagement to understand payment processes and opportunities to advance payment integrity and fraud reduction goals.” TR-0057. The engagement plan describes how the Fiscal Service will grant system access to the DOGE team at Treasury. For the “technical team member,” Elez, “USDS/DOGE confirmed . . . [he] require[d] access to Fiscal Service systems and data.” *See* TR-0058, TR-0061–62. The plan states that Fiscal Service will issue the technical team member a Fiscal Service laptop by January 28, 2025, and that Treasury will “provide[] access to in scope payment systems source code” and “[d]evelopment access to the in scope payment systems.” TR-0058–59. The engagement plan also notes that “USDS/DOGE requested to be granted ‘over the shoulder’ access to monitor Fiscal Service personnel conducting payment processing roles, which was approved by Fiscal Service on 1/23/25.” TR-0059. According to a spreadsheet attached to a February 3, 2025 email from a Treasury executive point person for the engagement, as of February 1, Elez had access to Treasury systems including PAM, SPS, and ASAP, and it was recommended that his access to other Treasury systems be expanded. TR-0061–62; *see* TR-0057.

⁴ In a February 21, 2025 letter, the government informed the Court that Treasury hired Ryan Wunderly “to perform the duties previously assigned to Marco Elez.” *See* ECF 35, at 1. According to a declaration from John York, Counselor to the Treasury Secretary, Wunderly “will join Mr. Krause on the Treasury DOGE Team to fill the position at the Bureau of the Fiscal Service previously held by Mr. Elez,” and “[h]is position description and job duties will be substantially the same as those of Mr. Elez.” ECF 35-1, ¶¶ 3–4. There is no indication that Wunderly’s access to the Treasury systems will be different from Elez’s access.

C. Plaintiffs

The organizational plaintiffs are: American Federation of Teachers (“AFT”), International Association of Machinists and Aerospace Workers (“IAM”), International Federation of Professional and Technical Engineers (“IFPTE”), National Active and Retired Federal Employees Association (“NARFE”), and National Federation of Federal Employees (“NFFE”). ECF 13, ¶¶ 18–21. AFT represents over 1.8 million people employed in the teaching and healthcare professions. ECF 14-9, ¶ 3 (S. Tammelleo Decl.). IAM and its affiliate organization NFFE represent more than 100,000 federal workers, as well as veterans and veterans’ groups. ECF 14-10, ¶ 3 (B. Bryant Decl.). IFPTE represents approximately 34,000 federal employees, most of whom work for the Department of Defense. ECF 14-12, ¶ 2 (M. Biggs Decl.). IFPTE members include nuclear submarine engineers, NASA scientists and researchers, administrative law judges at the Social Security Administration, nuclear engineers at the Tennessee Valley Authority, and Environmental Protection Agency employees. *Id.* NARFE represents approximately 128,000 current and former federal employees and spousal annuitants. ECF 14-11, ¶ 2 (W. Shackelford Decl.).

The individual plaintiffs are Jason Cain, Kristofer Goldsmith, Clifford Grambo, Thomas Fant, Donald Martinez, and Christopher Purdy. *Id.* ¶¶ 22–27. Cain, a U.S. Army veteran, receives veterans’ disability benefits and previously received GI bill benefits, student loans, and a VA home loan from the federal government. ECF 14-3, ¶¶ 3–5 (J. Cain Decl.). Cain also previously worked for the VA. *Id.* ¶ 6. Goldsmith, a U.S. Army veteran, receives veterans’ disability benefits and previously received federal student loans. ECF 14-5, ¶¶ 3–4 (K. Goldsmith Decl.). Grambo, a U.S. Navy veteran, receives veterans’ disability benefits and a military pension. ECF 14-6, ¶¶ 3–4 (C. Grambo Decl.). Fant, a veteran of the U.S. Coast Guard, receives veterans’ disability benefits. ECF

14-4, ¶¶ 3–4 (T. Fant Decl.). Martinez, a U.S. Army veteran, receives veterans’ disability and combat-related special compensation, Social Security disability insurance, and a VA home loan, and previously received vocational rehabilitation and employment payments from the VA. ECF 14-7, ¶¶ 3–5. Martinez previously worked for the Federal Emergency Management Agency and received federal student loans. *Id.* ¶¶ 5–6. Purdy, a veteran of the Army National Guard, receives veterans’ disability benefits and previously received federal student loans and a VA home loan. ECF 14-8, ¶¶ 3–5 (C. Purdy Decl.).

Because the members of the organizational plaintiffs and the individual plaintiffs have worked for the federal government, have federal student loans, and/or receive government benefits, their PII is housed in record systems maintained by Education, OPM, and/or Treasury. *See* ECF 13, ¶¶ 18–27; ECF 14-3, ¶¶ 7–8; ECF 14-4, ¶¶ 5–6; ECF 14-5, ¶¶ 6–7; ECF 14-6, ¶¶ 5–6; ECF 14-7, ¶¶ 7–8; ECF 14-8, ¶¶ 6–7; ECF 14-9, ¶¶ 6–7; ECF 14-10, ¶¶ 10–11; ECF 14-11, ¶¶ 5–6; ECF 14-12, ¶¶ 8–9.

The plaintiffs allege that Education, OPM, and Treasury have granted DOGE representatives sweeping access to systems that are typically accessed by only a small number of career employees at the respective agencies. *See* ECF 13, ¶¶ 49, 53, 56, 61, 74, 76–78, 103, 132. They cite to reports that DOGE representatives’ access to systems with sensitive data caused significant concern among career agency employees and cyber security experts. *Id.* ¶¶ 103, 135. They also cite to an article that describes a Treasury analyst characterizing DOGE as an “insider threat.” *Id.* ¶ 136. And they point to reports that DOGE representatives input sensitive data into artificial intelligence software. *Id.* ¶¶ 104, 110.

The plaintiffs allege that the “continued and ongoing disclosure of their records to DOGE representatives constitutes a violation of the Privacy Act, for which no exception applies.” *Id.* ¶

87. They say that Education, OPM, and Treasury have given DOGE representatives unrestricted access to their PII, *id.* ¶¶ 61, 76–78, 84, 85, 103–04, 108; that none of the plaintiffs or the members of the plaintiffs’ organizations requested disclosure or provided express written consent to the disclosure of their information to DOGE representatives, *id.* ¶¶ 62, 87, 109; and that none of the DOGE representatives needs to know the plaintiffs’ personal information to perform their duties, *id.* ¶¶ 64, 89, 113–14. The purportedly unlawful disclosures to DOGE representatives have caused the plaintiffs “major distress and anxiety, as they do not know who their data has been or will be shared with, whether these disclosures have made them vulnerable to further privacy breaches, and how it may be weaponized against them.” *Id.* ¶ 140.

The plaintiffs assert three violations of the APA. First, they allege that the agencies’ actions violated the Privacy Act and that the agencies did not act in accordance with law. *Id.* ¶¶ 145–51. Second, they allege that the agencies acted arbitrarily and capriciously when they failed to consider the requirements of the Privacy Act and failed to engage in reasoned decision-making when they granted DOGE representatives broad access to their record systems containing sensitive and personal information. *Id.* ¶¶ 152–56. Finally, they allege that the agencies violated non-discretionary duties to protect records from unauthorized disclosure. *Id.* ¶¶ 157–59.

On February 12, 2025, the plaintiffs filed a motion for a TRO to enjoin Education, OPM, Treasury, and the respective agency heads from granting access to record systems with the plaintiffs’ personal information. ECF 14. The Court granted in part and denied in part the plaintiffs’ motion. ECF 38. On February 24, 2025 at 8:00 a.m., the Court issued a TRO that enjoined Education and OPM from disclosing the plaintiffs’ PII to DOGE affiliates until March 10, 2025 at 8:00 a.m. *Id.* On February 26, the Court set a briefing schedule for a preliminary injunction motion. ECF 46. On March 7, the government produced the administrative records. ECF 51; *see also* ECF

58 (March 10 errata correcting parts of the Education and OPM administrative records). The next day, the plaintiffs moved for extra-record discovery, ECF 53, and the government opposed, ECF 54.⁵ On March 10, the plaintiffs filed a motion for a preliminary injunction. ECF 59. The government opposed. ECF 62. The plaintiffs replied. ECF 63. After the plaintiffs filed a reply, the government supplemented the OPM administrative record. ECF 64-1. The Court held a hearing on the preliminary injunction motion on March 17.⁶ For the reasons stated below, the Court grants the plaintiffs' motion for a preliminary injunction.

II. Discussion

The plaintiffs assert three claims under the APA, including a claim that the defendants violated the Privacy Act, 5 U.S.C. § 552a, and therefore acted “not in accordance with law,” *see* 5 U.S.C. § 706(2)(A). The Privacy Act restricts agencies from disclosing records that contain PII unless the subject requests or consents to disclosure or an exception to consent applies. *See* 5 U.S.C. § 552a(b). The plaintiffs have shown they are entitled to preliminary injunctive relief on their APA claim that the agencies did not act in accordance with the Privacy Act. Before explaining why, the Court confirms it has jurisdiction over this case.

A. Standing

Article III of the Constitution extends the “judicial Power” of the federal courts only to “Cases” or “Controversies.” U.S. Const. art. III, § 2, cl. 1; *see TransUnion LLC v. Ramirez*, 594

⁵ For reasons discussed in greater detail below, the Court confines its review of the merits of the plaintiffs' APA claims to the administrative records and a handful of judicially noticeable materials. The plaintiffs' motion for extra-record discovery is denied without prejudice.

⁶ At the hearing, the Court extended the TRO for good cause, for reasons stated on the record, until March 24, 2025 at 8:00 a.m. or until the Court rules on the preliminary injunction motion. The TRO expires upon the issuance of this ruling.

U.S. 413, 423 (2021). There is a case or controversy only if the plaintiff has standing to assert their claim. *TransUnion*, 594 U.S. at 423. To establish standing, a plaintiff must show “(1) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury would likely be redressed by judicial relief.” *Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 294 (4th Cir. 2024) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). The “injury must be actual or imminent, not speculative—meaning that the injury must have already occurred or be likely to occur soon.” *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 381 (2024) (citing *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013)). When, as here, “a plaintiff seeks prospective relief such as an injunction, the plaintiff must establish a sufficient likelihood of future injury.” *Id.* (citing *Clapper*, 568 U.S. at 401).⁷

⁷ Several plaintiffs are organizations. “An organization . . . can assert standing either in its own right or as a representative of its members.” *S. Walk at Broadlands Homeowner’s Ass’n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 182 (4th Cir. 2013). The organizational plaintiffs assert standing as representatives of their members. *See* ECF 14-9, ¶¶ 6–11; ECF 14-10, ¶¶ 10–15; ECF 14-11, ¶¶ 5–10; ECF 14-12, ¶¶ 8–13. An organization establishes “representational standing” by showing “that ‘(1) its own members would have standing to sue in their own right; (2) the interests the organization seeks to protect are germane to the organization’s purpose; and (3) neither the claim nor the relief sought requires the participation of individual members in the lawsuit.’” *S. Walk at Broadlands*, 713 F.3d at 184 (quoting *Md. Highways Contractors Ass’n, Inc. v. Maryland*, 933 F.2d 1246, 1251 (4th Cir. 1991)). The organizational plaintiffs have established that they have germane interests. *See* ECF 14-9, ¶¶ 4–5; ECF 14-10, ¶¶ 6–9; ECF 14-11, ¶¶ 3–4; ECF 14-12, ¶¶ 4–7. And “the Court discerns no reason Plaintiffs’ members must participate directly in this case rather than allow their associations to speak on their behalf.” *All. for Retired Americans v. Bessent*, --- F. Supp. 3d. ---, No. 25-0313, 2025 WL 740401, at *13 (D.D.C. Mar. 7, 2025) (finding third prong of associational standing met for organizations with APA claims, including for alleged Privacy Act violations); *see also United Food & Com. Workers Union Loc. 751 v. Brown Grp., Inc.*, 517 U.S. 544, 546 (1996) (“‘[I]ndividual participation’ is not normally necessary when an association seeks prospective or injunctive relief for its members”). Thus, the standing question in this case is the same for the organizational and individual plaintiffs: have they established an injury in fact. For convenience, the Court uses “plaintiffs” to refer to the individual plaintiffs and the members of the organizational plaintiffs.

The plaintiffs “must demonstrate standing ‘with the manner and degree of evidence’ required at the relevant ‘stage[] of the litigation.’” *Fernandez*, 116 F.4th at 295 (alteration in original) (quoting *Lujan*, 504 U.S. at 561). At this stage, that means they “must make a ‘clear showing’ that [they are] ‘likely’ to establish each element of standing.” *See Murthy v. Missouri*, 603 U.S. 43, 58 (2024) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008)). Only the first element—injury in fact—is at issue here. The plaintiffs’ injury is the ongoing access to their sensitive personal information by unauthorized government personnel. The Court finds that the plaintiffs have made a clear showing that they are likely to establish a concrete injury in fact.⁸

In *TransUnion LLC v. Ramirez*, the Supreme Court explained “[w]hat makes a harm concrete for purposes of Article III.” 594 U.S. at 424. To determine whether the concrete-harm requirement has been met, “courts should assess whether the alleged injury to the plaintiff has a ‘close relationship’ to a harm ‘traditionally’ recognized as providing a basis for a lawsuit in American courts.” *Id.* (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). “That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury.” *Id.* The inquiry “does not require an exact duplicate in American history and tradition.” *Id.* Traditional tangible harms include physical and monetary harms. *Id.* at 425. Intangible harms also can be concrete. *Id.* They include injuries such as “reputational harms, disclosure of private information, and intrusion upon seclusion.” *Id.*⁹

⁸ The Court “assumes the merits of a dispute will be resolved in favor of the party invoking [its] jurisdiction in assessing standing.” *See Equity In Athletics, Inc. v. Dep’t of Educ.*, 639 F.3d 91, 99 (4th Cir. 2011).

⁹ *TransUnion* reaffirmed what the Supreme Court held in *Spokeo*: “Article III standing requires a concrete injury even in the context of a statutory violation.” *TransUnion*, 594 U.S. at 426 (quoting *Spokeo*, 578 U.S. at 341).

In the wake of *TransUnion*, the Fourth Circuit held that an injury resulting from a violation of a statute aimed at protecting a person’s privacy bore a close relationship to a harm redressable at common law: invasion of privacy. In *Garey v. James S. Farrin, P.C.*, the plaintiffs were automobile drivers who had been involved in motor vehicle accidents. *See* 35 F.4th 917, 919–20 (4th Cir. 2022). They alleged that personal injury lawyers obtained accident reports from state law enforcement and private data brokers that contained their names and addresses and mailed them unsolicited advertisements. *Id.* at 920. The drivers alleged the personal injury lawyers violated the Driver’s Privacy Protection Act (“DPPA”), which provides a cause of action against “[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record,’ for an impermissible purpose.” *Id.* (quoting 18 U.S.C. § 2724(a)). The district court found the plaintiffs had standing to sue for damages.

On appeal, the Fourth Circuit’s standing analysis began with *TransUnion*: “[P]laintiffs proceeding under a statutory cause of action can establish a cognizable injury by ‘identif[ying] a close historical or common-law analogue for their asserted injury’ for which courts have ‘traditionally’ provided a remedy.” *Id.* at 921 (alteration in original) (quoting *TransUnion*, 594 U.S. at 424). “A plaintiff who does so has standing even if the precise injury would not, absent the statute, be sufficient for Article III standing purposes.” *Id.*

“Consistent with *TransUnion*,” the district court found that the drivers had alleged harms “closely related to the invasion of privacy, which has long provided a basis for recovery at common law.” *Id.* (citation omitted). The Fourth Circuit agreed. *Id.* The court observed that it “recently rebuffed a nearly identical standing challenge in a case arising under the Telephone Consumer Protection Act (‘TCPA’), another consumer privacy statute that, like the DPPA, provides a private right of action against offenders.” *Id.* at 921–22 (citing *Krakauer v. Dish Network, LLC*, 925 F.3d

643, 652–54 (4th Cir. 2019)). The court’s explanation of its *Krakauer* decision is worth recounting here:

In *Krakauer*, we explained that by enacting the TCPA, “Congress responded to the harms of actual people by creating a cause of action that protects their particular and concrete privacy interests.” And we noted that injuries to personal privacy have long been “recognized in tort law and redressable through private litigation.” . . . [W]e concluded that our inquiry “focuse[s] on types of harms protected at common law, not the precise point at which those harms become actionable.” Therefore, we held that the TCPA’s “private right of action . . . plainly satisfies the demands of Article III.”

Id. at 922 (third alteration in original) (citations omitted).

Applying its analysis in *Krakauer*, the court reached the same result in *Garey*. The drivers alleged in their complaint that they “sustained actual damages by having [their] privacy invaded by Defendants’ knowingly obtaining [their] name[s] and address[es] from motor vehicle record[s] for an impermissible purpose in violation of law.” *Id.* (citation omitted). These allegations stated a “legally cognizable privacy injury.” *Id.* It did not matter that there were “some differences between the common law privacy torts and the DPPA” because the inquiry ““does not require an exact duplicate in American history and tradition.”” *Id.* (quoting *TransUnion*, 594 U.S. at 424). By pleading a violation of a statute “aimed squarely at ‘the right of the plaintiff . . . to be let alone,’” the plaintiffs had standing. *See id.* (cleaned up) (quoting William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 389 (1960)).

Garey applies with full force here.¹⁰ Just as the drivers in *Garey* alleged personal injury lawyers invaded their privacy by obtaining their personal information, the plaintiffs allege the DOGE affiliates have invaded their privacy by obtaining their personal information. The privacy

¹⁰ The Court relied on *Garey* in its TRO ruling, *see* ECF 38, at 12, but the government did not address *Garey* at all in its opposition to the preliminary injunction motion, *see* ECF 62.

invasion here is far more severe than in *Garey*: The information the personal injury lawyers obtained—the drivers’ names and addresses—pales in comparison to the information the DOGE affiliates have obtained. That information includes the plaintiffs’ banking information; Social Security numbers; dates of birth; physical and email addresses; income and asset information; demographic information such as marital and citizenship status; employment records such as personnel actions; and information about family members, such as their financial status, demographic information, dates of birth, and addresses. If the drivers in *Garey* established a cognizable privacy injury by merely alleging their names and addresses were unlawfully obtained, the plaintiffs have established a privacy injury in spades.¹¹

And just as the plaintiffs in *Garey* alleged a violation of the DPPA, a privacy statute, the plaintiffs have alleged a violation of the Privacy Act, another privacy statute. “[W]hile the common law offers guidance, it does not stake out the limits of Congress’s power to identify harms deserving a remedy.” *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462–63 (7th Cir. 2020). “Congress is empowered to ‘elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law’. . . .” *Krakauer*, 925 F.3d at 654 (quoting *Spokeo*, 578 U.S. at 341). That is precisely what Congress did with the Privacy Act. The

¹¹ There is a factual difference between *Garey* and this case that, at first blush, might suggest *Garey* is materially distinguishable. In *Garey*, the personal injury lawyers not only obtained the drivers’ names and addresses, but they also used the information to mail the drivers unwanted solicitations. 35 F.4th at 920. Here, by contrast, there is no allegation that the DOGE affiliates have used the plaintiffs’ personal information to, for example, contact them. This difference does not matter for purposes of Article III standing. In *Garey*, the “cognizable privacy injury” was “having [the drivers’] privacy invaded by [the lawyers’] knowingly obtaining [their] name[s] and address[es] from motor vehicle record[s] for an impermissible purpose in violation of law.” *Id.* at 922. That the lawyers then used the information they obtained to mail unsolicited advertisements was not a reason why the Court found a privacy injury. Here, the plaintiffs’ cognizable privacy injury occurred when the DOGE affiliates obtained access to their personal information. Nothing more, under *Garey*, is required to establish concrete injury in fact.

Privacy Act is meant “to protect the privacy of individuals identified in information systems maintained by Federal agencies” by “regulat[ing] the collection, maintenance, use, and dissemination of information by such agencies.” *Doe v. Chao* (“*Chao P*”), 540 U.S. 614, 618 (2004) (quoting Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896). The Privacy Act’s purposes include “prevent[ing] the kind of illegal, unwise, overbroad, investigation and record surveillance of law abiding citizens produced in recent years from actions of some overzealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.” *Doe v. DiGenova*, 779 F.2d 74, 84 (D.C. Cir. 1985) (quoting S. Rep. No. 1183, 93d Cong., 2d Sess., *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6916)). So just like the drivers in *Garey*, the plaintiffs have alleged a violation of a statute “aimed squarely at the right. . . to be let alone.” *See Garey*, 35 F.4th at 922 (citation omitted). Their harm is closely related to an invasion of privacy. *See id.* at 921–22; *Pileggi v. Wash. Newspaper Publ. Co., LLC*, No. 23-345, 2024 WL 324121, at *5 (D.D.C. Jan. 29, 2024), *appeal pending*, (D.C. Cir.) (holding unlawful disclosure of consumer’s information to third party in violation of Video Privacy Protection Act bears close relationship to intrusion upon seclusion, “which subjects [a person] to liability for invasion of privacy”).¹²

To put a finer point on it, the plaintiffs’ injuries closely resemble a specific type of invasion of privacy—the common law tort of intrusion upon seclusion. “The right of privacy is invaded by,” among other things, “unreasonable intrusion upon the seclusion of another.” Restatement

¹² In *Garey*, the Fourth Circuit found that the plaintiffs did not have standing to sue for *injunctive* relief—and could sue only for money damages—because they did not allege “an ongoing or imminent ‘obtaining’ . . . violation vis-à-vis their own personal information.” *See* 35 F.4th at 922–24. Instead, “the obtaining of their personal information [wa]s a *fait accompli*.” *Id.* at 923. Here, the plaintiffs allege ongoing access to their sensitive personal information. They have “establish[ed] a sufficient likelihood of future injury.” *All. for Hippocratic Med.*, 602 U.S. at 381. Thus, they have alleged an injury-in-fact sufficient to sue for injunctive relief.

(Second) Torts § 652A. The Second Restatement of Torts defines “intrusion upon seclusion” as “intentional[] intru[sion], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, . . . if the intrusion would be highly offensive to a reasonable person.” *Id.* § 652B.

According to the plaintiffs’ allegations, declarations from government employees, and the administrative records, Education, OPM, and Treasury gave DOGE affiliates access to the plaintiffs’ sensitive personal information—data that obviously concerns their “private affairs.” The plaintiffs gave their private information to the government with the expectation that the government would not disclose it to anyone within the government who was not authorized to access it. *See* ECF 14-3, ¶¶ 7–10; ECF 14-4, ¶¶ 5–8; ECF 14-5, ¶¶ 6–9; ECF 14-6, ¶¶ 5–8; ECF 14-7, ¶¶ 7–10; ECF 14-8, ¶¶ 6–9; ECF 14-9, ¶¶ 6–9; ECF 14-10, ¶¶ 10–13; ECF 14-11, ¶¶ 5–8; ECF 14-12, ¶¶ 8–11. If the agencies’ disclosures violated the Privacy Act, as the Court must assume for purposes of the standing analysis, then the plaintiffs have established that their trust has been breached, that government employees who should not have access to their information do, and that those employees have accessed records containing their PII. Access to those records by unauthorized government officials intrudes into their private lives. This intrusion is not speculative; it is actual. The plaintiffs allege that DOGE affiliates have accessed information in record systems at each of the agencies. *See* ECF 13, ¶¶ 12, 55, 80, 85, 103–04, 110, 139. And the government submitted declarations that strongly suggest DOGE affiliates at all three agencies have accessed record systems that contain the plaintiffs’ PII. *See* ECF 27-1, ¶¶ 15–16 (T. Krause Decl.); ECF 27-7, ¶ 4 (T. Flagg Decl.); ECF 33-1, ¶¶ 11–12 (G. Hogan Suppl. Decl.). If no injunction were in place, the DOGE affiliates would continue to access records containing PII because, according to the government, the DOGE affiliates *need* to access these records to do their jobs.

See, e.g., ECF 62, at 26 (“all of the relevant employees have a need for the records to which they have access in the performance of their duties”); *see also* ECF 27-1, ¶ 15; ECF 27-3, ¶ 11; ECF 27-5 (A. Ramada Decl.), ¶ 9; ECF 33-1, ¶¶ 11–12. This ongoing intrusion into the plaintiffs’ private affairs is highly offensive to a reasonable person. *See, e.g., Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009) (“[C]onduct 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 . . .”). The plaintiffs’ alleged harms are closely related to intrusion upon seclusion.

The government argues that “[m]ere access to data housed by a government agency by government employees—even if the *quantity* of data is potentially large—does not bear the ‘close relationship to [the] traditional harm’ of intrusion upon seclusion.” ECF 62, at 14. This argument completely ignores the fact that the plaintiffs have a privacy interest in restricting access to their personal information *within* the government. They gave detailed sensitive personal information to the government for the purposes of obtaining federal employment, student loans, and government benefits with the expectation that only authorized government employees could access it. They now claim that, without their consent, the government has handed over their personal information to government employees who are not authorized to access it. To say that the plaintiffs suffer no intrusion upon their private affairs when their personal information is accessed by government employees who have no right to access it would nullify their cognizable interest in preventing unlawful government intrusion into their private affairs.¹³

¹³ The government argues the plaintiffs must allege an unauthorized public disclosure—disclosure to someone outside of government—to establish concrete injury in fact. But the common law tort of intrusion upon seclusion does not require public disclosure of personal information. Intrusion upon seclusion, unlike the tort of public disclosure of private information, “does not depend upon any publicity given to the person whose interest is invaded or to his affairs.” Restatement (Second)

The government insists that the alleged intrusion here is dissimilar from the types of intrusions contemplated by the Restatement. In the government’s view, intrusion upon seclusion “involve[s] more than mere access to records—[it] involve[s] an actual ‘intrusion,’ such as examination or review of sensitive material.” ECF 62, at 15. This argument, too, fails for several reasons.

First, the intrusion here is similar to the types of intrusion contemplated by the Restatement. The Restatement explains that a person’s privacy is invaded when there is “some . . . form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.” Restatement (Second) of Torts, § 652B, cmt. b. Here, the plaintiffs allege their privacy has been similarly invaded. Their PII is stored in government record systems—virtual filing cabinets with scores of information about their family, employment history, personal finances, and banking information, to name only a few. The plaintiffs trusted that the government would safeguard the keys to these virtual filing cabinets. Now, the plaintiffs allege that the agencies have handed the keys to government employees who are not authorized to open the cabinets but are doing so anyway. This alleged intrusion is just as, if not more, intrusive than an examination of a wallet or bank record.

Second, the Fourth Circuit in *Krakauer* rejected a similar argument that the alleged harm was not the same as an intrusion upon seclusion. In *Krakauer*, the intrusion was unwanted phone calls. There, the court explained that “Article III’s injury-in-fact requirement” does not have to

Torts, § 652B, cmt. a. The disclosure to unauthorized government employees suffices. *See, e.g., Hamberger v. Eastman*, 206 A.2d 239, 242 (N.H. 1964) (“The tort of intrusion on the plaintiffs’ solitude or seclusion does not require publicity and communication to third persons”).

rise “to a level that would support a common law cause of action.” 925 F.3d at 653–54. “This sort of judicial grafting is not what *Spokeo* had in mind.” *Id.* at 654. Instead, “[o]ur inquiry is focused on types of harms protected at common law, *not the precise point at which those harms become actionable.*” *Id.* (emphasis added); *see also Drazen v. Pinto*, 74 F.4th 1336, 1343 (11th Cir. 2023) (holding that “a close relationship” between alleged privacy invasion and intrusion upon seclusion does “not require carbon copies”).

As in *Krakauer*, the Court’s inquiry is focused on the type of harm protected at common law. That harm—intrusion upon seclusion—is closely related to the harm alleged here. Even if the facts in this case do not perfectly match the Restatement’s examples of intrusion, a perfect match is not necessary. The injury-in-fact inquiry “does not require an exact duplicate in American history and tradition.” *Garey*, 35 F.4th at 922 (quoting *TransUnion*, 594 U.S. at 424).

Finally, the government argues that “mere access to records,” without actual examination of the records, is not an intrusion upon seclusion. ECF 62, at 15. The government is incorrect. An unauthorized government employee’s access to sensitive personal information protected by the Privacy Act is an intrusion into private affairs. Even if it were not, there is more than mere access here. On the government’s account, the DOGE affiliates with “mere access to records” actually “have a *need* for the records to which they have access in the performance of their duties.” *See id.* at 26 (emphasis added); *id.* at 27 (at Treasury, DOGE affiliates “have a need to access Privacy Act-protected records”; at OPM, they “need to access such records”; and at Education, they “need to access such records”) (citations omitted)). If, by the government’s own lights, the DOGE affiliates *need* access to the Privacy Act-protected records to perform their duties, then the DOGE affiliates must be putting that access to use. And the government has introduced evidence that says as much, including declarations that DOGE affiliates are accessing the agencies’ systems and

records with sensitive personal information. *See* ECF 27-1, ¶¶ 15–16; ECF 27-3, ¶ 13, 18–19; ECF 27-5, ¶ 9; ECF 27-6, ¶ 7; ECF 27-7, ¶ 4; ECF 33-1, ¶¶ 11–13. This evidence aligns with the plaintiffs’ allegations that DOGE affiliates are accessing and examining the records containing their personal information. *See* ECF 13, ¶¶ 12, 54–55, 80, 85, 103–04, 110, 139. So, the government’s argument that “mere access to records” is insufficient to establish a concrete injury does not hold water. The plaintiffs have established an ongoing, concrete privacy injury.¹⁴

The government insists that the Court’s finding of standing cannot be squared with the Fourth Circuit’s decision in *O’Leary v. TrustedID, Inc.* Once again, the government is incorrect. In *O’Leary*, the Fourth Circuit held that an alleged violation of an identity theft statute did not closely relate to intrusion upon seclusion. 60 F.4th 240, 245 (4th Cir. 2023). The plaintiff, Brady O’Leary, input six digits of his Social Security number into a website to determine whether his data had been compromised in a data breach. *Id.* at 241. It had not. *Id.* Still, O’Leary filed suit against the website’s owner for an alleged violation of South Carolina’s Financial Identity Fraud and Identity Theft Protection Act, which prohibits “requir[ing] a consumer to use his social security number or a portion of it containing six digits or more to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site.” *Id.* (quoting S.C. Code Ann. § 37-20-180(A)(4)). When the Fourth Circuit addressed whether O’Leary had alleged a concrete injury in fact from this statutory violation, it observed that he had “pleaded that he chose to hand over his partial SSN ‘[i]n exchange for’ finding out whether he was impacted by Equifax’s data breach.” *Id.* at 246

¹⁴ *See also All. for Retired Ams.*, 2025 WL 740401, at *17 (finding concrete injury where “Plaintiffs’ members disclosed their information to Treasury; individuals falsely purporting to have lawful access to that information demanded its disclosure; when Treasury acquiesced to that demand, the individuals invaded Plaintiffs’ members’ privacy”).

(citation omitted). Those allegations, the Fourth Circuit held, were not “anything that closely relates” to “the unwanted intrusion into the home that marks intrusion upon seclusion.” *Id.* The court concluded that O’Leary had not “adequately pled that he was injured by the alleged statutory violation at all—much less in a way that closely relates to a traditional analog for a federal lawsuit.” *Id.* at 246.

This case is not *O’Leary*. O’Leary did not allege a violation of a statute that protected his right to privacy, as the plaintiffs have. O’Leary did not allege he entrusted troves of sensitive personal information to a party who breached his trust by unlawfully disclosing the information to others, as the plaintiffs have. O’Leary did not even allege that he expected the website not to disclose the last six digits of his Social Security number to anyone or that the website ever did disclose it. While the facts in *O’Leary* did not amount to an “unwanted intrusion into the home,” they do here. What could be more “home” than one’s Social Security number, banking information, income and asset information, and marital and citizenship status?

The ongoing unlawful access to the plaintiffs’ sensitive personal information by DOGE affiliates who are not authorized to access it is a concrete injury in fact.¹⁵ The plaintiffs have demonstrated that they have standing.

B. Final Agency Action

The APA allows for judicial review of “final agency action for which there is no other adequate remedy in a court.” 5 U.S.C. § 704. Whether there is a final agency action is a

¹⁵ The plaintiffs have suggested they suffered another injury in fact: the risk of identity theft. To establish standing based on the risk of identity theft, the plaintiffs must show that “their contention of an enhanced risk of future identity theft” is more than “speculative.” *See Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017). Because the Court finds that the unauthorized disclosure of sensitive personal information is a concrete injury, it need not decide whether the risk of identity theft also is a concrete injury.

jurisdictional question in the Fourth Circuit. *See, e.g., Jake’s Fireworks Inc. v. Consumer Prod. Safety Comm’n*, 105 F.4th 627, 631 (4th Cir. 2024) (“finality under the APA is a jurisdictional requirement”).

“‘[A]gency action’ includes the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act.” 5 U.S.C. § 551(13). “[T]he term is not so all-encompassing as to authorize [courts] to exercise ‘judicial review [over] everything done by an administrative agency.’” *Indep. Equip. Dealers Ass’n v. EPA.*, 372 F.3d 420, 427 (D.C. Cir. 2004) (quoting *Hearst Radio, Inc. v. FCC*, 167 F.2d 225, 227 (D.C. Cir. 1948)). Even so, “‘agency action’ undoubtedly has a broad sweep.” *Id.* “[T]he word ‘action[]’ . . . is meant to cover comprehensively every manner in which an agency may exercise its power.” *Whitman v. Am. Trucking Ass’ns*, 531 U.S. 457, 478 (2001); *see also FTC v. Standard Oil Co.*, 449 U.S. 232, 238 n.7 (1980) (“According to the legislative history of the APA: ‘The term “agency action” . . . assure[s] the complete coverage of every form of agency power, proceeding, action, or inaction.’” (quoting S. Doc. No. 248, 79th Cong., 2d Sess., 255 (1946))). The term “action” encompasses an agency’s “policy or routine practice.” *Amadei v. Nielsen*, 348 F. Supp. 3d 145, 164 (E.D.N.Y. 2018). And an agency policy is reviewable even when “the details of the . . . policy are still unclear.” *See Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 929–30 (D.C. Cir. 2008). An agency action need not even be written down. *See R.I.L.-R v. Johnson*, 80 F. Supp. 3d 164, 184 (D.D.C. 2015) (concluding plaintiffs “attack[ed] *particularized* agency action” even though they did not “cite any statute, regulation, policy memoranda, or any other document memorializing the policy they challenge[d]”); *Grand Canyon Tr. v. Pub. Serv. Co.*, 283 F. Supp. 2d 1249, 1252 (D.N.M. 2003) (“Unwritten agency actions have been subjected to judicial review under the

Administrative Procedure[] Act.” (citation omitted) (citing *San Juan Audubon Soc’y v. Veneman*, 153 F. Supp. 2d 1, 5–6 (D.D.C. 2001)).

The administrative records reveal that, in the earliest days of the new presidential administration, Education, OPM, and Treasury granted DOGE affiliates access to agency systems that house records containing the plaintiffs’ PII. They granted this access so that DOGE affiliates could implement the DOGE Executive Order.

At Education, CIO Thomas Flagg authorized “full and prompt access to all unclassified IT systems and data” to “USDS personnel onboarded to the Department of Education DOGE team” to “support the implementation of the [DOGE Executive Order].” ED-000025.

At OPM, declarations from the CIO describe “individuals with access to sensitive OPM records systems who are working to implement [the DOGE Executive Order],” ECF 27-8, ¶ 12 (G. Hogan Decl.), and “five key systems engineers, besides myself, implementing [the DOGE Executive Order],” ECF 33-1, ¶ 13; *see also* ECF 51-1, at 2 (certification of OPM administrative record describing “the granting of access to data systems to employees implementing [the DOGE Executive Order]”). In an email with the subject line “Getting DoGE Engineers access,” Acting Director Ezell directed an OPM employee to grant OPM DOGE affiliates access to agency records because OPM was “rapidly ramping up [these] engineers.” OPM-000028. Other emails confirm that OPM granted DOGE affiliates extensive access to OPM systems based on Acting Director Ezell’s request to quickly give political staff system administrator access. *See* OPM-000104, OPM-000107 (email chain with subject line “Re: urgent request from political tech staff” describing process by which OPM granted “administrator accounts with super user permissions” to “Individuals from the Political Team” at “[t]he request . . . [of] the Acting Director to MC on Monday January 20th to add these people to the system as admins”); OPM 000108 (“We have

already given several of the political devs/engineers comprehensive access Now we have 3 more individuals with the same requirement.”); OPM-000110 (February 3, 2025 email forwarding a request from OPM Chief of Staff Amanda Scales for OPM-8 to have “account creation info” with “admin access” for USA Staffing, “[s]imilar to” access granted to another DOGE affiliate pursuant to Acting Director Ezell’s January 27, 2025 email).

At Treasury, the engagement plan between the agency and “USDS/DOGE” describes the “ongoing Payment Process Engagement” whereby the “Fiscal Service is supporting the USDS/DOGE team during their 4–6-week engagement to understand payment processes and opportunities to advance payment integrity and fraud reduction goals.” TR-0057. The engagement plan sets forth how access to Fiscal Service systems will proceed, including how “USDS/DOGE confirmed” that the “designated technical team member[] requires access to Fiscal Service systems and data” and how “USDS/DOGE requested to be granted ‘over the shoulder’ access to monitor Fiscal Service personnel conducting payment processing roles, which was approved by Fiscal Service on 1/23/25.” TR-0058–59.

As these memoranda, declarations, and emails show, it is the policy of Education, OPM, and Treasury to grant DOGE affiliates access to agency record systems so that they may implement the DOGE Executive Order. *See Amadei v. Nielsen*, 348 F. Supp. 3d at 165 (inferring “existence of an official policy” of U.S. Customs and Border Patrol to request identification documents at the end of domestic flights even though the complaint did not allege an official policy); *De La Mota v. U.S. Dep’t of Educ.*, No. 02-CV-4276, 2003 WL 21919774, at *8 (S.D.N.Y. Aug. 12, 2003) (“[I]t is of no moment that the agency action here came in the form of an ‘informal’ email correspondence between a DOE employee and the law schools and plaintiffs.”); *see also Venetian*, 530 F.3d at 931 (deeming “the decision of the Commission to adopt a policy of disclosing

confidential information without notice” an agency action even though the policy was only referenced in a compliance manual). Even if “the details of the . . . policy are still unclear,” what is clear is that each agency has a policy of granting DOGE affiliates access to agency records systems, which include the plaintiffs’ PII. *See Venetian*, 530 F.3d at 929. The plaintiffs have challenged an agency action.

The government insists that by finding a reviewable agency action in this case, the Court is sanctioning judicial review over “broad programmatic attacks,” when judicial review should be limited to discrete agency actions. *See* ECF 62, at 18 (citing *Norton v. S. Utah Wilderness All.* (“*SUWA*”), 542 U.S. 55, 64 (2004) and *Lujan*, 497 U.S. at 891). The government is correct that “[c]ourts are well-suited to reviewing specific agency decisions” and are “woefully ill-suited . . . to adjudicate generalized grievances asking [the court] to improve an agency’s performance or operations.” *See City of New York v. U.S. Dep’t of Def.*, 913 F.3d 423, 431 (4th Cir. 2019); *see also id.* at 432 (“[C]ourts [may] review only those acts that are specific enough to avoid entangling the judiciary in programmatic oversight, clear enough to avoid substituting judicial judgments for those of the executive branch, and substantial enough to prevent an incursion into internal agency management.”). But the government is incorrect that the Court is reviewing an agency’s “performance or operations.” *Id.* Contrast the facts here with those in *Lujan* and *SUWA*. In *Lujan*, the National Wildlife Federation (“NWF”) broadly challenged what it termed Bureau of Land Management’s (“BLM”) “land withdrawal review program,” a term that encompassed “the continuing (and thus constantly changing) operations of the BLM in reviewing withdrawal revocation applications and the classifications of public lands and developing land use plans as required by [statute].” 497 U.S. at 890. The Court concluded that the NWF did not challenge “an identifiable ‘agency action’” because the term “land withdrawal review program” did “not refer to

a single BLM order or regulation, or even to a completed universe of particular BLM orders and regulations.” *Id.* In *SUWA*, organizations sought to compel agency action because they believed BLM had “fail[ed] to act to protect public lands in Utah from damage caused by ORV [off-road vehicle] use.” 542 U.S. at 60. The organizations “claim[ed], that by permitting ORV use in certain WSAs [wilderness study areas], BLM violated its mandate to ‘continue to manage [WSAs] . . . 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)). The Supreme Court observed that the challenged agency action had to be “discrete” for a remedy to exist under the APA and that “[t]he limitation to discrete agency action precludes the kind of broad programmatic attack [the Court] rejected in *Lujan*.” *Id.* at 62, 64. On that basis, it rejected the organizations’ request that the Court order BLM “to comply with the [statute’s] nonimpairment mandate” because “[g]eneral deficiencies in compliance . . . lack the specificity requisite for agency action.” *Id.* at 66.

This case is not *Lujan* or *SUWA*. Here, the plaintiffs do not challenge the “continuing (and thus constantly changing) operations of” the agencies, *see Lujan*, 497 U.S. at 873, or any “[g]eneral deficiencies in compliance” by the agencies, *see SUWA*, 542 U.S. at 66. The plaintiffs challenge the discrete agency decisions to grant DOGE affiliates access to systems that contain records with their PII. They ask the Court to stop the agencies from taking a specific action that they believe is contrary to law.

Next, the government argues that the plaintiffs are asking the Court to review the agencies’ “‘workaday’ dealings,” which are beyond the scope of judicial review. ECF 62, at 17 (quoting *Indep. Equip. Dealers Ass’n*, 372 F.3d at 427). The government likens the agency decisions at issue here to setting up employee email accounts, staffing decisions, and managing government programs. *Id.* at 17, 18. Trivial decisions about day-to-day workplace operations and even

substantive decisions about program management are hardly comparable. Unlike the “workaday” decisions in the government’s strained analogy, the agencies’ decisions to grant DOGE affiliates access to records with the PII of millions of Americans impacts the privacy rights of the people whose PII is housed within these systems. These decisions are agency actions.

And they are final agency actions. An agency action is “final” when two conditions are met: (1) “the action must mark the ‘consummation’ of the agency’s decisionmaking process—it must not be of a merely tentative or interlocutory nature,” and (2) “the action must be one by which ‘rights or obligations have been determined,’ or from which ‘legal consequences will flow.’” *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997) (first quoting *Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 113 (1948); and then quoting *Port of Boston Marine Terminal Ass’n v. Rederiaktiebolaget Transatl.*, 400 U.S. 62, 71 (1970)).

In *Venetian Casino Resort, L.L.C. v. EEOC*, the D.C. Circuit concluded that an agency’s decision to permit its employees to disclose confidential information without notice was a final agency action. 530 F.3d at 930–31. There, a company operating a hotel and casino (“Venetian”) filed suit against the EEOC. *Id.* Venetian asserted the EEOC violated the APA through a policy that allowed EEOC “employees to disclose an employer’s confidential information to potential . . . plaintiffs without first notifying the employer that its information [would] be disclosed.” *Id.* The EEOC argued that Venetian could not bring an APA claim because the challenged policy was referenced in its compliance manual, which was not a final agency action. *Id.* at 931. According to the D.C. Circuit, EEOC’s “argument [was] misdirected” because the final agency action at issue was not the manual but rather “the decision of the Commission to adopt a policy of disclosing confidential information without notice.” *Id.* “The Manual [wa]s relevant insofar as it illuminate[ed] the nature of the policy.” *Id.* The court determined that “the agency took final action

by adopting the policy” and that this action was subject to judicial review. *Id.* Ultimately, the *Venetian* Court found that “[a]dopting a policy of permitting employees to disclose confidential information without notice is surely a ‘consummation of the agency’s decisionmaking process’” and “‘one by which [the submitter’s] rights [and the agency’s] obligations have been determined.’” *Id.* (quoting *Bennett*, 520 U.S. at 178). The D.C. Circuit remanded the case for entry of “an injunction prohibiting the [EEOC] from disclosing Venetian’s confidential information pursuant to its current disclosure policy.” *Id.* at 927.

Here, as in *Venetian*, the decisions to grant DOGE affiliates access to agency record systems were final agency actions. Education, OPM, and Treasury granted DOGE affiliates access to systems that contain records with the plaintiffs’ PII. The decisions to grant access were neither tentative nor interlocutory in nature. They were “the ‘consummation’ of the agenc[ies]’ decisionmaking process.” *See Bennett*, 520 U.S. at 177–78 (quoting *Chicago & S. Air Lines*, 333 U.S. at 113). There was nothing further for the agencies to do to formalize the decisions. And while the agencies can and have revoked DOGE affiliates’ access to certain systems, that authority does not make their decisions tentative or interlocutory. The agencies decided that DOGE affiliates could access agency records containing PII and gave the affiliates such access. The agency actions marked the consummation of the agency’s decisionmaking process.

And here, as in *Venetian*, Education, OPM, and Treasury “[a]dopt[ed] a policy of permitting . . . disclos[ure]” that determines the plaintiffs’ legal rights and the agencies’ legal obligations. *See Venetian*, 530 F.3d at 931. The Privacy Act prohibits disclosure of the records at issue “except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains,” unless the disclosure falls within an enumerated exception. *See* 5 U.S.C. § 552a(b). The agencies determined that, to comply with the Privacy Act, they did not need

the plaintiffs’ consent to disclose their records to DOGE affiliates. Thus, the practical effect of the agencies’ decisions was to determine the plaintiffs’ rights and the agencies’ obligations under the Privacy Act. *See De La Mota*, 2003 WL 21919774, at *8 (“The practical effect of the DOE’s action, not the informal packaging in which it was presented, is the determining factor in evaluating whether the DOE’s action was ‘final.’”).

The government argues the agencies’ decisions had no “actual legal effect.” ECF 62, at 19 (citing *Nat’l Mining Ass’n v. McCarthy*, 758 F.3d 243, 252 (D.C. Cir. 2014) and *Mashni v. U.S. Army Corps of Eng’rs*, 535 F. Supp. 3d 475, 482 (D.S.C. 2021)). Here, too, they are mistaken. “Whether an agency action has ‘direct and appreciable legal consequences’ under the second prong of *Bennett* is a ‘pragmatic’ inquiry.” *Sierra Club v. EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020) (cleaned up) (quoting *U.S. Army Corps of Eng’rs v. Hawkes Co.*, 578 U.S. 590, 598–99 (2016)). The agencies determined that disclosure of the plaintiffs’ PII did not require their consent and that such disclosure fell within one of the Privacy Act’s exceptions. Thus, the decisions of Education, OPM, and Treasury had a legal effect: They determined the plaintiffs’ rights and the agencies’ obligations under the Privacy Act.

This case is not, as the government argues, similar to *Sierra Club v. EPA*, 955 F.3d 56. In *Sierra Club*, the D.C. Circuit held that agency guidance concerning a state permitting process was not final agency action because “it d[id] not determine rights or obligations and d[id] not effectuate direct or appreciable legal consequences.” *Id.* at 58. The guidance “impose[d] no obligations, prohibitions or restrictions on regulated entities, d[id] not subject them to new penalties or enforcement risks, preserve[d] the discretion of permitting authorities, require[d] any permitting decision relying on the Guidance be supported with a robust record, and d[id] not prevent challenges to individual permitting decisions.” *Id.* at 63. The guidance was “*not necessary* for a

permitting decision,” and “permitting authorities [we]re free to completely ignore it.” *Id.* at 64. And the guidance “by itself d[id] not expose any regulated entity to the possibility of an enforcement action or to enhanced fines or penalties.” *Id.* at 65.

Sierra Club is inapposite. It involved mere agency guidance that did not impose rights or obligations on regulated entities or interfere with the discretion of the state authorities making permitting decisions. In contrast, the agency actions challenged here did “determine rights or obligations” and did “effectuate direct or appreciable legal consequences.” 955 F.3d at 58. The decision to grant DOGE affiliates access to agency systems with records containing PII had “direct or appreciable legal consequences” under the Privacy Act. *See id.* That statute—the “NorthStar” that “govern[s] the action at issue”—implicates the plaintiffs’ rights to protect their sensitive personal information from unlawful disclosure and the agencies’ obligations, with certain exceptions, to obtain their consent before disclosure. *See Cal. Cmty. Against Toxics v. EPA*, 934 F.3d 627, 631 (D.C. Cir. 2019) (“[C]ourts should take as their NorthStar the unique constellation of statutes and regulations that govern the action at issue.”).¹⁶

The agency decisions to grant DOGE affiliates access to systems that house records with the plaintiffs’ PII are final agency actions. *See New York v. Trump*, No. 25-CV-01144, 2025 WL 573771, at *19 (S.D.N.Y. Feb. 21, 2025) (finding Treasury’s decision to grant DOGE affiliates access to PII reviewable under the APA because “the APA allows challenges to unwritten agency policies and practices where the requirements of finality are otherwise satisfied”).

¹⁶ *California Communities Against Toxics v. EPA*, another case the government relies on, also is factually distinct. There, the D.C. Circuit held that an EPA memo forecasting the agency’s interpretation of a statute was not a final agency action because it “has no direct and appreciable legal consequences.” 934 F.3d at 638–39.

C. Preliminary Injunction

The party seeking a preliminary injunction must establish (1) that they are likely to succeed on the merits; (2) that they are likely to suffer irreparable harm if preliminary relief is not granted; (3) that the balance of equities favors them; and (4) that an injunction is in the public interest. *See Frazier v. Prince George’s County*, 86 F.4th 537, 543 (4th Cir. 2023) (citing *Winter*, 555 U.S. at 20).

1. Likelihood of Success on the Merits

i. Administrative Procedure Act

“Congress enacted the APA to provide a general authorization for review of agency action in the district courts.” *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988). The APA “requires agencies to engage in ‘reasoned decisionmaking’” and establishes procedures for judicial review and “accountab[ility] to the public.” *Dep’t of Homeland Sec. v. Regents of the Univ. of Cal.*, 591 U.S. 1, 16 (2020) (first quoting *Michigan v. EPA*, 576 U.S. 743, 750 (2015) (internal quotation marks omitted), and then quoting *Franklin v. Massachusetts*, 505 U.S. 788, 796 (1992)).

The APA directs courts to “hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law” or “in excess of statutory jurisdiction, authority, or limitations, or short of statutory right.” 5 U.S.C. § 706(2)(A),(C). In determining whether agency action is “not in accordance with law,” the court must “bear[] in mind that it is [the court’s] duty under the APA to ‘decide all relevant questions of law’ and to ‘interpret constitutional and statutory provisions.’” *Perez v. Cuccinelli*, 949 F.3d 865, 872 (4th Cir. 2020) (citing 5 U.S.C. § 706). “[W]here an agency’s decision does not comport with governing statutes or regulations, that decision is ‘not in accordance with law’ and must be set aside.” *J.E.C.M. ex rel. Saravia v. Lloyd*, 352 F. Supp. 3d

559, 583 (E.D. Va. 2018). An agency’s “order may not stand if the agency has misconceived the law.” *SEC v. Chenery Corp.*, 318 U.S. 80, 94 (1943). When a court makes a final decision on the merits that an agency made an error of law, “the case must be remanded to the agency for further action consistent with the corrected legal standards.” *PPG Indus., Inc. v. United States*, 52 F.3d 363, 365 (D.C. Cir. 1995) (citing *Chenery*, 318 U.S. at 94–95).

In its review, the court “must only consider the record made before the agency at the time the agency acted” because it “may not ‘intrude upon the domain which Congress has exclusively entrusted to an administrative agency.’” *Dow AgroSciences LLC v. Nat’l Marine Fisheries Serv.*, 707 F.3d 462, 467 (4th Cir. 2013) (quoting *Chenery*, 318 U.S. at 88). The record includes “the facts presented to the agency” and “the reasons given by the agency for taking the action.” *Id.* The record generally does not include “facts and justifications for agency action provided to a reviewing court for the first time.” *Id.* at 468. Put differently, the court “‘may not accept [the agency] counsel’s *post hoc* rationalizations for agency action’” because the “court may look only to the[] *contemporaneous* justifications in reviewing the agency action.” *Id.* at 467–68 (emphasis in *Dow AgroSciences*) (quoting *Motor Vehicle Mfr. Ass’n v. State Farm Auto. Ins. Co.*, 463 U.S. 29, 50 (1983)). “During its evaluation of the agency action, ‘the court shall review the whole record or those parts of it cited by a party, and due account shall be taken of the rule of prejudicial error.’” *Ergon-W. Va., Inc. v. EPA*, 980 F.3d 403, 410 (4th Cir. 2020) (quoting 5 U.S.C. § 706).

The court may, under narrow circumstances, look beyond the record. If the record utterly “fail[s] to explain administrative action” by not providing even a “curt” explanation and, as a result, “frustrate[s] effective judicial review,” the court may “obtain from the agency, either through affidavits or testimony, such additional explanation of the reasons for the agency decision as may prove necessary.” *Camp v. Pitts*, 411 U.S. 138, 142 (1973); see *Env’t Def. Fund, Inc. v.*

Costle, 657 F.2d 275, 285 (D.C. Cir. 1981) (noting that “[w]hen the record is inadequate,” the court may seek “additional explanations,” but “[t]he new materials should be merely explanatory of the original record and should contain no new rationalizations” (citing *Bunker Hill Co. v. EPA*, 572 F.2d 1286, 1292 (9th Cir. 1977))). Further, a “court may go outside [the] record for explanation of highly technical matters.” *J.H. Miles & Co., Inc. v. Brown*, 910 F. Supp. 1138, 1147 (E.D. Va. 1995) (citing *Asarco, Inc. v. EPA*, 616 F.2d 1153, 1159–60 (9th Cir. 1980)); *Bunker Hill*, 572 F.2d at 1292 (“[C]ourts are not straightjacketed to the original record in trying to make sense of complex technical testimony, which is often presented in administrative proceedings without ultimate review by nonexpert judges in mind.”).

To be clear, the court cannot accept a more fulsome explanation to supplant an explanation, albeit brief, in the record. If there is some explanation in the record, then the agency action must “stand or fall on the propriety of that [explanation], judged, of course, by the appropriate standard of review.” *Camp*, 411 U.S. at 143. If the explanation “is not sustainable on the administrative record made, then the [agency’s] decision must be vacated and the matter remanded . . . for further consideration.” *Id.*

ii. Privacy Act

Congress passed the Privacy Act “in light of the government’s ‘increasing use of computers and sophisticated information technology,’ which ‘greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.’” *Tankersley v. Almand*, 837 F.3d 390, 395 (4th Cir. 2016) (quoting the Privacy Act of 1974 § 2(a)(2)).

The Privacy Act prohibits agencies from “disclos[ing] any record which is contained in a system of records by any means of communication to any person, or to another agency, except

pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” 5 U.S.C. § 552a(b). This restriction on disclosure extends to employees within the agency. Disclosure to the agency’s employees is limited “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).

The Privacy Act defines a “record” 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.” *Id.* § 552a(a)(4). A “system of record” is “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” *Id.* § 552a(a)(5).

The Privacy Act does not define “disclosure,” but agencies have interpreted the term to include granting access to records. *See* OMB Guidelines, 40 Fed. Reg. 28948, 28953 (July 9, 1975) (“A disclosure may be either the transfer of a record or the granting of access to a record.”); 5 C.F.R. § 297.102 (“Disclosure means providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject’s authorized representative, parent, or legal guardian.”). Likewise, courts have construed the term “liberally to include not only the physical disclosure of the records, but also the accessing of private records.” *See Wilkerson v. Shinseki*, 606 F.3d 1256, 1268 (10th Cir. 2010); *Tolbert-Smith v. Chu*, 714 F. Supp. 2d 37, 43 (D.D.C. 2010) (reading “disclosure” to include “plac[ing] records . . . on a server accessible by other federal employees and members of the public”); *cf. Wilborn v. Dep’t of Health & Human Servs.*, 49 F.3d

597, 600–01 (9th Cir. 1995) (“[T]he Privacy Act, if it is to be given any force and effect, must be interpreted in a way that does not ‘go[] against the spirit’ of the Act” (quoting *MacPherson v. IRS*, 803 F.2d 479, 481 (9th Cir. 1986)), *abrogated on other grounds by Chao I*, 540 U.S. 614. Some courts have required “actual viewing or imminent viewing by another.” *Wrocklage v. Dep’t of Homeland Sec.*, 769 F.3d 1363, 1369 (Fed. Cir. 2014). But courts that have required more than mere transmission of records have suggested that disclosure occurs when “information has been exposed in a way that would facilitate easy, imminent access.” *See, e.g., In re Sci. Applications Int’l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 29 (D.D.C. 2014).

iii. The APA Claim

The plaintiffs assert that Education, OPM, and Treasury did not act “in accordance with law”—the Privacy Act—when they disclosed agency records containing the plaintiffs’ PII to DOGE affiliates. 5 U.S.C. § 706(2)(A). To determine whether the plaintiffs have established a likelihood of success on the merits of this claim, the Court confines its review of the final agency actions to the administrative records and looks outside the records only “for explanation of highly technical matters.” *J.H. Miles & Co.*, 910 F. Supp. at 1147 (citing *Asarco*, 616 F.2d at 1159–60). Upon review of the administrative records, the Court finds that the plaintiffs have shown a likelihood of success on the merits of their APA claim that Education, OPM, and Treasury took final agency actions “not in accordance with law.” 5 U.S.C. § 706(2)(A).¹⁷

¹⁷ At the TRO stage, the government argued that the plaintiffs have not stated an APA claim because they have an “adequate remedy” under the Privacy Act. *See* 5 U.S.C. § 704 (“[F]inal agency action[s] for which there is no other adequate remedy in a court are subject to judicial review.”). The government reasserted this argument in its opposition to the motion for a preliminary injunction. As the Court explained in the TRO, ECF 38, at 18–19, the Privacy Act provides a cause of action for damages when an agency improperly discloses records, but it does not provide a cause of action for injunctive relief in these circumstances. *See Doe v. Chao* (“*Chao II*”), 435 F.3d 492, 504–05 & n.17 (4th Cir. 2006). The plaintiffs seek injunctive relief, not damages. Thus, they do not have an adequate remedy under the Privacy Act. Their only available

The government does not dispute that the agencies granted DOGE affiliates access to systems of records that contain sensitive personal information subject to the Privacy Act, that the plaintiffs did not request disclosure of their PII contained in these systems, or that the agencies did not obtain the plaintiffs' consent before they granted DOGE affiliates access to the information. Still, the government insists the disclosures complied with the Privacy Act because, under the statute, the agencies did not need to obtain the plaintiffs' consent.¹⁸

The Privacy Act lists thirteen exceptions to the general rule that disclosure of agency records requires consent. *See* 5 U.S.C. § 552a(b). Of relevance here, disclosure is permitted “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). To fall within this exception, the disclosure must be within the agency that maintains the record, *see Britt v. Naval Investigative Serv.*, 886 F.2d 544, 547 (3d Cir. 1989), and the recipient must “examine[] the record in connection with the performance of duties assigned to him . . . in order to perform those duties properly,”

remedy is an APA action for injunctive relief. *See id.* at 504 n.17 (explaining that “[o]ften . . . injunctive relief for a Government’s violation of the [Privacy] Act” is “appropriate and authorized by the APA,” which “empower[s] courts to ‘hold unlawful and set aside agency action . . . found to be . . . not in accordance with [] law’”) (quoting 5 U.S.C. § 706(2)(A)). Thus, the plaintiffs challenge a “final agency action for which there is no other adequate remedy in a court.” *See* 5 U.S.C. § 704. The APA allows for judicial review of their claim.

¹⁸ The government also suggests that no “disclosure” has occurred because there is no evidence that the DOGE affiliate have actually viewed the plaintiffs’ information. For this proposition, they cite *Wrocklage v. Dep’t of Homeland Security*, 769 F.3d at 1368–69. But in *Wrocklage*, the Federal Circuit determined an email with an attachment that contained someone’s Social Security number, address, date of birth, and license plate number did not constitute “disclosure” of a record under the Privacy Act because “[i]t is undisputed that the recipient deleted the email and it is therefore not imminently viewable.” *Id.* at 1365–66, 1368–69. Here, absent injunctive relief, the plaintiffs’ records at Education, OPM, and Treasury would be “imminently viewable” by DOGE affiliates, *id.* at 1369, and the government has asserted that the DOGE affiliates need to access this information to perform their job duties. The agencies have disclosed the plaintiffs’ records for Privacy Act purposes. *See, e.g., Tolbert-Smith*, 714 F. Supp. 2d at 43.

Bigelow v. Dep't of Def., 217 F.3d 875, 877 (D.C. Cir. 2000). The government relies on the need-to-know exception to defend the disclosure of entire systems of records to DOGE affiliates at Education, OPM, and Treasury.

“[T]he need to know exception applies only to intra-agency disclosures.” *Britt*, 886 F.2d at 547. The government insists that the disclosures are intra-agency disclosures because the DOGE affiliates are employees of Education, OPM, and Treasury. The plaintiffs assert that at least some of the DOGE affiliates at Education are not employees. This dispute does not impact the likelihood of success analysis, because even if the disclosures were intra-agency, the administrative records do not show that the DOGE affiliates had “a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). The Court assumes, without deciding, that the DOGE affiliates are employees of the agencies that granted them access to systems of records.

Courts have found that the Privacy Act’s need-to-know exception applies when there is a valid explanation for why the employee needed access to the protected information to perform their job duties. *See, e.g., Howard v. Marsh*, 785 F.2d 645, 648 (8th Cir. 1986) (attorney and personnel specialist gathering information about a discrimination complaint against the agency needed complainant’s employment records to respond to the complaint); *Covert v. Harrington*, 876 F.2d 751, 752–54 (9th Cir. 1989) (Inspector General’s agents needed employees’ personnel files after receiving allegations that employees were falsifying their permanent residences to obtain a per diem); *Dinh Tran v. Dep’t of Treasury*, 351 F. Supp. 3d 130, 137–39 (D.D.C. 2019) (employees evaluating a detail request needed to know information in the requestor’s performance appraisal to evaluate her skillset and suitability for the detail), *aff’d per curiam* 798 F. App’x 649 (D.C. Cir. 2020).

For example, in *Bigelow v. Department of Defense*, Noyes, a U.S. Army colonel, reviewed the personnel file of Bigelow, whom Noyes supervised at the Pentagon. 217 F.3d at 876. Noyes reviewed Bigelow's personnel file after he "learned of allegations of misconduct concerning Bigelow," including "that he sometimes disappeared in foreign countries near sensitive international borders." *Id.* Bigelow sued the Department of Defense under the Privacy Act for the intra-agency disclosure of his personnel file. *See id.* The *Bigelow* Court's analysis focused on the need-to-know exception. The court explained that "[w]hat must be determined . . . is whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly." *Id.* at 877. As Bigelow's immediate supervisor, Noyes had a duty enumerated in Defense Department regulations to evaluate Bigelow's trustworthiness. *Id.* The court determined that because Noyes received information that "cast[] doubt" on Bigelow's trustworthiness, Noyes "had a need to examine the file in view of the doubts that had been raised in his mind about Bigelow and Bigelow's access to the country's top secrets." *Id.* The *Bigelow* Court assuaged the dissenting judge's concerns that the decision would "dramatically expand[] the number of people' within the military who may examine personnel files" by explaining that "[t]here may be many people in the military who have access to the nation's most important secrets, but we doubt that their supervisors regularly receive information casting doubt on their trustworthiness." *Id.* (quoting *id.* at 881–82 (Tatel, J., dissenting)). The court held that the need-to-know exception applied. *See id.* at 876, 878.

The Tenth Circuit reached the opposite conclusion in *Parks v. IRS*, 618 F.2d 677 (10th Cir. 1980). There, IRS employees sued the agency and the United States after other IRS employees used information from their personnel files to call them and solicit their purchase of U.S. Savings Bonds. *Id.* at 679. The government argued that "disclosure of savings bond information was

necessary to the performance of [the employees'] duties" because of an executive order signed by President Nixon. *Id.* at 681. The executive order "established an Interdepartmental Committee for the Voluntary Payroll Savings Plan for the Purchase of United States Savings Bonds." *See id.* The committee, "consist[ing] of the heads of all federal executive-branch agencies," was "charged . . . to formulate a plan of organization and sales promotion of the savings bond program." *Id.* The Tenth Circuit rejected the government's argument that the executive order justified the disclosure of the savings bond information from personnel files:

Even though this may have been a worthy effort, it does not justify the use of information derived from the personnel files of employees, particularly in view of the subsequent passage of the Privacy Act. In short, the order, which was at odds with the stated legislative purpose of the Privacy Act, does not license the defendants to violate the Privacy Act

Id. The court held that the need-to-know exception did not apply. *See id.* at 681.

These cases establish the framework for the Court's analysis of the need-to-know exception. Factually, they are like other Privacy Act cases where the exception is invoked to defend the disclosure of a limited number of records. Here, the need-to-know exception has been invoked to defend the disclosure of millions of records. There appears to be no precedent with similar facts. However, even under existing precedent, the agencies' disclosures likely violate the Privacy Act. As discussed in detail below, the administrative records do not explain why the DOGE affiliates at Education, OPM, and Treasury need access to the plaintiffs' PII to do their jobs. "[P]ermitt[ing] agency-wide distribution under § 552a(b)(1) without any showing of why each employee needed to receive the information would allow the exception to swallow the rule." *Dick v. Holder*, 67 F. Supp. 3d 167, 178 (D.D.C. 2014).

a. Education

DOGE affiliates have been granted seemingly unfettered access to Education’s unclassified systems of record. In a February 5, 2025 memorandum, Education’s CIO, Thomas Flagg, “document[ed] the need to know and authorize[d] USDS personnel onboarded to the Department of Education DOGE team full and prompt access to all unclassified IT systems and data.” ED-000025. These unclassified systems at Education include systems of records that contain many of the plaintiffs’ PII, including income and asset information, Social Security numbers, taxpayer identification numbers, dates of birth, demographic information (such as citizenship and marital statuses), and some similar information about family members. *See, e.g.*, Privacy Act of 1974; System of Records, 89 Fed. Reg. at 44656–57 (listing categories of records in the NSLDS); Privacy Act of 1974; System of Records, 88 Fed. Reg. at 41947–48 (listing categories of records in the CODS); Privacy Act of 1974; System of Records, 88 Fed. Reg. at 42222; Privacy Act of 1974; System of Records—Financial Management System (FMS), 73 Fed. Reg. at 178 (listing categories of records in the FMS); Privacy Act of 1974; System of Records, 88 Fed. Reg. at 42222 (listing categories of records in the FAS);¹⁹ *see also* ECF 14-3, ¶¶ 7–8; ECF 14-5, ¶¶ 6–7; ECF 14-7, ¶¶ 5, 8; ECF 14-8, ¶¶ 6–7; ECF 14-9, ¶¶ 6–7; ECF 14-10, ¶¶ 10–11; ECF 14-11, ¶¶ 5–6; ECF 14-12, ¶¶ 8–9.²⁰

The reasons *why* DOGE affiliates at Education need “full and prompt access to all unclassified IT systems and data” to perform their job duties are unclear. *See* ED-000025.

¹⁹ The Court takes judicial notice of the Federal Register. *See* 44 U.S.C. § 1507.

²⁰ The government submitted an extra-record declaration from Steven Matteson, “an Executive Project Manager at the U.S. Department of Education, Federal Student Aid.” ECF 62-1, ¶ 1 (S. Matteson Decl.). Matteson declares that he conducted a system access audit for NSLDS, COD, FAS, and FMS on March 7, 2025, and identified only one DOGE affiliate at Education—Adam Ramada—with a user account that “had access to, or had accessed, any of th[e]se four systems”—

According to the February 5 memorandum from Education’s CIO, access was granted to “support the implementation of” the DOGE Executive Order. *Id.* The DOGE Executive Order states that DOGE is established “to implement the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.” DOGE Executive Order § 1. In pursuit of that purpose, the Executive Order directs agency heads to establish “DOGE Teams,” with “DOGE Team Leads” that “coordinate their work with USDS and advise their respective Agency Heads on implementing the President’s DOGE Agenda.” *Id.* § 3(c). 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 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). The DOGE Executive Order does not explain why DOGE affiliates at Education (or any agency for that matter) need access to “all unclassified IT systems and data” to modernize technology and software. *See* ED-000025. And by merely citing to the DOGE Executive Order, the February 5 memorandum does not explain

the FMS. *Id.* ¶¶ 2–4. Matteson affirmed that Ramada’s user account access was “substantially limited” as he “could not access any personally identifiable information.” *Id.* ¶ 4. The Court will not consider Matteson’s declaration to assess the merits of the plaintiffs’ APA claim because it is not in the administrative record. In the record, there is no evidence that the sweeping access authorized by the February 5, 2025 memorandum has been curtailed. Even if the Court considered extra-record evidence, other government declarations contradict Matteson’s statements. Ramada declared on February 13 that the DOGE affiliates at Education “require access to Department of Education information technology and data systems related to student loan programs in order to audit those programs for waste, fraud, and abuse.” *See* ECF 27-5, ¶ 9. Education CIO Flagg declared on February 15 that DOGE affiliates “have accessed Department information technology and data systems.” *See* ECF 27-7, ¶ 4. And the government has asserted that DOGE affiliates at Education “need access to [Privacy Act-protected] records in order to audit student loan programs for waste, fraud, and abuse.” ECF 62, at 27. The government cannot, on the one hand, ask the Court to rely on one extra-record declaration that says DOGE affiliates are not accessing PII, and on the other, assert that DOGE affiliates need access to this information.

why full access to Education systems and data—which contain the sensitive personal information of millions of Americans, including many of the plaintiffs—is *necessary* for DOGE affiliates at Education to “support the implementation of” the DOGE Executive Order. *See id.*²¹

The DOGE affiliates may need some form of system access to modernize technology and software, but that does not mean that they need access to all of the records containing PII housed in those systems. At least one of Education’s systems of records allows for masking PII with “dummy” data, but there is no indication in the administrative record that the DOGE affiliates’ access is limited in this manner. *See* Education, *Privacy Impact Assessment (PIA) for the Financial Management System (FMS)* 21 (2024), <https://www.ed.gov/sites/ed/files/notices/pia/fsa-financ-manag-syst.pdf> [<https://perma.cc/3JKT-K7WK>].²² By granting “full and prompt access” to all unclassified IT systems and data to DOGE affiliates, Education apparently did not contemplate limiting access to avoid the disclosure of PII. *See* ED-000025. An agency may not grant extensive access to records with PII “without any *showing* of why each employee needed to receive the information.” *Dick*, 67 F. Supp. 3d at 178 (emphasis added); *see also Walker v. Gambrell*, 647 F. Supp. 2d 529, 538 n.4 (D. Md. 2009) (explaining disclosure did not fall within the need-to-know exception because “it is difficult to see how knowledge with such specificity was necessary”); *cf. Vargas v. Reno*, No. 99-2725, slip op. at 13 (W.D. Tenn. Mar. 30, 2000) (denying government’s

²¹ The DOGE Executive Order instructs agency heads to grant “full and prompt access to all unclassified records, software systems, and IT systems,” but only “to the maximum extent consistent with law.” DOGE Executive Order § 4(b). When agency heads implemented the DOGE Executive Order, they had to comply with the Privacy Act.

²² The Court takes judicial notice of Privacy Impact Assessments and Privacy and Civil Liberties Impact Assessments retrieved from government websites. *See United States v. Garcia*, 855 F.3d 615, 621 (4th Cir. 2017) (“This court and numerous others routinely take judicial notice of information contained on state and federal government websites.”).

summary judgment motion on Privacy Act claim of unlawful intra-agency disclosure to an investigator where “[d]efendants ha[d] not submitted evidence that Vargas had potentially violated any law or regulation or that Vargas’s records were relevant or necessary to [the] investigation”). Neither the February 5 memorandum nor the DOGE Executive Order to which the memorandum refers explains why DOGE affiliates need to know the information in Education’s records to perform their jobs.

Nothing else in the administrative record explains why either. At the preliminary injunction hearing, the government suggested the job descriptions of DOGE affiliates at Education explain why they have a need for the Privacy Act-protected records. But a review of the job descriptions in the record reveals they provide no such explanation.

A document titled “Terms and Conditions for Reimbursable Work” describes the “scope of work” for the USDS employees detailed to Education as follows:

Providing software engineering, modern architecture and system design, project and team leadership, software delivery, security and site reliability engineering, data engineering, engineering management, and/or executive leadership expertise to champion and deliver modern technology[;] Performing a wide range of activities including debugging, software testing, and programming. USDS employees will quickly adapt and learn by problem-solving within legacy systems and organizational constraints while working collaboratively for rapid prototyping[;] . . . assess[ing] the state of current projects in agencies and plans and/or leads interventions where major corrections are required[;] Assisting on IT projects including infrastructure, implementing safeguards to prevent fraud, and ensuring the integrity and success of these efforts[;] Championing data strategies and building interoperability across other agencies as well as internal and external stakeholders.

See ED-000001. According to this document, USDS detailees at Education have job duties that cover a wide range of IT services, such as software engineering and programming, establishing protections to prevent fraud, and building interoperability. Other documentation in the record indicates that some Education DOGE affiliates perform research duties. ED-1 “conduct[s] research

to support EOP Department of Government Efficiency efforts.” ED-000005. ED-3 is a software engineer detailed from GSA “conducting research and analysis to identify inefficiencies and areas for improvement in ED’s administrative and programmatic functions.” ED-000013. ED-3 is also responsible for “reviewing internal processes and operational procedures to identify areas for improvement.” *Id.* Another DOGE affiliate, ED-4, is apparently tasked with duties that will lead to “[l]ess dollars . . . flow[ing]” from Education “to many non-profit and for profit institutions and companies.” ED-000018. And there is a broader goal stated in several descriptions of DOGE affiliates’ duties: “improvement of government efficiency.” *See, e.g.*, ED-000003. None of these myriad job duties explain why the person performing them has a need for records with PII contained within Education’s systems.

Apparently aware that the administrative record does not answer the need-to-know question, the government attempts to fill this gap after the fact with its own answers. The government asserts that “[a]ll six [DOGE affiliates] work to audit contract, grant and related programs for waste, fraud and abuse” and that they need access to records “in order to audit student loan programs for waste, fraud, and abuse.” ECF 62, at 7, 27. This rationale appears to be created out of whole cloth. The DOGE Executive Order does not mention waste, fraud, and abuse, and it certainly does not mention auditing student loan programs. And the parts of the administrative record cited by the government for the proposition that DOGE affiliates were hired to audit Education programs do not describe any auditing tasks. *See id.* at 7 (citing ED-000001–19, ED-000021).

While the record does state that some DOGE affiliates are tasked with “improv[ing] government efficiency,” *see, e.g.*, ED-000003, a vague reference to government efficiency cannot reasonably be interpreted to include auditing federal student loan programs for waste, fraud, and

abuse. It is more reasonable to interpret this “efficiency” goal in light of the DOGE Executive Order, which established DOGE for the purpose of “implement[ing] the President’s DOGE Agenda, *by modernizing Federal technology and software to maximize governmental efficiency and productivity*,” DOGE Executive Order, § 1 (emphasis added). Other descriptions of DOGE affiliates’ job duties refer to similarly ill-defined “efficiency” roles. Consider ED-3. Recall that this DOGE affiliate is tasked with “conducting research and analysis to identify inefficiencies and areas for improvement in ED’s administrative and programmatic functions and reviewing internal processes and operational procedures to identify areas for improvement.” ED-000013. But ED-3 is a software engineer detailed from GSA. *See id.* It is unclear how a software engineer’s “research and analysis” to “identify inefficiencies and areas for improvement” in either the programmatic or administrative functions of the agency would encompass an audit of federal student loan programs. Or consider ED-4—an unpaid consultant with “[s]ignificant experience in education [and] technology” tasked with “[a]dvising the Department on change management” and “[p]erforming cost reductions.” ED-000018. ED-4’s duties will purportedly lead to “[l]ess dollars . . . flow[ing] from [the] Department of ED to many non-profit and for profit institutions and companies.” *See* ED-000018. It is not at all evident from these nebulous descriptions of ED-4’s job duties that they are auditing federal student loan programs.

The administrative record does not support the government’s assertion that Education granted full access to its systems of records to DOGE affiliates because they need to audit federal student loan programs. *See Boyd v. Snow*, 335 F. Supp. 2d 28, 38 (D.D.C. 2004) (denying the government’s argument that disclosure fell under the need-to-know exception because “[i]t [wa]s

far from clear” from the record that the government employee disclosed Privacy Act-protected information “for the reason offered by the IRS”).²³

The administrative record does not explain why the DOGE affiliates at Education need access to all of Education’s unclassified systems and data—which include the plaintiffs’ PII—in the performance of their job duties. On the contrary, the record suggests that Education likely shared this protected information with DOGE affiliates who had no need to know the vast amount of sensitive personal information to which they were granted access.

b. OPM

OPM granted DOGE affiliates access to several OPM systems of record that contain the plaintiffs’ PII. Those systems of record include eOPF, EHRI, USA Staffing, and USA Performance, among others. *See* OPM-000028–29, OPM-000103, OPM-000104–10; ECF 14-3, ¶¶ 7–8; ECF 14-7, ¶¶ 7–8; ECF 14-9, ¶¶ 6–7; ECF 14-10, ¶¶ 10–11; ECF 14-11, ¶¶ 5–6; ECF 14-12, ¶¶ 8–9. The PII in these systems includes Social Security numbers, names and addresses, dates of birth, citizenship statuses, salaries, criminal history information, and personnel actions such as

²³ The government also cites to declarations from one of the DOGE affiliates at Education who says they need “access to Department of Education information technology and data systems related to student loan programs in order to audit those programs for waste, fraud, and abuse.” *See* ECF 27-5, ¶ 9; ECF 62, at 27. Yet at the same time, the government asserts that the Court need not look outside the administrative records because the records “contain the extant materials that informed or reflect each agency’s decisionmaking as to systems access for DOGE affiliates, and those materials provide sufficient information for the Court to evaluate Defendants’ decisions.” ECF 54, at 7. Indeed, the “court may look only to the[] *contemporaneous* justifications in reviewing the agency action.” *Dow AgroSciences*, 707 F.3d at 467–68 (citing *Chenery*, 318 U.S. at 87–88); *see also Environ. Def. Fund.*, 657 F.2d at 285 (noting that while “[w]hen the record is inadequate, a court may ‘obtain from the agency, either through affidavits or testimony, such additional explanations of the reasons for the agency decision as may prove necessary,’” but this “new materials should be merely explanatory of the original record and *should contain no new rationalizations*” (emphasis added) (quoting *Camp*, 411 U.S. at 143)). So, as the government concedes, the Court may not consider extra-record evidence as justification for the agency’s actions.

promotions and suspensions. *See, e.g.,* OPM, *Privacy Impact Assessment for Electronic Official Personnel Folder System (eOPF)* 5 (2020); OPM, *Privacy Impact Assessment for USA Staffing*® 6 (2021); OPM, *Privacy Impact Assessment for Enterprise Human Resources Integration Data Warehouse (EHRI DW)* 3; OPM, *Privacy Impact Assessment for USA Performance (USAP)* 4.

As with Education, nothing in the administrative record explains why DOGE affiliates at OPM need to know the PII in OPM’s systems of records in the performance of their job duties. The OPM record includes several internal emails from late January that document the agency’s decision to grant DOGE affiliates access to the OPM systems of records, but none of the emails explains the DOGE affiliates’ need to access the records contained within these systems. In a January 27, 2025 email with the subject line “Getting DoGE Engineers access,” Acting OPM Director Ezell instructed an OPM employee to grant access to OPM computer systems to “some engineers”—several DOGE affiliates at OPM. *See* OPM-000028–29. As Ezell explained, “We are rapidly ramping up” these engineers, and “[t]o accomplish this goal,” the DOGE affiliates needed “a short list of all the systems OPM operates and manages” and, “for each computer system,” a list of permissions and access. *See id.* This included access to the back end of these systems, such as code read and write permissions; the ability to access the system as a “regular user,” like a hiring manager who accesses USA Staffing; and “admin user” access. OPM-000029. Another email with the subject line “urgent request from political tech staff” indicates that OPM “ha[d] already given several of the political devs/engineers comprehensive access to USAJOBS and USA Staffing” and that, pursuant to Ezell’s request, “[OPM-2, OPM-4, and OPM-6 have] the same requirement.” OPM-000108–09. The email describes granting access to USAJOBS, USA Staffing, eOPF, EHRI, and USA Performance. OPM-000108. A January 30 email reveals that DOGE affiliates OPM-3, OPM-5, and OPM-7—described as “Individuals from the Political Team”—gained access to OPM

systems as “admins” with “super user permissions for the USAJOBS admin systems” based on a January 20 Ezell directive. *See* OPM-000104, OPM-000107. Between January 24 and February 7, other DOGE affiliates at OPM gained access to various OPM systems with PII, including USA Performance, the Federal Employee Health Benefits system, and the Postal Service Health Benefits Data Platform. OPM-000103.

These emails do not explain *why* the DOGE affiliates at OPM must know the PII contained in OPM’s systems to perform their job duties. In fact, the emails suggest some of them do not have a need to know. Ezell granted sweeping access to OPM systems to DOGE affiliates who are engineers even though “[they] [did not] have immediate plans to change anything” and OPM did not “have any immediate plans for new engineers to make direct changes to any of these systems.” OPM-000028–29. Ezell apparently granted DOGE affiliates broad access to OPM’s systems to be prepared if OPM “need[ed] to move quickly” at some point to make system changes. OPM-000029. Then, after Ezell authorized this access, the CIO of OPM rolled it back. The CIO said that the DOGE affiliates who were granted access pursuant to Ezell’s January 27 email “have never needed access to E[HR]/eOPF.” *See* OPM-000026–29.

These emails all but confirm that OPM disclosed records with the plaintiffs’ PII to DOGE affiliates who did not have a need to know the information. Ezell granted extensive access to OPM systems even though the DOGE affiliates “[did not] have immediate plans to change anything.” And Hogan later confirmed that these DOGE affiliates never needed access to some of these systems after all. This shoot first, ask questions later method of disclosing Privacy Act-protected records undermines the government’s position that the disclosures were made on a need-to-know basis.

Nothing else in the OPM administrative record answers the need-to-know question. The record does not contain any substantive job descriptions, scope of work details, or other information about the DOGE affiliates' responsibilities at OPM. All that can be ascertained from the emails are that many of these individuals are engineers, developers, or "tech staff." *See* OPM-000028–29, OPM-000107–09. The employment forms in the record provide only meager clues as to their roles at OPM. OPM-2, OPM-3, OPM-6, and OPM-7 are "Expert[s]" who will "provide a high level of expertise relative to issues which have a significant impact on the formulation of agency goals and objectives to the OPM director." OPM-000008, OPM-000011, OPM-000022, OPM-000111. OPM-2 is also listed as a "Senior Advisor" with no corresponding job duties. OPM-000006. OPM-4 is another "Expert," though no additional details about their role are provided. *See* OPM-000014. OPM-5 is a "Senior Advisor to the Director for Information Technology," and OPM-8 is a "Senior Advisor to the Director." OPM-000017, OPM-000115. The record contains no information about their job duties. And there is no information about the positions or job duties of other DOGE affiliates who gained access to OPM systems of records—let alone why those positions or duties required access to records containing PII.

With nothing in the administrative record to justify OPM's disclosure, the government argues the DOGE affiliates need access to OPM systems of records because of the DOGE Executive Order's directive to modernize technology. Once again, the government does not cite any record evidence that explains *why* a directive to modernize technology requires access to the extensive PII housed within OPM's systems. And what little record evidence there is indicates that certain DOGE affiliates at OPM did not actually need the broad access to that Ezell initially authorized. OPM-000026.

The government also suggests that DOGE affiliates need access to these records to implement “workplace reform.” *See* ECF 62, at 27. Ostensibly, this refers to the Executive Order “Implementing the President’s ‘Department of Government Efficiency’ Workforce Optimization Initiative,” issued on February 11, 2025. Exec. Order No. 14,210, 90 Fed. Reg. 9669 (Feb. 14, 2025) (“Workforce Executive Order”).²⁴ Nothing in the record remotely suggests the DOGE affiliates gained access to OPM systems of record to implement the Workforce Executive Order. That is likely because the Workforce Executive Order was issued *after* all OPM DOGE affiliates were granted access to these systems. *See* OPM-000103. So even if OPM could rely on post-hoc rationalizations to explain the reason for its disclosure of Privacy Act-protected records to DOGE affiliates, the explanation makes no sense.

Upon a review of the administrative record, the Court finds that OPM likely disclosed records with the plaintiffs’ PII to DOGE affiliates who did not have a need to know the information in the performance of their duties.

c. Treasury

Treasury granted two DOGE affiliates access to several payment systems, including the SPS, PAM, and ASAP. *See* TR-0062; TR-0058. These systems contain payment records with PII such as Social Security numbers, names, addresses, and bank information. *See, e.g.*, Fiscal Service, *Privacy and Civil Liberties Impact Assessment: Payment Automation Manager* 5; Fiscal Service, *Privacy and Civil Liberties Impact Assessment Secure Payment System (SPS)* 7; Fiscal Service, *Privacy and Civil Liberties Impact Assessment: Automated Standard Application for Payments*

²⁴ The Workforce Executive Order “commences a critical transformation of the Federal bureaucracy.” Workforce Executive Order § 1. It proclaims that the Trump “Administration will empower American families, workers, taxpayers, and our system of Government itself” by “eliminating waste, bloat, and insularity.” *Id.*

(*ASAP*) 6–7. Treasury also provided “over the shoulder” access to watch Fiscal Service employees process payments. *See* TR-0059 (“USDS/DOGE requested to be granted ‘over the shoulder’ access to monitor Fiscal Service personnel conducting payment processing roles, which was approved by Fiscal Service on 1/23/25”). By granting Treasury DOGE affiliates access to these payment systems, Treasury has given them access to records with the plaintiffs’ PII. *See* ECF 14-3, ¶¶ 7–8; ECF 14-4, ¶¶ 5–6; ECF 14-5, ¶¶ 6–7; ECF 14-6, ¶¶ 5–6; ECF 14-7, ¶¶ 7–8; ECF 14-8, ¶¶ 6–7; ECF 14-9, ¶¶ 6–7; ECF 14-10, ¶¶ 10–11; ECF 14-11, ¶¶ 5–6; ECF 14-12, ¶¶ 8–9.

The administrative record reveals that the DOGE affiliates at Treasury were granted access to the payment systems to modernize technology at the agency. What the record does not reveal is *why* the DOGE affiliates need access to the PII within those payment systems to modernize technology.

One of the two DOGE affiliates at Treasury is Thomas Krause. Krause is a Senior Advisor for Technology and Modernization (“Senior Advisor”). TR-0007, TR-0015, TR-0024.²⁵ In his role as a Senior Advisor, Krause’s job duties center on technology modernization and innovation. His duties are manifold. He was hired to provide services such as “advancing the Treasury’s technology infrastructure, financial management systems, and cybersecurity initiatives”; “lead[ing] IT modernization efforts”; “oversee[ing] modernization of legacy systems”;

²⁵ In addition to being a Senior Advisor for Technology and Modernization, Krause also has been delegated the duties of the Fiscal Assistant Secretary. Those duties do not shed any light on why Krause might need to know PII within Treasury’s payment systems because he was granted “over the shoulder” access to Treasury payment systems *before* he assumed the duties of Fiscal Assistant Secretary. *See* TR-0003 (delegation of Fiscal Assistant Secretary duties dated February 5, 2025); TR-0024 (appointment affidavit showing Krause’s date of appointment as a Senior Advisor as January 23, 2025); TR-0056–59 (engagement plan describing how the “USDS/DOGE team” got “over the shoulder” access to “monitor Fiscal Service personnel conducting payment processing” on January 23, 2025). So, any duties Krause might have assumed *after* he was granted access to Treasury payment systems cannot justify the disclosure.

“integrating real-time analytics, automation, and enhanced data-sharing capabilities across agencies”; “strengthen[ing] cybersecurity protocols to protect critical financial systems and mitigate risks”; and “foster[ing] public-private partnerships . . . to drive innovation.” TR-0007, TR-0015. He is expected to “provide critical recommendations that shape government technology and financial management strategies” and to develop “policy guidance, modernization efforts, and strategic partnerships.” *Id.* He will work with various Treasury officials “to lead . . . the development, execution, and management of the information technology and technological modernization efforts” and “programs for the Department of the Treasury and the internal management of the Department and its bureaus . . . as it relates to technology.” TR-0013, TR-0021.

As plentiful as the descriptions of Krause’s job duties are, they do not suggest Krause needs to know the PII in Treasury’s payment records to perform any of his duties. Krause was hired to modernize Treasury’s technology systems, improve cybersecurity, advise on financial management strategy, and take the lead on Treasury “information technology and technological modernization efforts and programs” and “internal management of [Treasury]. . . *as it relates to technology.*” *See, e.g.*, TR-0021 (emphasis added). To perform these duties, Krause does not appear to require access to payees’ Social Security numbers, names, addresses, or bank information. And both the record and a privacy and civil liberties impact assessment indicate that some of this personal information can be redacted. *See* TR-0063 (email describing “unredacted” files in PAM and SPS systems); *Privacy and Civil Liberties Impact Assessment Secure Payment System (SPS)* 7 (“Treasury is committed to eliminating unnecessary collection, use, and display of full Social Security numbers (‘SSN’) and redacting, truncating, and anonymizing SSNs in systems and

documents to limit their accessibility to individuals who do not have a need to access the full SSN in order to perform their official duties.”).

The other DOGE affiliate at Treasury is Ryan Wunderly, who was hired to fill Marko Elez’s role of Special Advisor for Information Technology and Modernization (“Special Advisor”). The Special Advisor was granted access to several Treasury systems containing PII as early as February 1, 2025. *See* TR-0062. Like Krause, Wunderly’s role centers on technology modernization. The Special Advisor’s “primary purpose” is “to serve in a close and confidential capacity to the Chief of Staff’s Senior Advisor for Information Technology and Modernization” (*i.e.*, Krause). TR-0022. Like Krause, Wunderly’s job description is lengthy. He “is responsible for advising [Krause] on engineering, software, hardware, systems, and other technology matters.” *Id.* His responsibilities are to “[c]onduct[] special and confidential studies on a variety of strategies and issues related to Treasury’s information technology”; “[r]eview[] and furnish[] [Krause] with recommendations regarding Treasury’s critical software infrastructure”; “[i]dentif[y], analyze[], and make[] recommendations to strengthen Treasury’s hardware and software”; “work closely with the engineers in [the Fiscal Service] on Information Technology matters to execute Fiscal’s mission of promoting the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services”; and “assist on key issues for Fiscal, 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.” TR-0022–23. The engagement plan describes how “USDS/DOGE confirmed” that the Special Advisor (the “designated technical team member”) “requires access to Fiscal Service systems and data” and “will be provided access to in scope payment systems source code.” TR-0058.

Like the job descriptions of the Senior Advisor, the descriptions of the Special Advisor's job do not reveal why Wunderly needs access to the PII within Treasury's payment records. His role is focused on "engineering, software, hardware, systems, and other technology matters." TR-0022. His job responsibilities center on technology. He recommends, assists, and collaborates on "Treasury's critical software infrastructure"; "Treasury's hardware and software"; and "Information Technology matters." TR-0023. Nothing in his job description—and nothing in the administrative record as a whole—suggests he requires access to the PII in Treasury's payment records.

The record indicates that the Special Advisor "will not be able to adequately perform his/her duties without being privy to the critical information technology hardware and software infrastructure of Treasury Department," "will be exposed to conversations, dialogues, and other kinds of sensitive information," and will "perform[] a variety of confidential assignments requiring analysis and evaluation of programs and activities of importance to [Krause]." TR-0022. But nothing in the records suggests this "sensitive information" includes PII or that "confidential assignments" require access to PII.

Finally, the engagement plan describes how DOGE affiliates will "outlin[e] recommendations for greater efficiencies and potential improvements to the existing payment processes and associated technology and policies in support of payment integrity and fraud prevention." TR-0057. This task, when viewed in the context of the entire engagement plan and the DOGE affiliates' job duties, is part of the efforts to improve Treasury's technology. *See id.* It is not a directive to look at the PII within payment records to ferret out fraud.²⁶

²⁶ The administrative record contains a "Preliminary Work Plan for IT Access" that describes the need for "[s]ystem access as well as on-going discussions with subject matter experts" to "understand[] and verify[] how [Treasury] payment and accounting systems work." TR-0060. The

With nothing in the administrative record to support the DOGE affiliates' need to know, the government argues that they need access to Treasury payment systems to implement the DOGE Executive Order. But once again, the government does not explain why implementing the DOGE Executive Order—which focuses on technology modernization—requires access to PII within Treasury payment records.

The administrative record does not show that DOGE affiliates at Treasury need access to the PII in the payment record systems to modernize technology at the agency.

* * *

The administrative records indicate that Education, OPM, and Treasury disclosed records with the plaintiffs' PII to DOGE affiliates. They also indicate that the DOGE affiliates do not need to know this information to perform their job duties. And on the record before the Court, no other Privacy Act exception applies to these disclosures.²⁷ Education, OPM, and Treasury likely violated the Privacy Act. In so doing, the agencies likely violated the APA by acting “not in accordance

document is not dated and its author is not identified. Regardless, it does not show that the author—or whichever DOGE affiliate is implicated by the document—needs access to PII to “understand[] and verify[]” how the systems work. *Id.*

²⁷ The government points to a provision of the Privacy Act that permits disclosure “for a routine use,” defined as “the use of such record for a purpose which is compatible with the purpose for which it was collected.” 5 U.S.C. § 552a(a)(7), (b)(3); *see* ECF 62, at 27–28. When an agency discloses records under the “routine use” exception, it must retain an account of “the date, nature, and purpose of each disclosure of a record to any person or to another agency” and the “name and address of the person or agency to whom the disclosure is made.” *See* 5 U.S.C. § 552a(c)(1). The government has not produced such an accounting. The OPM account creation audit does not show the purpose of the disclosure to the DOGE affiliates. *See* OPM-000089–103. Nor does the BFS System Access Request in the administrative record for Treasury. *See* TR-0062. There is no account of the access given to DOGE affiliates at Education. And there is nothing else in the administrative records that resembles a documentation of use or access. The gap in the records cannot be backfilled by the Statement of Record Notices from the Federal Register in the OPM and Treasury records. The government’s invocation of the routine use exception appears to be an after-the-fact attempt to fit the disclosures into an exception.

with law.” *See* 5 U.S.C. § 706(2)(A); *Doe v. Chao* (“*Chao II*”), 435 F.3d 492, 504 n.17 (4th Cir. 2006); *accord Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988) (noting case involving unauthorized disclosure claims under the Veterans’ Records Statute, which incorporates the Privacy Act, “clearly is a case of agency action ‘not in accordance with law’” (quoting 5 U.S.C. § 706(2))). The plaintiffs have established a likelihood of success on the merits of their APA claim that Education, OPM, and Treasury acted “not in accordance with law.”²⁸ *See* 5 U.S.C. § 706(2)(A).

2. Irreparable Harm

“To establish irreparable harm, the movant must make a ‘clear showing’ that it will suffer harm that is ‘neither remote nor speculative, but actual and imminent’” and that the harm “‘cannot be fully rectified by the final judgment after trial.’” *Mountain Valley Pipeline, LLC v. 6.56 Acres of Land*, 915 F.3d 197, 216 (4th Cir. 2019) (first quoting *Direx Isr., Ltd. v. Breakthrough Med. Corp.*, 952 F.2d 802, 812 (4th Cir. 1991); and then quoting *Stuller, Inc. v. Steak N Shake Enters., Inc.*, 695 F.3d 676, 680 (7th Cir. 2012)).

The plaintiffs have made a clear showing that they are likely to suffer actual and imminent harm without injunctive relief. Allegations that personal information is “currently” being “obtain[ed]” or will be obtained “imminently, unless they receive injunctive relief” are sufficient to show “an ongoing or imminent injury.” *See Garey*, 35 F.4th at 923. Through their allegations and the record evidence, the plaintiffs have shown that DOGE affiliates have been granted access to systems of records that contain some of the plaintiffs’ most sensitive data—such as Social

²⁸ The plaintiffs have raised two other APA claims against the government: that the agencies acted arbitrarily and capriciously and in excess of their statutory authority. Because the Court finds that the plaintiffs have shown a likelihood of success on the merits of one APA claim, it need not consider the plaintiffs’ likelihood of success on the other APA claims.

Security numbers, dates of birth, home addresses, bank information, income and assets, and citizenship status—and that, without an injunction, the DOGE affiliates’ access to this trove of personal information will continue. In fact, the government takes the position that the DOGE affiliates’ access to records containing the plaintiffs’ PII is not only lawful, but it is *necessary* for them to do their jobs. *See* ECF 62, at 27 (asserting the “relevant personnel . . . have a need to access Privacy Act-protected records”). If the agencies’ disclosures are not enjoined, the DOGE affiliates—whose mission to implement the DOGE Executive Order is ongoing—will access records with the plaintiffs’ personal information.²⁹ The plaintiffs have made a clear showing that they will suffer actual and imminent harm if the Court does not order injunctive relief.

They also have made a clear showing that their harm is irreparable. The Fourth Circuit has not decided whether the continuing unlawful disclosure of sensitive personal information is irreparable harm. Other courts presented with similar questions have. Many have found that ongoing unauthorized disclosure, and even the mere unauthorized retention, of sensitive personal

²⁹ The OPM administrative record shows that some DOGE affiliates at OPM had their access to two systems of record—eOPF and EHRI—revoked prior to the Court’s issuance of a TRO. *See* OPM-000023–27. However, the administrative record also shows that many OPM DOGE affiliates still have access to other OPM systems of records that house records with the plaintiffs’ PII. *See* OPM-000103. And a declaration submitted by the government suggests that some DOGE affiliates still have access to eOPF and may re-gain access to EHRI in the future. *See* ECF 33-1, ¶¶ 12–14. Thus, the partial and apparently temporary revocation of access to certain OPM systems of records does not render the harm any less actual or imminent. The same goes for Education. Matteson, an Executive Project Manager, says that only one of the DOGE affiliates’ user accounts had access to one of the four Education systems of records identified in the plaintiffs’ complaint and that this access was “substantially limited” as he “could not access any personally identifiable information.” *See* ECF 62-1, ¶ 4. However, the Court cannot ignore the February 5 memorandum from Education’s CIO that granted DOGE affiliates at Education “full and prompt access to all unclassified IT systems and data,” ED-000025; Ramada’s declaration that “[t]he relevant employees require access to Department of Education information technology and data systems related to student loan programs in order to audit those programs for waste, fraud, and abuse,” ECF 27-5, ¶ 9, or the government’s assertion that the DOGE affiliates at Education “need to access to [Privacy Act-protected] records in order to audit student loan programs for waste, fraud, and abuse,” ECF 62, at 27—all of which suggest that the harm to the plaintiffs is ongoing.

information is irreparable harm that money damage cannot remedy. *See, e.g., Norman-Bloodsaw v. Lawrence Berkeley Lab’y*, 135 F.3d 1260, 1275 (9th Cir. 1998) (finding “the retention of [the plaintiffs’] undisputedly intimate medical information [without consent] . . . would constitute a continuing ‘irreparable injury’ for purposes of equitable relief”); *Roberts v. Austin*, 632 F.2d 1202, 1214 (5th Cir. 1980) (finding irreparable harm from state agency’s unauthorized release of food stamp recipients’ files to state’s attorney because “the [Food Stamp] Act and accompanying regulations give recipients statutory protection from disclosure of confidential information” and “recipients possess a legitimate expectation that the information will be kept confidential”); *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 802 (N.D. Cal. 2022) (“The invasion of privacy triggered by the Pixel’s allegedly ongoing disclosure of plaintiffs’ medical information is precisely the kind of intangible injury that cannot be remedied by damages.”); *Haw. Psychiatric Soc. v. Ariyoshi*, 481 F. Supp. 1028, 1052 (D. Haw. 1979) (finding irreparable injury because “[t]he disclosure of the highly personal information contained in a psychiatrist’s files to government personnel is itself a harm that is both substantial and irreversible”); *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 499 (S.D.N.Y. 2019) (“The disclosure of private, confidential information ‘is the quintessential type of irreparable harm that cannot be compensated or undone by money damages.’” (quoting *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000))).

In *Trump v. Deutsche Bank AG*, 943 F.3d 627, 637 (2d Cir. 2019), *vacated and remanded on other grounds sub nom. Trump v. Mazars USA, LLP*, 591 U.S. 848 (2020), the Second Circuit affirmed a holding that President Trump would suffer irreparable harm if his personal financial information were disclosed to two congressional committees. Although the district court denied the preliminary injunction because President Trump had not shown a likelihood of success on the merits, the court concluded he had shown an irreparable injury if his financial information were

disclosed. *See Trump v. Deutsche Bank AG*, No. 19 Civ. 3826 (ER), 2019 WL 2204898, at *1 (S.D.N.Y. May 22, 2019); Joint Appendix at 149, *Deutsche Bank AG*, 943 F.3d 627 (No. 19-1540). The district court reasoned that the “plaintiffs have an interest in keeping their records private from everyone, including congresspersons, and that interest necessarily will be impinged by the records’ disclosure to the committees.” *See* Joint Appendix at 125–26, *Deutsche Bank AG*, 943 F.3d 627 (No. 19-1540). It acknowledged that “some courts outside of this circuit have questioned whether the mere disclosure of information, absent evidence of misuse or unauthorized disclosure by the receiving party automatically constitutes irreparable injury.” *See id.* at 124–25 (citing *Baker DC, LLC v. NLRB*, 102 F. Supp. 3d 194 (D.D.C. 2015)). The court did not find those cases persuasive. Instead, the court concluded, “that plaintiffs possess strong privacy interests in their financial information such that unwanted disclosure may properly constitute irreparable injury, without an additional showing of likelihood of misuse or unauthorized disclosure by the recipient.” *Id.* at 125.³⁰

³⁰ The court referred to a case from the U.S. District Court for the District of Columbia. In that jurisdiction, the mere disclosure of personal information, without more, is not automatically irreparable harm if it is expected that the recipient will keep the information confidential. In *Ashland Oil, Inc. v. FTC*, a district court held that disclosure of a company’s trade secrets to a congressional committee would not cause irreparable injury because they did not show that their trade secret information would be disclosed to competitors or to the public. 409 F. Supp. 297, 308 (D.D.C. 1976), *aff’d*, 548 F.2d 977 (D.C. Cir. 1976) (per curiam). The court “presume[ed] that the committees of Congress w[ould] exercise their powers responsibly and with due regard for the rights of affected parties.” *Id.* The D.C. Circuit affirmed. 548 F.2d at 982. Similarly, in *Baker DC, LLC v. NLRB*, a district court concluded that no irreparable harm resulted from an agency rule compelling an employer to divulge its employees’ “names, job locations, phone numbers, and email addresses” to a union. 102 F. Supp. 3d 194, 203 (D.D.C. 2015). The court reasoned that the rule “place[d] explicit limits on the purposes for which employee information can be used.” *Id.* And it concluded that any risk that the union would misuse the employees’ private information or disclose it to outside individuals was speculative. *Id.* Relying on *Ashland Oil* and *Baker DC*, two judges in the District of Columbia have denied preliminary injunctive relief in similar cases against Treasury and Education because the plaintiffs did not establish irreparable harm. *See Univ. of Cal. Student Ass’n*, Civ. No. 25-354 (RDM), 2025 WL 542586, at *5 (D.D.C. Feb. 17, 2025); *All. for Retired Ams. v. Bessent*, Civ. No. 25-0313 (CKK), 2025 WL 740401, at *21 n.7 (D.D.C. Mar. 7,

In line with courts in the Second, Fifth, and Ninth Circuits, this Court finds that the ongoing disclosure of the plaintiffs' PII to government employees not authorized to access it constitutes irreparable harm. The plaintiffs have a strong interest in keeping their PII private, they have not consented to its disclosure to DOGE affiliates, and they have shown it is likely that the DOGE affiliates will continue to have and use access to records with their sensitive personal information absent an injunction. This ongoing violation of the plaintiffs' privacy interests cannot be redressed by a final judgment of money damages or by permanent injunctive relief.

Without a preliminary injunction, the DOGE affiliates' access to the plaintiffs' private information will continue. This invasion of the plaintiffs' privacy and the intrusion upon their seclusion is neither speculative nor remote; it is actual and imminent. A final judgment of money damages or a permanent injunction will not make them whole. The plaintiffs have made a clear showing that they will experience irreparable harm without an injunction.

3. Balance of Equities and Public Interest

The balance of the equities and the public interest "merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009). To balance the equities, the Court considers "the relative harms to the [plaintiffs] and [defendants], as well as the interests of the public at large." *Barnes v. E-Sys., Inc. Grp. Hosp. Med. & Surgical Ins. Plan*, 501 U.S. 1301, 1305 (1991) (Scalia, J., in chambers) (quoting *Rostker v. Goldberg*, 448 U.S. 1306, 1308 (1980) (Brennan, J., in chambers)). These factors weigh in favor of a preliminary injunction.

The plaintiffs have shown that Education, OPM, and Treasury likely violated the APA by granting DOGE affiliates sweeping access to their sensitive personal information in defiance of

2025). *Ashland Oil* and *Baker DC* are not binding on this Court, and the Court does not find them persuasive.

the Privacy Act. “There is generally no public interest in the perpetuation of unlawful agency action.” *League of Women Voters v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016). Although the Court should not “collapse[] the first *Winter* factor—likelihood of success on the merits—with the merged balance of equities and public interest factor,” *USA Farm Lab., Inc. v. Micone*, No. 23-2108, 2025 WL 586339, at *4 (4th Cir. Feb. 24, 2025), the factors overlap here. The likely unlawful agency action concerns the privacy rights of individuals who had to give their sensitive personal information to the federal government to obtain federal benefits, student loans, or employment. They trusted the federal government to safeguard their information. That public trust likely has been breached. Preventing the government’s unauthorized disclosure of the plaintiffs’ sensitive personal information is in the public interest. *See CACI, Inc. – Fed. v. U.S. Navy*, 674 F. Supp. 3d 257, 279 (E.D. Va. 2023) (“There is a strong public interest in curing the effects of the government’s unlawful acts.”).

The government argues that preliminary injunctive relief would harm the public interest because it would “limit[] the President’s ability to effectuate the policy choices the American people elected him to pursue by limiting his advisors and other employees’ ability to access information necessary to inform that policy.” ECF 62, at 32. A preliminary injunction in this case does not prevent the President from effectuating the administration’s policies. It prevents the likely unlawful disclosure of the plaintiffs’ sensitive personal information to DOGE affiliates who, on the record before the Court, do not have a need to know the information to perform their duties.

The balance of the equities and the public interest favor preliminary injunctive relief.

The plaintiffs have established that they are entitled to a preliminary injunction.

D. Scope of the Injunction

“[I]njunctive relief should be designed to grant the full relief needed to remedy the injury to the prevailing party,” but “it should not go beyond the extent of the established violation.” *Hayes v. N. State Law Enforcement Officers Ass’n*, 10 F.3d 207, 217 (4th Cir. 1993). “Whenever the extraordinary writ of injunction is granted, it should be tailored to restrain no more than what is reasonably required to accomplish its ends.” *S.C. Dep’t of Wildlife & Marine Res. v. Marsh*, 866 F.2d 97, 100 (4th Cir. 1989) (quoting *Consol. Coal Co. v. Disabled Miners*, 442 F.2d 1261, 1267 (4th Cir. 1971)).

Here, the injury is the unauthorized disclosure of the plaintiffs’ PII to DOGE affiliates at Education, OPM, and Treasury. To prevent the injury pending the outcome of this case, the Court will limit the preliminary injunctive relief to the disclosure of the PII of the individual plaintiffs and the organizational plaintiffs’ members.

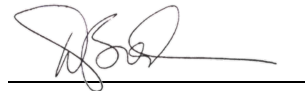
III. Conclusion

On the first day of his second term in office, President Trump signed an Executive Order directing agencies to “take all necessary steps . . . to the maximum extent consistent with law, to ensure” people implementing his DOGE agenda have “full and prompt access to all unclassified agency records, software systems, and IT systems.” DOGE Executive Order § 4(b). Following this directive, Education, OPM, and Treasury granted expansive access to their systems of record—which house the plaintiffs’ PII—to individuals charged with implementing the President’s DOGE Executive Order. In doing so, the agencies likely violated the Privacy Act and the APA.

Enacted 50 years ago, the Privacy Act protects from unauthorized disclosure the massive amounts of personal information that the federal government collects from large swaths of the public. Congress’s concern back then was that “every detail of our personal lives can be assembled

instantly for use by a single bureaucrat or institution” and that “a bureaucrat in Washington or Chicago or Los Angeles can use his organization’s computer facilities to assemble a complete dossier of all known information about an individual.” See Danielle Keats Citron, *A More Perfect Privacy*, 104 B.U. L. Rev. 1073, 1078 (2024) (first quoting 120 Cong. Rec. 36,917 (1974) (statement of Sen. Goldwater); and then quoting 120 Cong. Rec. 36,917 (statement of Sen. Percy)). Those concerns are just as salient today. No matter how important or urgent the President’s DOGE agenda may be, federal agencies must execute it in accordance with the law. That likely did not happen in this case. The plaintiffs’ motion for a preliminary injunction is granted. A separate order follows.

Date: March 24, 2025

A handwritten signature in black ink, appearing to read 'DLB', is written over a horizontal line.

Deborah L. Boardman
United States District Judge