UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

ELECTRONIC PRIVACY INFORMATION CENTER, et al., Plaintiffs, v. U.S. OFFICE OF PERSONNEL MANAGEMENT, et al., Defendants.	Civil No. 1:25-cv-255-RDA-WBP

DEFENDANTS' MEMORANDUM IN OPPOSITION TO PLAINTIFFS' MOTION FOR A TEMPORARY RESTRAINING ORDER

Defendants U.S. Office of Personnel Management ("OPM"); Charles Ezell, in his official capacity as Acting Director of OPM; U.S. Department of the Treasury ("Treasury"); Scott Bessent, in his official capacity as Secretary of the Treasury; the U.S. Digital Service, redesignated as the U.S. Department of Government Efficiency Service, or U.S. DOGE Service ("USDS"); the Acting U.S. Digital Service Administrator; and the U.S. DOGE Service Temporary Organization, pursuant to the Court's February 14, 2025 Order (ECF No. 11) submit this Memorandum in Opposition to Plaintiffs' Motion for Temporary Restraining Order[1] (ECF No. 5).

INTRODUCTION

This is one of a spate of similar lawsuits seeking unprecedented judicial micromanagement of the Executive Branch's ability to share government data with its own employees in exercising politically accountable oversight of agency activities. Relying on unverified press reports, Plaintiffs spin a tale of anonymous "DOGE staff" "swooping in" and "demanding access to sensitive government systems." Pls.' Mem. (ECF No. 7) at 8. Among the agencies allegedly targeted are Treasury and OPM, where, Plaintiffs allege, there are data systems containing their personal identifying information. Plaintiffs claim that their information has been compromised in violation of federal statutes and the Constitution.

The true story is far less sensational. In response to lawful Executive Orders issued by President Trump, Treasury and OPM have assembled small teams of the agencies' own employees, including detailees, to oversee implementation of the new Administration's policies to root out waste, fraud, and abuse across the federal government. Although these teams liaise with USDS—

[1] The Court should exercise its discretion to convert Plaintiffs' motion to one for a preliminary injunction because Defendants have "had a fair opportunity to oppose it." *U.S. Dep't of Lab. v. Wolf Run Mining Co.*, 452 F.3d 275, 283 (4th Cir. 2006) ("[A] district court could properly consider a motion for a TRO as a request for a preliminary injunction, . . . focusing not on a specific time period but on whether the opposing party had a fair opportunity to oppose it.").

a component of the Executive Office of the President—it is the agencies' employees, and only those employees, who have access to the data systems containing the personal information upon which Plaintiffs premise their claims.

Those claims accordingly fail both at the threshold and on the merits, and Plaintiffs are not entitled to the extraordinary preliminary relief that they seek. Plaintiffs lack standing, each of their claims is unlikely to succeed, they face no irreparable harm, and the equities and public interest weigh against them for the same reason. The entirety of their motion relies on one claim: that it is unlawful for one employee of a federal agency to provide access to its data systems to another employee for the purpose of carrying out an Executive Order of the President. That claim cannot be correct, so their motion fails.

BACKGROUND

I. The United States Department of Government Efficiency Service

On January 20, 2025, President Trump signed Executive Order 14,158, which directs changes to the previously established U.S. Digital Service designed to implement the President's agenda of "improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." 90 Fed. Reg. 8441, § 4 ("USDS EO"). The USDS EO also redesignated the U.S. Digital Service as the Department of Government Efficiency Service, or U.S. DOGE Service ("USDS"). *Id.* § 3(a). It established a "U.S. DOGE Service Temporary Organization" in the Executive Office of the President under 5 U.S.C. § 3161, which will terminate on July 4, 2026. USDS EO § 3(b). The USDS EO requires agency heads to establish in their respective agencies a USDS team of at least four employees. *Id.* § 3(c).

The USDS EO directs USDS to collaborate with Executive agencies to modernize the technology and software infrastructure of the federal government to increase efficiency and productivity as well as ensure data integrity. USDS EO § 4. As to Treasury, the need to modernize

and ensure data integrity is uniquely critical: the Government Accountability Office ("GAO") has identified "problems in accounting for transactions between federal agencies," resulting in potentially improper payments totaling approximately $2.7 trillion dollars. *See* GAO Report, "Financial Statement Audit: Bureau of the Fiscal Service's FY22 Schedules of the General Fund" (March 30, 2023), *available at* https://www.gao.gov/products/gao-23-104786 (last visited Feb. 18, 2025). And as to OPM, GAO has identified 16 "priority recommendations" involving "preventing improper payments," "improving payroll data," and "strengthening IT security and management." *See* GAO Report, "Priority Open Recommendations: Office of Personnel Management" (May 28, 2024) at 1-2, *available at* https://www.gao.gov/assets/gao-24-107323.pdf (last visited Feb. 18, 2025) (capitalization and bold removed). GAO stated that "[f]ully implementing these open recommendations could significantly improve both OPM's operations and its efforts to assist federal agencies in addressing various human capital management issues." *Id*. at 1.

To accomplish its objectives, the USDS EO directs USDS to work with relevant agency heads, and vice versa, to ensure USDS has access to "unclassified agency records, software systems, and IT systems" to the "extent consistent with law." USDS EO § 4(b). At all times, the USDS EO instructs, USDS must "adhere to rigorous data protection standards." *Id*.

II. Review of and access to Bureau of the Fiscal Service payment systems to effectuate the USDS EO

As background, the Bureau of the Fiscal Service ("BFS") is a component of the Treasury, established in October 2012 by then-Secretary of the Treasury Timothy Geithner. *See Treasury Order Establishing the Bureau of the Fiscal Service*, 78 Fed. Reg. 31,629 (May 24, 2013) (Treasury Order 136-01). Among other responsibilities, the BFS is responsible for "manag[ing] the government's accounting, central payment systems, and public debt, . . . and . . . serves as the

central payment clearinghouse for all payments to and from federal agencies." *See* Ex. A, Declaration of Thomas H. Krause, Jr. ("Krause Decl.") ¶ 5.

Currently, there is only one member of Treasury's USDS team, Thomas Krause.[2] Krause Decl. ¶ 3. Mr. Krause is a Treasury employee and is the USDS team lead at the agency. Krause Decl. ¶¶ 1-2. His position at Treasury as Senior Advisor for Technology and Modernization was created to effectuate the mission of USDS by reducing and eliminating improper and fraudulent payments, addressing the problems of waste, fraud, and abuse, and improving the accuracy of financial reporting. Krause Decl. ¶ 2. Although Mr. Krause coordinates with officials at USDS and provides them with regular updates on the team's progress, he is not an employee of USDS. Krause Decl. ¶ 4. Instead, he is an employee of Treasury and, as of February 13, has been delegated the duties of the Fiscal Assistant Secretary, in a Temporary Transition Schedule C position. *See* Ex. B, Declaration of Michael J. Wenzler ("Wenzler Decl.") ¶¶ 4, 7.

Mr. Krause's role at Treasury is to find ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of the current Administration. Krause Decl. ¶ 4. As part of the President's USDS efforts, Mr. Krause's mandate is to understand how BFS's end-to-end payment systems and financial reporting tools work, recommend ways to update and modernize those systems to better identify improper and fraudulent payments, and better allow federal agencies to quickly adapt to changing conditions. Krause Decl. ¶ 11. Mr. Krause has never had any direct access to any BFS payment system. His only access to

[2] A second Treasury USDS team member, Marko Elez, *see* Pls.' Mem. at 10, began working at the Treasury Department on January 21, 2025, but resigned from his role on February 6. Krause Decl. ¶ 3. On that same day, he turned in his government-issued laptops, access card, and other government devices; his BFS systems access was terminated; and he has not conducted any work related to the BFS payment systems since that date. Krause Decl. ¶ 3.

those systems was so-called "over the shoulder" access to review activity others performed in the system or data others accessed from the system. Krause Decl. ¶ 16.

III. OPM and the USDS EO

OPM is an Executive Branch "establishment" that, among other things, is responsible for "executing, administering, and enforcing . . . the civil service rules and regulations of the President." 5 U.S.C. §§ 1101; 1103(a)(5)(A). OPM plays a critical role in overseeing and managing the federal workforce. *See* Ex. C, Declaration of Greg Hogan ("Hogan Decl.") ¶ 8. Given that central role, numerous OPM employees, both political and career, have contributed to facilitating the President's initiatives related to workforce reform, including the deferred resignation program that closed on February 12, 2025. Hogan Decl. ¶ 8.

All individuals with access to sensitive OPM records systems, including Enterprise Human Resources Integration ("EHRI"), who are central to implementing the USDS EO are employees of OPM. Hogan Decl. ¶¶ 12-13. They were all hired directly by OPM as employees or, in one case, detailed to OPM by another agency. Hogan Decl. ¶¶ 12-13. All such OPM employees who have participated in workforce reform, like all OPM employees, are subject to applicable privacy, ethics, and other requirements. Hogan Decl. ¶ 9. Many OPM employees involved in these efforts hold policymaking, legal, or similar positions that do not require access to sensitive data systems. Hogan Decl. ¶¶ 9-10.

For systems engineers who require access to sensitive systems such as eOPF and EHRI, the OPM's Chief Information Office will periodically review access permissions to ensure that they are limited to those with a need to know. For example, in early February, the CIO removed eOPF and EHRI access for three engineers whose job duties do not require prospective access. Hogan Decl. ¶ 11.

IV. Pending litigation involving Treasury and OPM

Before this suit and motion for a TRO, several other lawsuits were filed against Treasury and OPM seeking relief similar to that sought here.

As to Treasury, in *Alliance for Retired Americans v. Treasury*, 1:25-cv-313 (D.D.C.), the parties have agreed to a consent order to preserve the status quo, which included permitting Mr. Krause to continue accessing BFS systems and data. *See id*., ECF No. 13. The court converted the TRO to a preliminary injunction; oral argument is set for February 24.

In *State of New York, et al., v. Treasury, et al.,* No. 1:25-cv-1144 (S.D.N.Y), the emergency "Part I" judge entered an *ex parte* TRO on February 8. *Id*., ECF No. 8. That order was amended in part on February 11. *Id*., ECF No. 28. The order (as amended by the court) prohibits the USDS team at Treasury (Mr. Krause) from accessing Treasury systems containing personal or financial information, pending preliminary injunction proceedings. *Id*. Argument on the preliminary injunction was heard February 14.

A third suit, and motion for TRO, was filed against Treasury on February 10, 2025, in the District of Maryland. *See Am. Fed'n of Teachers, et al., v. Bessent, et al*, No. 8:25-cv-430 (D. Md.). Defendants filed an opposition on February 17; a hearing is set for February 19. Finally, a fourth suit was filed against Treasury on February 17, in the District of Columbia. *See Center for Taxpayer Rights v. IRS*, No 1:25-cv-457 (D.D.C.).

OPM also is a defendant that District of Maryland matter and in a similar suit in the Southern District of New York. *See AFL/CIO, et al., v. Office of Personnel Mgmt., et al.,* No. 1:25-cv-1237 (S.D.N.Y.). In the *AFL/CIO* matter, a TRO motion was filed on February 14; a briefing schedule is due February 18.

There is also similar litigation pending against other agencies, and in two cases courts have denied motions for TROs. *See* Mem. Op. & Order (ECF No. 20), *Univ. of Ca. Student Assoc. v.*

Carter, et al., No. 1:25-cv-354 (D.D.C. Feb. 17, 2025); Mem. Op. & Order (ECF No. 34), *Am. Fed. of Labor of Indus. Orgs. v. Dep't of Labor*, No. 1:25-cv-339, (D.D.C. Feb. 14, 2025).[3]

V. Plaintiffs' claims and motion for a temporary restraining order

Plaintiffs filed this suit on February 10, 2025. Compl. (ECF No. 1). Plaintiffs are the Electronic Privacy Information Center ("EPIC"), a nonprofit organization, and Doe 1, a current federal agency employee. Compl. ¶¶ 9-10.

The Complaint asserts five causes of action. In Count One, Plaintiffs allege that Treasury and OPM's conduct is arbitrary, capricious, an abuse of discretion, or otherwise contrary to law under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), because Treasury and OPM have administered systems "without complying with statutorily required security protections under" the Federal Information Security Modernization Act of 2014 ("FISMA"), 44 U.S.C. §§ 3554(a)(1)-(2). Compl. ¶¶ 105-09. In Count Two, Plaintiffs allege that Treasury and OPM have violated the Privacy Act of 1974 by "disclos[ing]" Plaintiffs' personal data in violation of 5 U.S.C. § 552a(b) and by "us[ing] such data for computer matching" in violation of § 552a(o). *Id*. ¶¶ 110-12. In Count Three, Plaintiff Doe 1, only, alleges that Treasury and USDS, but not OPM, have "disclos[ed] and inspect[ed]" her tax return information in violation of the Internal Revenue Code, 26 U.S.C. § 6103. *Id*. ¶¶ 113-18. In Count Four, Plaintiffs claim that Defendants, "by providing access to confidential personal information," have deprived EPIC's members and Doe 1 of their liberty interest in "avoiding disclosure of personal matters" under the Fifth Amendment's Due Process Clause. *Id*. ¶¶ 119-22. And in Count Five, Plaintiffs assert a mandamus claim, alleging that the "DOGE Defendants" have engaged in ultra vires actions "[i]n directing and controlling the use and administration" of the BFS and EHRI systems without legal authority. *Id*. ¶¶ 123-128.

[3] Defendants will update the Court in writing of any developments in these matters no later than February 20 and, if needed, will further update the Court at the hearing on February 21.

Plaintiffs filed a motion for temporary restraining order on February 12. Mot. (ECF No. 5). Plaintiffs seek (1) to enjoin Treasury and OPM "from allowing DOGE-affiliated personnel to access" BFS or EHRI systems, (2) to enjoin "DOGE-affiliated personnel from accessing Treasury or OPM systems containing personally identifiable information except consistent with relevant SORNs [Systems of Records Notices]," and (3) to require Treasury and OPM to file a status report within 24 hours of the issuance of a TRO, "confirming that DOGE-affiliated personnel no longer have access to EHRI or BFS systems." Mot. at 2; Pls.' Mem. at 29.

STANDARD OF REVIEW

"A [TRO or] preliminary injunction[4] is 'an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief' and may never be awarded 'as of right.'" *Mountain Valley Pipeline, LLC v. W. Pocahontas Properties Ltd. P'ship*, 918 F.3d 353, 366 (4th Cir. 2019) (quoting *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22, 24 (2008)). A preliminary injunction is "intended to protect the status quo and prevent irreparable harm during the pendency of a lawsuit." *Di Biase v. SPX Corp.*, 872 F.3d 224, 230 (4th Cir. 2017); *Fed. Trade Comm'n v. Pukke*, 795 F. App'x 184, 188 (4th Cir. 2020) ("The purpose of a preliminary injunction is to preserve the relative positions of the parties until a trial . . . and to protect the status quo and to prevent irreparable harm during the . . . lawsuit ultimately to preserve the court's ability to render a meaningful judgment on the merits.") (internal quotation marks and citation omitted).

"A party 'seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.'" *Roe v. Dep't*

[4] "The standard for granting either a TRO or a preliminary injunction is the same." *Sarsour v. Trump*, 245 F. Supp. 3d 719, 728 (E.D. Va. 2017) (quotation marks and citation omitted).

of Def., 947 F.3d 207, 219 (4th Cir. 2020), as amended (Jan. 14, 2020) (quoting *Winter*, 555 U.S. at 20). If a plaintiff fails to succeed on any one of these requirements, the motion for a preliminary injunction must be denied. *Mountain Valley Pipeline*, 918 F.3d at 366 ("Each of these four requirements must be satisfied.") (citing *Winter*, 555 U.S. at 20).

ARGUMENT

Plaintiffs are not entitled to the relief they seek. They are not likely to succeed on the merits because the intra-agency data systems access at issue here does not violate the Privacy Act, the Internal Revenue Code, the APA, or any Fifth Amendment privacy right. And for the same reason, Plaintiffs have shown no harm to any of their privacy rights or that the balance of equities and public interest weigh in their favor. Their motion should be denied.

I. Plaintiffs are not likely to succeed on the merits.

A. Plaintiffs lack Article III standing because they have not shown an injury in fact.

The Court should deny the temporary restraining order at the threshold because both EPIC and Doe lack standing. *Sarsour*, 245 F. Supp. 3d at 728 ("[T]o obtain the requested injunction, Plaintiffs must first demonstrate that they have standing to challenge EO–2."); *McKague v. HSCGP, LLC*, 2022 WL 3010472, at *2 (W.D. Va. July 29, 2022) ("On a motion for a preliminary injunction, a plaintiff's burden of showing a likelihood of success . . . necessarily depends on a likelihood that plaintiff has standing.") (internal quotation marks and citation omitted).

To establish standing, "a plaintiff must demonstrate (i) that she has suffered or likely will suffer an injury in fact, (ii) that the injury likely was caused or will be caused by the defendant, and (iii) that the injury likely would be redressed by the requested judicial relief." *Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 380 (2024) (citations omitted). "Those specific standing requirements constitute an essential and unchanging part of the case-or-controversy

requirement of Article III." *Id*. (internal quotation marks and citations omitted). Facts demonstrating each of these elements "must affirmatively appear in the record" and "cannot be inferred argumentatively from averments in the [plaintiff's] pleadings." *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 231 (1990) (citation omitted). And "[t]he party seeking to establish standing carries the burden of demonstrating these elements." *Chambers Med. Techs. of S.C., Inc. v. Bryant*, 52 F.3d 1252, 1265 (4th Cir. 1995).

For the injury-in-fact requirement, a plaintiff must show a "concrete" ("real," not "abstract") injury-in-fact, which is "particularized" to the plaintiff and not a "generalized grievance." *Alliance*, 602 U.S. at 381. The injury must be "certainly impending;" "allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). And "'[w]hen the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult' to establish.'" *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 489 (4th Cir. 2025) (quoting *Summers v. Earth Island Inst.*, 555 U.S. 488, 493-94 (2009)).

1) EPIC lacks organizational standing because it has not shown injury-in-fact as to its members.

As an organization, EPIC "can demonstrate Article III standing either in [its] own right or as a representative of [its] members." *Maryland Election Integrity, LLC v. Maryland State Bd. of Elections*, No. 24-1449, 2025 WL 377752, at *3 (4th Cir. Feb. 4, 2025) (internal quotation marks and citation omitted). EPIC does not rely on alleged injury to the organization itself but instead to the privacy interests of its members. Pls.' Mem. at 24 ("[M]any of EPIC's members have filed their federal tax returns electronically . . . so BFS systems contain extensive financial information about them"); Compl. ¶ 120 ("Defendants, by providing access to confidential personal information . . . have deprived EPIC's members . . . of their liberty interest in avoiding disclosure

of personal matters."). "To establish representational standing," EPIC "must demonstrate that" its "members would otherwise have standing to sue in their own right." *Maryland Election Integrity, LLC*, 2025 WL 377752, at *3 (internal quotation marks and citation omitted). To do so, EPIC must establish injury-in-fact as to those members. *Id*.

As a basis for standing, EPIC alleges one type of injury, that its members "reasonably expected that the information they had provided the government was subject to comprehensive protections against unlawful disclosure" and that "[b]reaking those expectations in violation of statute injures" EPIC's members "in a way that creates statutory harm and confers standing." *See* Pls.' Mem. at 24 (internal quotation marks and citation omitted); *id*. at 25 ("The disclosure of confidential and sensitive information causes substantial and irreparable harm to those to whom the information belongs."). That argument is factually and legally incorrect.

As an initial matter, there has been no third-party or unauthorized disclosure at Treasury or OPM, as only authorized agency employees have accessed the data systems at issue, as set forth above. But even assuming—solely for purposes of the injury-in-fact analysis, *see, e.g.*, *Warth v. Seldin*, 422 U.S. 490, 502 (1975)—that there had been such access, EPIC still fails to establish standing. This is because even unauthorized access alone would not give rise to an actual, concrete harm sufficient to establish standing. *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021), leaves no doubt that a statutory violation is not, by itself, a cognizable Article III injury. *Id.* at 426-27. Rather, "[o]nly those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that . . . defendant over that violation in federal court." *Id.* at 427 (emphasis in original).

For EPIC to establish some *concrete* harm on behalf of its members based on a disclosure theory—and absent any independent, claimed harm—it would need to show not just *access* to its members' information but show that the access has resulted in an intangible harm that is analogous

to a common-law tort. *See Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 295 (4th Cir. 2024) ("[I]ntangible injuries, although perhaps more difficult to recognize, can also be concrete. We evaluate whether an alleged injury is concrete by assessing whether it has a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts. That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury.") (internal quotation marks and citation omitted). To the extent that Plaintiffs intend to allege reputational harm, they would have to show that the information had been publicly disclosed. *See id.* at 295-96 ("[T]he presence of the same misleading [information] in an internal credit file causes no concrete harm if it is not disclosed to a third party. . . . [T]here is no historical or common-law analog where the mere existence of inaccurate information amounts to concrete injury.") (internal quotation marks and citation omitted); *see also TransUnion*, 594 U.S. at 434 n.6 ("Many American courts did not traditionally recognize intra-company disclosures as actionable publications for purposes of the tort of defamation.") (citations omitted).

There has been no public disclosure of EPIC's members' information.[5] Instead, there has been (at most) an exchange within the federal government. *Elhady v. Kable*, 993 F.3d 208, 225 (4th Cir. 2021) ("The federal government's intragovernmental dissemination of [Terrorist Screening Database] information to other federal agencies and components, to be used for federal law enforcement purposes, is not public disclosure for purposes of a [harm to constitutional liberty interest in reputation]."). EPIC does not allege—much less establish—that the government

[5] Plaintiffs originally alleged that "information exfiltrated from the BFS payment systems was broadcast . . . on Twitter/X" when "retired Lt. Gen. Mike Flynn disclosed screenshots showing 42 payments from . . . to various recipients." Compl. ¶ 65; Pls.' Mem. at 11. But Plaintiffs have since informed the Court that this information was publicly available before the post. *See* Not. of Factual Develop. (ECF No 18) at 2. And they do not allege that anyone has publicly disclosed EPIC members' or Doe's (or any anyone else's) information.

employees with BFS systems access have disclosed any EPIC members' information publicly, let alone in a way that causes tangible harm. *Cf.* Mem. Op. & Order (ECF No. 34), *Am. Fed. of Labor of Indus. Orgs. v. Dep't of Labor*, No. 1:25-cv-339, at 3 n.1 (D.D.C. Feb. 14, 2025) (Bates, J.) ("*AFL* Order"). And because there has been no outside-of-government disclosure, this case is unlike *Gaston v. LexisNexis Risk Solutions, Inc.*, *see* Pls.' Mem. at 24, where the private-company defendants sold information-service subscriptions that provided access to police accident reports containing personal information. 483 F. Supp. 3d 318, 331 (W.D.N.C. 2020).

Nor do EPIC's claims of "likely . . . further disclos[ure]" or "a heightened risk of exposure or exfiltration by hostile actors" establish injury-in-fact. *See* Pls.' Mem. at 24. These alleged future harms are too speculative on their own to support standing. *See Clapper*, 568 U.S. at 416 ("[F]ears of hypothetical future harm that is not certainly impending," without more, cannot satisfy Article III); *see also Murthy v. Missouri*, 603 U.S. 43, 57 (2024) (no standing where a theory of injury "relies on a highly attenuated chain of possibilities"). Further, these theories are contradicted by the declarations in the record regarding the extensive security mitigation measures Treasury and OPM have employed. *See* Ex. D, Declaration of Joseph Gioeli, III ¶¶ 11-15 ("Gioeli Decl."); Krause Decl. ¶ 15; Hogan Decl. ¶ 9.

2) Doe lacks standing because she has not shown injury-in-fact.

Plaintiff Doe cannot show an injury in fact, and thus lacks standing, for the same reasons that EPIC cannot. *Alliance*, 602 U.S. at 381. Doe's standing argument is the same as EPIC's, alleged "unlawful disclosure" of her information. *See* Pls.' Mem. at 24.[6] Because there has been

[6] Plaintiffs attach a declaration from Doe 1 to their memorandum of law, but other than a signature from "Doe 1," that document appears to be blank. *See* ECF No. 7-1. The declaration from EPIC member Alan Butler is unsigned. ECF No. 7-2 at 4.

no external-to-government disclosure of her information, Doe does not allege a cognizable injury based on OPM or Treasury employees' access to the BFS or EHRI systems.

B. Plaintiffs cannot prevail on any of their claims.

1) Plaintiffs have not shown a violation of the Privacy Act because § 552a(b) permits intra-agency disclosure for official duties.

Plaintiffs are not likely to succeed on their Privacy Act claim. This claim rests on the flawed notion that what Plaintiffs term "DOGE operatives" are not federal employees, or at least not employees of Treasury and OPM. Pls.' Mem. at 18. Plaintiffs are mistaken. As a result, the Privacy Act expressly allows disclosure of the records at issue in this case.

The Privacy Act limits the ability of an "agency" to "disclose any record which is contained in a system of records . . . to any person, or to another agency." 5 U.S.C. § 552a(b). As relevant here, such 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). "[F]or purposes of" Title 5 of the U.S. Code, "employee" "means an officer and an individual who is" first "appointed in the civil service by one of the following acting in an official capacity"; as relevant here, the list of potential appointers includes "the President" and "an individual who is an employee under this section." *Id.* § 2105(a)(1)(A), (D). An employee must also be "engaged in the performance of a Federal function under authority of law or an Executive act; and . . . subject to the supervision of an individual named by paragraph (1) of this subsection while engaged in the performance of the duties of his position." *Id.* § 2105(a)(2). Because the Privacy Act is part of Title 5, section 2105's definition of employee directly applies to its use of the term "employee." *See id.* § 552a(b)(1).[7]

[7] Because the Privacy Act expressly permits disclosure to agency "employees" generally, any attempt by Plaintiffs in their reply to artificially parse the term into different categories of employee for purposes of disallowing access has no basis in the Privacy Act's text and is therefore

As explained above, the individuals whose access Plaintiffs challenge are (or were) employees of Treasury and OPM. All have been appointed to their positions under federal law, including the detailees. Krause Decl. ¶¶ 1-3; Wenzler Decl. ¶¶ 3-4, 7-10; Hogan Decl. ¶¶ 12. All are "engaged in the performance of a Federal Function under authority of . . . an Executive act," *i.e.*, the USDS EO. Krause Decl. ¶¶ 2, 11-12; Hogan Decl. ¶¶ 8, 12. And all are ultimately subject to the supervision of the senior leadership of their respective agencies, whether because they have been appointed as agency employees under agency-specific statutes directly or because they are detailed to those agencies. Krause Decl. ¶ 2; Hogan Decl. ¶¶ 9, 12-13.

The relevant employees also satisfy the requirement that they be employees "of" Treasury and OPM. *See* 5 U.S.C. § 552a(b)(1). At each agency, some of the employees were hired directly by the agency, clearly resolving their status. Wenzler Decl. ¶¶ 3-4, 7-10; Krause Decl. ¶¶ 1, 3; Hogan Decl. ¶ 12. The detailees from other components of the Executive Branch qualify, too. While courts in the Fourth Circuit do not appear to have considered the question, the D.C. Circuit has adopted a functional approach in evaluating the employment status of detailees, looking to the subject matter and purpose of the individual's work, their supervision, and their physical worksite as illustrative (but not conclusive) factors. *Judicial Watch v. Dep't of Energy*, 412 F.3d 125, 131-32 (D.C. Cir. 2005). Here, those factors clearly cut in favor of the detailees' status as employees of their respective agencies. *See id.*; *see also Liable v. Lanter*, 91 F.4th 438, 442 (6th Cir. 2024); *Mount v. U.S. Postal Serv.*, 79 F.3d 531, 532, 533 (6th Cir. 1996); *Ciralsky v. CIA*, 689 F. Supp. 2d 141, 155 (D.D.C. 2010); *Freeman v. EPA*, 2004 WL 2451409, at *4-5 (D.D.C. Oct. 25, 2004).

irrelevant. *See BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004) (explaining that a court's interpretive "inquiry begins with the statutory text, and ends there as well if the text is unambiguous").

These employees also have a "need to know," for purposes of the Privacy Act, with respect to the data systems at issue.[8] The USDS EO provides that these individuals have a need to know "*all* unclassified agency records, software systems, and IT systems" to perform their duties. 90 Fed. Reg. 8441, § 4 (emphasis added). More specifically, the relevant personnel at Treasury have a need to access systems containing Privacy Act-protected records to identify potential waste, fraud, and abuse in payments made by Treasury. Krause Decl. ¶¶ 2, 5, 7-14, 17-21; Gioeli Decl. ¶¶ 4-10;, 13-15; Wenzler Decl. ¶ 5; Ex. E, Declaration of Vona S. Robinson ("Robinson Decl.") ¶¶ 6-11.[9] In connection with this access, Treasury employees—including career civil servants—identified exactly the sort of risks Plaintiffs complain of and implemented appropriate security and mitigation measures. Krause Decl. ¶ 15; Gioeli Decl. ¶¶ 11-22. Likewise, OPM personnel need to access such records to facilitate President Trump's workplace-reform initiatives, including the deferred-resignation program recently offered to federal employees. Hogan Decl. ¶¶ 8-9.[10] *Cf. AFL* Order at 3-4, 8. Contrary to Plaintiffs' conclusory insistence that there is no "lawful or legitimate need" to access the relevant data systems, Pls.' Mem. 28, compliance with the President's Executive Orders in fact furthers the aims of the agencies that the same President controls, *cf. Collins v. Yellen*, 594 U.S. 220, 252 (2021) (emphasizing that "because the President, unlike

[8] As explained below, access to these systems as a whole is not the same as disclosure of *Plaintiffs' records* allegedly contained within those systems. *See infra*, p. 17.

[9] For the Court's information—and though not relevant to Plaintiffs' claims—Treasury's USDS team shared data from a BFS system concerning USAID payments with the State Department as part of a foreign-aid review process in connection with an Executive Order temporarily freezing such payments. *See* Robinson Decl. ¶¶ 8-15. Plaintiffs do not challenge this data sharing, which was appropriate pursuant to one of Treasury's routine uses under the Privacy Act in any event. *See infra*, p. 17.

[10] These OPM employees are also required to observe privacy and ethics protocol, and periodic re-assessments ensure access is limited to those with a need to know. Hogan Decl. ¶¶ 9, 11-13.

agency officials, is elected," Presidential control "is essential to subject Executive Branch actions to a degree of electoral accountability").

In the alternative, Defendants' actions are permissible under the Privacy Act's exception for "routine use." *See* 5 U.S.C. § 552a(b)(3) (permitting disclosure absent consent for certain "Routine Uses" that are defined in a published Systems of Record Notice ("SORN")). One of Treasury's published routine uses permits disclosure to a federal agency "for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, federal funds." 85 Fed. Reg. 11,776, 11,780 (2020). Treasury's USDS team is tasked with doing just that. Krause Decl. ¶¶ 2-4.

Setting aside that any disclosure of Privacy Act records was authorized, as just discussed, Plaintiffs' Privacy Act claim fails for two additional reasons. First, Plaintiffs produce no evidence, and do not even seriously argue, that *their* records have been disclosed. Rather, they contend that Treasury and OPM have provided access to systems that *contain* Plaintiffs' records. But accessibility alone is not sufficient, as disclosure of a plaintiff's record(s) may not be presumed. *See*, *e.g.*, *Luster v. Vilsack*, 667 F.3d 1089, 1098 (10th Cir. 2011); *Walia v. Chertoff*, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008); *Schmidt v. U.S. Dep't of Veterans Affairs*, 218 F.R.D. 619, 630 (E.D. Wis. 2003); *Mittleman v. U.S. Dep't of Treasury*, 919 F. Supp. 461, 468 (D.D.C. 1995). Because Plaintiffs are unable to show that any such actual disclosure occurred, they also cannot make out the separate requirement of a Privacy Act claim that the disclosure has been "intentional or willful," 5 U.S.C. § 552a(g)(4), which requires "more than gross negligence," *Reinbold v. Evers*, 187 F.3d 348, 361 n.14 (4th Cir. 1999).

Finally, even if Plaintiffs could make out a viable disclosure claim under the Privacy Act, the injunctive relief that they seek would not be appropriate. The statute provides for injunctive

relief in only two narrow circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C. § 552a(g)(1)(A), (g)(2)(A); and (2) to order an agency to allow an individual access to his records, *id.* § 552a(g)(1)(B), (g)(3)(A). Where, as here, "[a] 'statute provides certain types of equitable relief but not others, it is not proper to imply a broad right to injunctive relief.'" *Parks v. IRS*, 618 F.2d 677, 84 (10th Cir. 1980) (citation omitted). Accordingly, injunctive relief is not available for any other type of Privacy Act claim. *See Sussman v. U.S. Marshal Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007) ("We have held that only monetary damages, not declaratory or injunctive relief, are available to § 552a(g)(1)(D) plaintiffs.") (citing *Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988)).

2) Plaintiffs have not shown a violation of the Internal Revenue Code § 6103 because § 6103(h) permits disclosure to the Treasury employees.

Plaintiffs next turn to the set of statutory protections applicable to tax returns or return information in § 6103 of the Internal Revenue Code. Pls.' Mem. at 15-18. Plaintiffs claim this provision has been violated only with respect to Treasury; they do not argue that OPM's data was improperly accessed or disclosed in violation of § 6103. *See id.* at 18.

But Plaintiffs' argument fails with respect to Treasury because an exception to the general rule of § 6103(a) applies for "[d]isclosure to certain Federal officers and employees for purposes of tax administration." 26 U.S.C. § 6103(h). Indeed, "officers and employees of the Department of the Treasury" may obtain returns and return information if their "official duties require such inspection or disclosure for tax administration purposes." *Id.* "Tax administration," in turn, is defined to include "the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws." *Id.* § 6103(b)(4)(A)(i). The payment systems at issue in this case disburse the vast majority of government payments, including tax

refunds. *See* Fiscal Service Overview, available at https://www.fiscal.treasury.gov/about.html (last visited Feb. 18, 2025).

The Treasury DOGE team satisfied these statutory conditions for access to returns and return information. They are, to start, Treasury employees. Krause Decl. ¶¶ 1-3. And their official duties include "improving the controls, processes, and systems that facilitate payments and enable consolidated financial reporting" and "us[ing] technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of this Administration." Krause Decl. ¶¶ 2, 4. Indeed, some of the Treasury USDS team's duties related to GAO concerns regarding improper payments generally, and one of the programs GAO identified with a high risk of improper payments is IRS's Earned Income Tax Credit refunds. Krause Decl. ¶ 8. Moreover, the returns and return information subject to the protections of § 6103 pass through (and are stored on) the very same systems that the Treasury USDS team is responsible for improving pursuant to Executive Order 14,158. Just like all of the other Treasury employees, contractors, and others who work every day to maintain and improve the operation of these critical payment systems, they therefore had the requisite need to obtain § 6103 material in the exercise of their official duties.

3) Plaintiffs cannot prevail on their APA claim

(i) An agency's FISMA implementation is not subject to judicial review.

Plaintiffs argue that by "[g]ranting access to sensitive information systems . . . in violation of the Federal Information Systems Modernization Act" ("FISMA"), Defendants "violated the Administrative Procedure Act." *See* Pls.' Mem. at 18. But, in addition to the fact that there is no unauthorized access here, the APA provides no cause of action to review an agency's compliance with its FISMA responsibilities because a federal agency's FISMA compliance is committed to agency discretion—as the U.S. District Court for the District of Columbia held when addressing a

nearly identical claim last week. *See AFL* Order at 9 ("Plaintiffs' arguments that defendants are violating . . . FISMA . . . are not likely to succeed because FISMA may not be subject to review under the APA." (citing *Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006))).

The judicial review provisions of the APA, 5 U.S.C. §§ 701-06, establish a cause of action for parties adversely affected either by agency action or inaction. *Heckler v. Chaney*, 470 U.S. 821, 827 (1985). But the APA explicitly excludes from judicial review those agency actions that are "committed to agency discretion by law." 5 U.S.C. § 701(a)(2). To determine whether a matter has been committed to agency discretion, the Fourth Circuit applies a two-part inquiry. *Holbrook v. Tennessee Valley Auth.*, 48 F.4th 282, 290 (4th Cir. 2022). First, whether the agency action "is the kind of agency action that has traditionally been committed to agency discretion." *Id*. (internal quotation marks and citations omitted). Second, whether the relevant statute "intentionally limits agency discretion by setting guidelines or otherwise providing a limit" for agency discretion. *Id*.

Here, as to the first part, Congress passed FISMA to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). However, Congress specifically "recognize[d] that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products." 44 U.S.C.A. § 3551(6). In the FISMA context, then, agency action is expressly "the kind of agency action . . . committed to agency discretion." *Holbrook*, 48 F.4th at 290.

As to the second part—any limit to that discretion—FISMA offers no specific prescriptions for the tools or methods required, which is unsurprising considering the rapidly evolving nature of both technology and cyber threats. Instead, Congress vested agencies with broad discretion to adopt "security protections commensurate with the risk and magnitude of the harm" resulting from

cyber threats. 44 U.S.C. § 3554(a)(1)(A). FISMA gives agencies latitude to develop security policies and procedures that are "appropriate" and "cost-effectively reduce information security risks to an acceptable level." *Id*. at § 3554(b)(2)(B). To achieve its goals, FISMA assigns *exclusive* responsibility for overseeing the management and security of information systems of civilian agencies to the Director of the Office of Management and Budget ("OMB"). FISMA mandates that the OMB Director "shall oversee agency information security policies and practices, including . . . overseeing agency compliance with the requirements of this subchapter [of FISMA.]" *Id.* § 3553(a)(5). FISMA specifically authorizes the OMB Director "to enforce accountability for compliance," *id.*, through various mechanisms, including by "tak[ing] any action that the Director considers appropriate, including an action involving the budgetary process or appropriations management process," 40 U.S.C. § 11303(b)(5)(A). The Director also must review each agency's security programs at least annually and approve or disapprove them. 44 U.S.C. § 3553(a)(5). Finally, he must report to Congress annually on the "effectiveness of information security policies and practices during the preceding year." *Id.* § 3553(c). Accordingly, a federal agency's compliance with FISMA is committed to agency discretion by law, and FISMA cannot be the basis of Plaintiffs' APA claim. *See Cobell*, 455 F.3d at 314 ("Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in carrying out its FISMA obligations.").

(ii) The intra-agency informational transfer alleged here is not agency action that is subject to APA review

Plaintiffs do not challenge discrete Treasury or OPM action but instead the routine, mine-run determinations to give specific employees access to specific systems for specific purposes—exactly the type of programmatic activity that is not agency action subject to APA review. "When challenging agency action . . . the plaintiff must . . . identify specific and discrete governmental

conduct, rather than launch a broad programmatic attack on the government's operations." *City of New York v. U.S. Dep't of Def.*, 913 F.3d 423, 431 (4th Cir. 2019) (internal quotation marks and citation omitted). And "[r]eview is available only when acts are discrete in character, required by law, and bear on a party's rights and obligations." *Id*. at 432.

Plaintiffs here do not identify a specific unauthorized disclosure that they are challenging. They instead challenge Treasury and OPM's information practices in general in effectuating Executive Order 14,158. *See generally* Compl. Plaintiffs thus "ask that [the Court] supervise an agency's compliance with the broad statutory mandate of [FISMA]." *City of New York*, 913 F.3d at 433 (internal quotation marks and citation omitted). That compliance "is the sort of public policy problem that often requires reallocating resources, developing new administrative systems, . . . working closely with partners across government[, and] will likely require expertise in information technology and deep knowledge of how [Treasury and OPM] needs intersect with data collection." *Id*. It is "exactly the sort of 'broad programmatic' undertaking for which the APA has foreclosed judicial review." *Id*. (quoting *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 64 (2004) (quoting 5 U.S.C. § 704) ("*SUWA*")).

(iii) Even if Plaintiffs had identified judicially reviewable agency action, they have not identified a final agency action.

Even if Plaintiffs had identified judicially reviewable agency action, their APA claim fails because they have not identified a *final* agency action. APA review is limited to "final agency action." *SUWA*, 542 U.S. at 61-62 (quoting 5 U.S.C. § 704). Agency action is final only when it "mark[s] the consummation of the agency's decisionmaking process" and is "one by which rights or obligations have been determined, or from which legal consequences will flow." *U.S. Army Corps of Eng'rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997)).

Plaintiffs have alleged that "the decision of Treasury and OPM to grant DOGE operatives access to their information systems represents final agency action." Pls.' Mem. at 15. But it is difficult to understand how providing new employees with system access necessary to their functions "consummate[es]" the agency's decision-making process in any formal sense. *Hawkes Co.*, 578 U.S. at 597. And "informal" agency actions, as a general matter, have not been considered "final" under *Bennett*'s first prong. *See Soundboard Ass'n v. FTC*, 888 F.3d 1261, 1267 (D.C. Cir. 2018) (quoting *Abbott Laby's v. Gardner*, 387 U.S. 136, 151 (1967)). Nor is it apparent how an employee's access to a system and the data in it has "direct and appreciable legal consequences" for anyone at all. *See Cal. Cmtys. Against Toxics v. EPA*, 934 F.3d 627, 640 (D.C. Cir. 2019). To establish finality, Plaintiffs would need to show (at least) that their members' data has, in fact, been improperly disclosed, including to the employees implementing the USDS EO—not just that they had access to it. By analogy, an agency's decision to give an employee access to its systems is not itself final agency action, even if the employee might conceivably use the computer to effect final agency action (*e.g.*, in approving or denying benefits). Because finality is analyzed from a "pragmatic" point of view, these facial oddities seriously undermine Plaintiffs' claim that it exists here. *See Hawkes Co.*, 578 U.S. at 599.

But the Court need not rely on pragmatism alone. Precedent confirms what common sense suggests: that "broad programmatic attack[s]" like Plaintiffs' fall categorically outside the ambit of judicial review under § 704. *See SUWA*, 542 U.S. at 64. In *Lujan v. National Wildlife Federation*, the plaintiffs challenged an agency's "land withdrawal review program" in its entirety. 497 U.S. 871, 890 (1990). That challenge could not proceed, the Supreme Court held, because the "program" did "not refer to a single [agency] order or regulation, or even to a completed universe of particular [agency] orders and regulations." *Id.* Instead, the "program" was "simply the name

by which [the plaintiffs] have occasionally referred to the continuing (and thus constantly changing) operations of the [agency] in reviewing withdrawal revocation applications and the classifications of public lands and developing land use plans as required by" federal law. *Id.* Plaintiffs' challenge to these employees' "access" to Defendants' systems is deficient in similar ways. Despite Plaintiffs' framing, the "decisions of the Treasury and OPM Defendants to grant DOGE Defendants access to their respective actions" as a final agency action, Pls.' Mem at 18, those decisions are not discrete events with legal consequences for Plaintiffs' members. Instead, Defendants' decisions mark a series of ongoing and "continuing (and thus constantly changing) operations," which include taking various steps to modernize and strengthen protections for its data systems. *See Nat'l Wildlife Fed'n*, 497 U.S. at 890

4) Even assuming that Plaintiffs have a Fifth Amendment right to informational privacy and that it applied to intra-government information sharing, Plaintiffs have not shown a Fifth Amendment violation.

For at least three independent reasons, Plaintiffs are not likely to succeed on their claim that Defendants' challenged actions infringe on their claimed due process right to "informational privacy" under the Fifth Amendment.

a. As a threshold matter, the Supreme Court has never held that a constitutional right to informational privacy exists. In the few decisions considering such claims, the Court has merely assumed, without holding, that there is such a right in the course of concluding that the challenged government action did not violate it. *See, e.g.*, *NASA v. Nelson*, 562 U.S. 134, 144-48 (2011). Despite this nonchalance, the Fourth Circuit has recognized an "individual interest in avoiding disclosure of personal matters," albeit one limited to "information with respect to which the individual has a reasonable expectation of privacy." *Payne v. Taslimi*, 998 F.3d 648, 655 (4th Cir.

2021) (quoting *Walls v. City of Petersburg*, 895 F.2d 188, 192-93 (4th Cir. 1990), *abrogated in other part by Lawrence v. Texas*, 539 U.S. 558 (2003)).[11]

Leaving to one side the questionable provenance of the right Plaintiffs claim, to the extent that it exists, it is quite narrow. The Supreme Court and the Fourth Circuit have considered informational privacy only in the context of (1) the government's *collection* of information (*i.e.*, whether the government may compel individuals to disclose information in the first instance), and (2) the government's *public* disclosure of information within its control (*i.e.*, whether the government may disseminate information it has obtained to third parties). *E.g.*, *Nelson*, 562 U.S. at 138 (employment background investigation); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 429 (1977) (compelled production of former President's papers and tape recordings); *Whalen v. Roe*, 429 U.S. 589, 591 (1977) (compilation of prescriptions for certain drugs); *Payne*, 998 F.3d at 652-53 (doctor's disclosure of prisoner's HIV-positive status); *Walls*, 895 F.2d at 189 (employment questionnaire). And even in those cases, both courts have concluded that the government action either did not implicate or did not violate whatever right to informational privacy there might be.

Defendants have not found a case, and Plaintiffs point to none, involving the distinct question, posed by this case, of whether a government's *internal* sharing of information it already possesses implicates a constitutional informational-privacy right. To the extent that there is any authority on this question, it seems to cut the other way. *See In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 74 (D.C. Cir. 2019) ("[A]ssuming (without deciding) the existence of a constitutional right to informational privacy, it affords relief only for intentional disclosures

[11] Although *Payne* was constrained to follow *Walls*, the Fourth Circuit made a point of noting the unstable foundation of the claimed right to informational privacy. *See* 998 F.3d at 653-57; *see also Am. Fed'n of Gov't Emps. v. HUD*, 118 F.3d 786, 788 (D.C. Cir. 1997) (expressing "grave doubts" that a right to informational privacy exists).

or their functional equivalent." (internal citations omitted)). In such an "uncharted area" as this, where "guideposts for responsible decision-making . . . are scarce and open-ended," the Court "must be 'reluctant to expand the concept of substantive due process.'" *Hawkins v. Freeman*, 195 F.3d 732, 738 (4th Cir. 1999) (quoting *Washington v. Glucksburg*, 521 U.S. 702, 720 (1997)).

b. Even if Plaintiffs could demonstrate that a right to informational privacy exists *and* that intra-governmental sharing of information implicates the right, Plaintiffs' claim would still fail because the Supreme Court has made clear that "a 'statutory or regulatory duty to avoid unwarranted disclosures' generally allays . . . privacy concerns." *Nelson*, 562 U.S. at 155 (quoting *Whalen*, 429 U.S. at 605). As relevant here, the requirements of the Privacy Act and the IRC "give 'forceful recognition' to a Government employee's interest in maintaining the 'confidentiality of sensitive information . . . in his personnel files." *Id.* at 156 (quoting *Detroit Edison Co. v. NLRB*, 440 U.S. 301, 318 n.16 (1979)). The Privacy Act and the IRC therefore "'evidence a proper concern' for individual privacy" and obviate any constitutional question regarding individuals' informational privacy. *Id.* (quoting *Whalen*, 429 U.S. at 605).

c. Finally, on top of the fatal defects above, Plaintiffs cannot show that the challenged Executive actions rise to the egregious level required to make out a due process claim. "An executive act can violate substantive due process only when the act shocks the conscience." *United States v. Al-Hamdi*, 356 F.3d 564, 574 (4th Cir. 2004). And "[u]sually," intent to harm is "necessary to satisfy the shocks-the-conscience test for a substantive due process violation." *Slaughter v. Mayor & City Council of Baltimore*, 682 F.3d 317, 320 (4th Cir. 2012) (citing *Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 849 (1998)).

Nothing of the sort occurred here. Treasury and OPM have merely provided agency employees access to digital systems that contain Plaintiffs' personal information. Notwithstanding

Plaintiffs' protestations that *these particular* federal employees should not be able to access Plaintiffs' information, and their speculation that such access may make that information more vulnerable to a hypothetical future breach, something so quotidian as intra-governmental information-sharing cannot colorably be classed among "the most egregious official conduct." *Id.* at 321 (quoting *Lewis*, 523 U.S. at 846). Accordingly, because Plaintiffs cannot show that Defendants "*intended to harm*" them, they cannot establish "conscience-shocking conduct . . . as would be necessary to establish a substantive due process violation." *Id.* at 322.[12]

II. Plaintiffs cannot satisfy the other preliminary injunction factors.

A. Plaintiffs cannot show irreparable harm.

"[F]or a preliminary injunction to issue, Plaintiffs must show they are 'likely to suffer irreparable harm in the absence of preliminary relief.'" *Roe*, 947 F.3d at 228 (quoting *Winter*, 555 U.S. at 20). Plaintiffs must make a "clear showing" that the irreparable injury is "likely" because "[i]ssuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with [the Supreme Court's] characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter*, 555 U.S. at 22. And "[t]o 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.'" *Mountain Valley Pipeline, LLC v. 6.56 Acres of Land*, 915 F.3d 197, 216 (4th Cir. 2019) (quoting *Direx Israel, Ltd. v. Breakthrough Med. Corp.*, 952 F.2d 802, 812 (4th Cir. 1991)).

For all of the reasons that Plaintiffs have failed to show cognizable injury for the purposes of Article III standing, they have necessarily failed to show any irreparable harm. The failure to

[12] Plaintiffs do not rely on their non-APA or common law ultra vires claim, *see* Compl. ¶¶ 123-28, in support of the TRO Motion. *See generally* Pls.' Mem.

make that showing by itself disposes of their motion. *Mountain Valley Pipeline*, 918 F.3d at 366 ("Each of these four requirements must be satisfied.").

Even if they had shown a cognizable injury, Plaintiffs nonetheless fail to make a clear showing of actual and imminent harm. Plaintiffs identify a *possibility* of harm from the alleged disclosure of their personal data. *See* Pls.' Mem. at 24 ("The longer Defendants are permitted unauthorized access to these sensitive systems, *the more likely it* is that they will access or further disclose Plaintiffs' individual data, and the longer Plaintiffs' data remains at a *heightened risk* of exposure or exfiltration by hostile actors.") (emphasis added). But they offer nothing to suggest that this "likel[ihood]" will come to pass at all, let alone actually and imminently. Speculation cannot form the basis for emergency injunctive relief, as the U.S. District Court for the District of Columbia held yesterday when addressing a similar claim against the Department of Education. *See* Mem. Op. & Order (ECF No. 20), *Univ. of Ca. Student Assoc. v. Carter*, et al., No. 1:25-cv-354 at 11-12 (D.D.C. Feb. 17, 2025 (Moss, J.) ("[Plaintiff] . . . cites no authority for the proposition that mere 'access' to personal data by government employees who are not formally authorized to view it, without more, creates an irreparable injury. . . . [Plaintiff] provides no evidence, beyond sheer speculation, that would allow the Court to infer that ED or DOGE staffers will misuse or further disseminate this information."). *See Winter*, 555 U.S. at 22 ("Issuing a preliminary injunction based only on a possibility of irreparable harm is inconsistent with our characterization of injunctive relief as an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief.").[13]

[13] To the extent that Plaintiffs contend that the claimed violation of their constitutional rights constitutes irreparable harm, Pls.' Mem. at 25-26, their failure to make out a viable due process claim defeats that argument, *see Miranda v. Garland*, 34 F.4th 338, 365 (4th Cir. 2022) ("Without [their] alleged constitutional injury, [Plaintiffs] . . . failed to show . . . irreparable harm.").

B. The balance of the equities and public interest weigh in Defendants' favor.

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). Neither the balance of the equities nor the public interest favors Plaintiff's request for preliminary relief.

Plaintiffs' argument for why the equities and the public interest fall in their favor largely collapse into the merits. They say that because the injunction is seeking to "end an unlawful practice," and the agency's action is "unlawful," its proposed injunction is proper. Pls.' Mem. at 27-28. To be clear, Defendants' practice is *not* unlawful, for the reasons stated above. Regardless, the Supreme Court has made clear that considering only likelihood of success is insufficient to justify injunctive relief. *See, e.g.*, *Winter*, 555 U.S. at 376-77 ("In each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief. In exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction.") (citations and quotation marks omitted).

The proposed injunction would harm the public interest. At its core, it would harm the public interest by limiting 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. It would also frustrate the President's ability to identify fraud, waste, and abuse throughout the government. *See* Krause Decl. ¶ 2. And it would draw false distinctions between different types of employees, unsupported in the statutory text, frustrating the flexibility that Congress provided through multiple avenues to federal employment.

Finally, denying Plaintiffs' request for emergency relief would not leave EPIC's members or Plaintiff Doe without remedy. If the government violates its legal obligations in a way that

meets the standards Congress articulated, those members can pursue monetary remedies under the Privacy Act or the Internal Revenue Code in the ordinary course, *see* 5 U.S.C. 552a(g)(4); 26 U.S.C. § 7431(a), which Plaintiffs already seek here, Compl. ¶¶ 112, 117.

C. If the Court grants the motion, it should enter a stay pending any appeal under Rule 62(c).

If the Court grants the Motion, it should enter a stay pending any appeal under Rule 62(c), which allows courts to stay injunctions pending appeals. Fed. R. Civ. P. 62(c). "'[T]he power to stay proceedings is incidental to the power inherent in every court to control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants.'" *Fraser v. Alcohol*, 2023 WL 5617894, at *2 (E.D. Va. Aug. 30, 2023) (quoting *Landis v. N. Am. Co.*, 299 U.S. 248, 254 (1936)). A stay pending appeal is "extraordinary relief." *Id*. (quotation marks and citation omitted). When determining if a stay pending appeal is appropriate, courts consider (1) whether the stay applicant has made a strong showing that he is likely to succeed on the merits, (2) whether the applicant will be irreparably injured absent a stay, (3) whether issuance of the stay will substantially injure the other parties interested in the proceeding, and (4) where the public interest lies. *Id*. (citing *Nken*, 556 U.S. at 426).

For all of the reasons set forth above, Defendants satisfy those factors.

CONCLUSION

The Court should deny Plaintiffs' Motion for a Temporary Restraining Order.

Dated: February 18, 2025

Respectfully submitted,

ERIK S. SIEBERT
UNITED STATES ATTORNEY

By: /s/ Jonathan T. Lucier
JONATHAN T. LUCIER, VSB No. 81303
Office of the United States Attorney
919 East Main Street, Suite 1900
Richmond, Virginia 23219
Tel.: (804) 819-5400
Fax: (804) 771-2316
Email: jonathan.lucier@usdoj.gov

PETER B. BAUMHART
Office of the United States Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel.: (703) 299-3738
Fax: (703) 299-3983
Email: Peter.Baumhart@usdoj.gov

BRETT A. SHUMATE
Acting Assistant Attorney General
Civil Division

MARCIA BERMAN
JOSEPH E. BORSON, VSB No. 85519
Assistant Directors
Federal Programs Branch

OLIVIA G. HORTON
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, NW
Washington, D.C. 20005
Tel.: (202) 305-0747
Email: olivia.g.horton@usdoj.gov

Attorneys for Defendants

CERTIFICATE OF SERVICE

I certify that on February 18, 2025, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/

Jonathan T. Lucier, VSB No. 81303
Attorney for Defendants
Office of the United States Attorney
919 East Main Street, Suite 1900
Richmond, Virginia 23219
Telephone: (804) 819-5400
Facsimile: (804) 771-2316
Email: jonathan.lucier@usdoj.gov