

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF
GOVERNMENT EMPLOYEES, AFL-CIO, *et al.*,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL
MANAGEMENT, *et al.*,

Defendants.

No. 25 Civ. 1237 (DLC)

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

MATTHEW PODOLSKY
Acting United States Attorney for the
Southern District of New York
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel.: (212) 637-2695/2772
Attorney for Defendants

JEFFREY OESTERICH
DAVID E. FARBER
Assistant United States Attorneys
- Of Counsel -

TABLE OF CONTENTS

TABLE OF AUTHORITIES..... ii

PRELIMINARY STATEMENT..... 1

BACKGROUND 2

 I. The United States DOGE Service..... 2

 II. Implementation of the USDS Executive Order at OPM..... 3

 III. This Litigation..... 4

STANDARD OF REVIEW 5

ARGUMENT..... 6

 I. Plaintiffs Lack Article III Standing..... 6

 A. Plaintiffs Fail to Establish a Cognizable Injury-in-fact 7

 B. Plaintiffs Fail to Establish Causation or Redressability..... 11

 II. A Temporary Restraining Order Is Unwarranted..... 13

 A. Plaintiffs’ Claims Are Not Reviewable Under the APA..... 14

 1. Plaintiffs have not identified the requisite final agency action..... 14

 2. Plaintiffs have an adequate, alternative remedy under the Privacy Act..... 16

 B. Plaintiffs Cannot Establish a Violation of the Privacy Act 19

 1. All of the individuals with access to OPM’s records systems who are advancing the USDS Executive Order are OPM employees. 20

 2. All of the individuals with access to OPM’s records systems who are advancing the USDS Executive Order have a need for access in the performance of their duties.... 22

 C. Defendants’ Actions Are Not *Ultra Vires*..... 23

 D. Plaintiffs Have Not Shown Irreparable Injury 24

 E. The Balance of the Equities Favors Defendants 25

 III. Plaintiffs’ Proposed Injunction Is Improper..... 26

CONCLUSION..... 27

TABLE OF AUTHORITIES

Cases	Pages(s)
<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015)	8
<i>AFL-CIO v. DOL</i> , No. 25 Civ. 339, Mem. Op. and Order (ECF No. 34) (D.D.C. Feb. 14, 2025).....	13, 22
<i>Apter v. HHS</i> , 80 F.4th 579 (5th Cir. 2023).....	23
<i>Arizona v. Biden</i> , 31 F.4th 469 (6th Cir. 2022).....	15
<i>Block v. Cmty. Nutrition Inst.</i> , 467 U.S. 340 (1984).....	17
<i>Bowen v. Massachusetts</i> , 487 U.S. 879 (1988).....	16
<i>Branch of Citibank, N.A. v. De Nevares</i> , 74 F.4th 8 (2d Cir. 2023).....	6
<i>Cell Assocs., Inc. v. NIH</i> , 579 F.2d 1155 (9th Cir. 1978).....	19
<i>Chrysler Corp. v. Brown</i> , 441 U.S. 281 (1979).....	14
<i>Citizens United to Protect Our Neighborhoods v. Vill. of Chestnut Ridge, New York</i> , 98 F.4th 386 (2d Cir. 2024).....	7
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	7, 11, 12
<i>Dew v. United States</i> , 192 F.3d 366 (2d Cir. 1999).....	17
<i>Doe v. Chao</i> , 435 F.3d 492 (4th Cir. 2006).....	18
<i>Doe v. DOJ</i> , 660 F. Supp. 2d 31 (D.D.C. 2009)	23
<i>Doe v. OPM</i> , No. 25 Civ. 234 (RDM), 2025 WL 513268 (D.D.C. Feb. 17, 2025)	9, 16
<i>Doe v. Stephens</i> , 851 F.2d 1457 (D.C. Cir. 1988)	18
<i>El Rio Santa Cruz Neighborhood Health Ctr. v. HHS</i> , 396 F.3d 1265 (D.C. Cir. 2005)	16
<i>FAA v. Cooper</i> , 566 U.S. 284 (2012).....	17, 18

Faiveley Transport Malmo AB v. Wabtec Corp.,
 559 F.3d 110 (2d Cir. 2009) 24

FDA v. Alliance for Hippocratic Med.,
 602 U.S. 367 (2024)..... 7, 11, 12

Freeman v. EPA,
 No. 02 Civ. 0387, 2004 WL 2451409 (D.D.C. Oct. 25, 2004) 21

Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.,
 460 F.3d 13 (D.C. Cir. 2006) 14

Garcia v. Vilsack,
 563 F.3d 519 (D.C. Cir. 2009) 16

Gazzola v. Hochul,
 88 F.4th 186 (2d Cir. 2023)..... 6

Geller v. de Blasio,
 613 F. Supp. 3d 742 (S.D.N.Y. 2020) (Cote, J.)..... 6

Gill v. Whitford,
 585 U.S. 48 (2018)..... 26

Judicial Watch v. Dep’t of Energy,
 412 F.3d 125 (D.C. Cir. 2005) 21

Local 1814, Int’l Longshoreman’s Ass’n, AFL-CIO v. N.Y. Shipping Ass’n,
 965 F.2d 1224 (2d Cir. 1992) 6

Lujan v. Defenders of Wildlife,
 504 U.S. 555 (1992)..... 6

Manning v. City of New York,
 No. 24 Civ. 4747 (LGS), 2024 WL 3377997 (S.D.N.Y. July 11, 2024) 6

Moore v. Consol. Edison Co. of N.Y.,
 409 F.3d 506 (2d Cir. 2005) 24

Munaf v. Geren,
 553 U.S. 674 (2008)..... 5

Murthy v. Missouri,
 603 U.S. 43 (2024)..... 12

Nat’l Sec. Sys., Inc. v. Iola,
 700 F.3d 65 (3d Cir. 2012) 16

New York ex rel. Schneiderman v. Actavis PLC,
 787 F.3d 638 (2d Cir. 2015) 24

Nken v. Holder,
 556 U.S. 418 (2009)..... 6, 25

Norton v. S. Utah Wilderness All.,
 542 U.S. 55 (2004)..... 14, 15

NYCLU v. New York City Transit Auth.,
 684 F.3d 286 (2d Cir. 2012) 7

Parks v. IRS,
 618 F.2d 677 (10th Cir. 1980)..... 18

Pearl River Union Free Sch. Dist. v. King,
 214 F. Supp. 3d 241 (S.D.N.Y. 2016) 14

Poss v. Kern,
 No. 23 Civ. 2199, 2024 WL 4286088 (D.D.C. Sept. 25, 2024)..... 18

Riddick v. Maurer,
 730 F. App’x 34 (2d Cir. 2018)..... 1

Salazar v. King,
 822 F.3d 61 (2d Cir. 2016) 14

Salazar v. Nat’l Basketball Ass’n,
 118 F.4th 533 (2d Cir. 2024) 8

Schneiter v. United States,
 159 Fed. Cl. 356 (2022) 11

Soundboard Ass’n v. FTC,
 888 F.3d 1261 (D.C. Cir. 2018) 15

Sprint Commc’ns Co. v. APCC Servs, Inc.,
 554 U.S. 269 (2008)..... 11

Sussman v. U.S. Marshal Serv.,
 494 F.3d 1106 (D.C. Cir. 2007)..... 18

TransUnion LLC v. Ramirez,
 594 U.S. 413 (2021)..... passim

Tripp v. DOD,
 193 F. Supp. 2d 229 (D.D.C. 2002) 18

U.S. Army Corps of Eng’rs v. Hawkes Co., Inc.,
 578 U.S. 590 (2016)..... 14, 15

Univ. of Cal. Student Assoc. v. Carter,
 No. 25 Civ. 354, Mem. Op. and Order (ECF No. 20) (D.D.C. Feb. 17, 2025)..... 13, 24

USPS v. Gregory,
 534 U.S. 1 (2001)..... 11

Warth v. Seldin,
 422 U.S. 490 (1975)..... 7

We The Patriots USA, Inc. v. Hochul,
 17 F.4th 266 (2d Cir. 2021)..... 5

Westcott v. McHugh,
 39 F. Supp. 3d 21 (D.D.C. 2014) 18

Winter v. Nat. Res. Def. Council, Inc.,
 555 U.S. 7 (2008)..... 5, 25

Statutes

5 U.S.C. § 2105(a)(1)..... 20
 5 U.S.C. § 3161..... 2
 5 U.S.C. § 552a..... 20
 5 U.S.C. § 552a(b)(1)..... 20, 22
 5 U.S.C. § 552a(e)(10)..... 15
 5 U.S.C. § 552a(g) 17, 18
 5 U.S.C. § 701(a)(2)..... 16
 5 U.S.C. § 704..... 14, 16
 31 U.S.C. § 1120(a)(1)..... 23
 Information Technology Modernization Centers of Excellence Program Act, Pub. L. 116-194,
 134 Stat. 981 (2020)..... 23
 National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1587..... 23

Other Authorities

Executive Order 14,158, 90 Fed. Reg. 8,441 (Jan. 20, 2025)..... passim
 Executive Order 14,170, 90 Fed. Reg. 8,621 (Jan. 20, 2025)..... 22
 Executive Order 14,210, 90 Fed. Reg. 9,669 (Feb. 11, 2025) 22
 GAO Report, “Priority Open Recommendations: Office of Personnel Management”
 (May 28, 2024)..... 3
 OPM, Information Technology Strategic Plan, Fiscal Years 2023-2026 4

Rules

Fed. R. Civ. P. 65(d)(1)(C)..... 26

Defendants the U.S. Office of Personnel Management (“OPM”); Charles Ezell, in his official capacity as Acting Director of OPM; U.S. DOGE Service (“USDS” or “DOGE”); the Acting USDS Administrator; U.S. DOGE Temporary Service; and Elon Musk, in his official capacity as Director of USDS submit this Memorandum in Opposition to Plaintiffs’ Motion for a Temporary Restraining Order¹ (ECF No. 27).

PRELIMINARY STATEMENT

Plaintiffs bring this lawsuit in the wake of several other suits making similar allegations of violations of the Privacy Act—suits that the government has defended in public filings in multiple courts. As with these other actions, Plaintiffs’ suit was prompted by erroneous information contained in news reports claiming that OPM is improperly disclosing sensitive data to DOGE staffers. Plaintiffs use that inaccurate information to demand a temporary restraining order (“TRO”) that would limit the Executive Branch’s ability to manage its own internal affairs, to exercise politically accountable oversight of agency activities, and to implement the Office of the President’s policy priorities. Contrary to the erroneous reporting on which Plaintiffs rely, all of the employees advancing the President’s DOGE priorities with access to OPM’s sensitive data systems are employees of OPM, none of the Defendants have made any public disclosure of sensitive personal records maintained by OPM, and Defendants have not violated the Privacy Act. Furthermore, even if such Privacy Act claims were viable, Plaintiffs do not have standing to raise them, and such claims are not cognizable under the Administrative Procedure Act (“APA”).

This Court should deny Plaintiffs’ request for a TRO because, as a threshold matter, they lack standing as they have not suffered a cognizable Article III injury, and they fail to sufficiently

¹ The Court should construe Plaintiffs’ motion as one for a preliminary injunction because notice and an opportunity to respond was given to Defendants, and Plaintiffs’ motion seeks much of the same relief requested in their underlying complaint. *See Riddick v. Maurer*, 730 F. App’x 34, 36 (2d Cir. 2018).

allege causation or redressability. In addition, none of the injunctive-relief factors weighs in favor of relief. *First*, Plaintiffs are unlikely to succeed on the merits of APA claims because they do not identify a final agency action, and they have adequate, alternative remedies under the Privacy Act. Likewise, Plaintiffs cannot show a Privacy Act violation in this case, as only authorized employees of OPM with a “need to know” have accessed sensitive personal information in OPM’s records systems. *Second*, Plaintiffs have not made a sufficient showing that they likely face imminent irreparable harm. *Finally*, both the equities and the public interest support permitting OPM to exercise its lawful authority to hire employees and give those employees access to its data systems as required for their job duties.

At bottom, Plaintiffs’ motion relies on one claim: that it is unlawful for OPM to grant its employees access to OPM records systems for the purpose of carrying out an Executive Order of the President. That claim cannot be correct, so their motion fails. For all of these reasons, Plaintiffs’ motion for a temporary restraining order should be denied.

BACKGROUND

I. The United States DOGE Service

On January 20, 2025, President Trump signed Executive Order 14,158, which directs changes to the previously established United States Digital Service in order 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. 8,441, § 4 (“USDS E.O.”). The USDS E.O. redesignated the United States Digital Service as the Department of Governmental Efficiency Service, or U.S. DOGE Service. *Id.* § 3(a). Similarly, it established a “U.S. DOGE Service Temporary Organization” within the Executive Office of the President pursuant to 5 U.S.C. § 3161, which will terminate on July 4, 2026. USDS E.O. § 3(b). Agency

heads are required under the USDS E.O. to establish within their respective agencies a USDS Team of at least four employees, which may include Special Government Employees. *Id.* § 3(c).

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

II. Implementation of the USDS Executive Order at OPM

OPM plays a critical role in overseeing and managing the federal workforce. *See* 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 modernization of technology, ensuring data integrity, and facilitating related workforce reforms. *Id.* ¶ 9.

With respect to OPM, the Government Accounting Office (“GAO”) has previously identified sixteen “priority recommendations” for improving OPM’s operations involving, among other things, “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 accessed Feb. 19, 2025). 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. OPM has previously acknowledged the need for modernization and innovation in its information technology

systems, noting that “the OPM legacy technology debt it has been carrying for years is a significant inhibitor to the agency’s ability to accomplish its . . . strategic goals.” OPM, Information Technology Strategic Plan, Fiscal Years 2023-2026, at 7, *available at* <https://www.opm.gov/about-us/reports-publications/2023-2026-information-technology-strategic-plan.pdf> (last accessed February 19, 2025).

All individuals with access to OPM records systems who are working to implement the USDS E.O. are employees of OPM. Hogan Decl. ¶ 13. They were all hired and onboarded directly by OPM. *Id.* ¶ 12. All such OPM employees who have participated in workforce reform, like all OPM employees, are subject to applicable privacy, ethics, and other requirements, *id.* ¶ 9, and all of the individuals implementing the USDS E.O. have completed appropriate ethics, records management, cybersecurity, or data privacy trainings, *id.* ¶ 13. Many OPM employees involved in these efforts hold policymaking, legal, or similar positions that do not require access to sensitive data systems. *Id.* ¶ 10. Each of OPM’s sensitive data systems requires authentication for internal access, and access is granted on a need-to-know basis. *Id.* ¶ 11. For systems engineers who require access to sensitive systems, such as the Electronic Official Personnel Folder (“eOPF”) and Enterprise Human Resources Integration (“EHRI”) systems, the Chief Information Office (“CIO”) will periodically review access permissions to ensure that they are limited to those with a need to know. *Id.* ¶ 12. For example, in early February, the CIO removed access to eOPF and EHRI for three engineers whose job duties do not require prospective access to those systems. *Id.*

III. This Litigation

Plaintiffs filed their Complaint in this matter on February 11, 2025. *See* ECF No. 1 (“Compl.”). The Complaint includes five claims for relief against all Defendants, all of which are premised on violations of the Privacy Act. Plaintiffs’ First and Second Claims for Relief assert claims under the Privacy Act itself, *id.* ¶¶ 47-59, their Third and Fourth Claims for Relief assert

claims under the APA that Defendants' actions violated the Privacy Act, *id.* ¶¶ 60-75, and their Fifth Claim for Relief asserts a claim that Defendants' actions were *ultra vires*, *id.* ¶¶ 76-84.

On February 14, 2025, Plaintiffs filed their Motion for a Temporary Restraining Order, ECF No. 27 ("Mot."), and Memorandum of Law in Support of Plaintiffs' Motion for a Temporary Restraining Order, ECF No. 28 (Pls' Mem."). Plaintiffs request that the Court temporarily enjoin Defendants (1) "from disclosing to DOGE-affiliated agents any OPM records[,] from granting DOGE-affiliated agents access to OPM's records[,] and from allowing such agents to obtain personal information about individual contained therein"; (2) "to ensure future disclosure of individual records will occur only in accordance with the Privacy Act"; (3) "to impound and destroy all copies of individuals' personal information that has been unlawfully disclosed by OPM," and (4) file a status report within 48 hours indicating whether "any DOGE-affiliated agents continue to have access to any OPM systems," and whether the DOGE Defendants have destroyed copies of individuals' personal information. Mot. at 1-2.²

STANDARD OF REVIEW

Issuance of a temporary restraining order or a preliminary injunction "is an 'extraordinary and drastic remedy' that is 'never awarded as of right.'" *We The Patriots USA, Inc. v. Hochul*, 17 F.4th 266, 279 (2d Cir. 2021) (quoting *Munaf v. Geren*, 553 U.S. 674, 689-90 (2008)). As such, it may "only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). To obtain this relief, a plaintiff "must establish [1] that he is likely to succeed on the merits, [2] he is likely to suffer irreparable harm in

² OPM is a defendant in multiple lawsuits alleging similar Privacy Act claims. In *Am. Fed. Of Teachers v. Bessent*, No. 25 Civ. 430 (D. Md.), OPM's opposition to an application for a TRO was filed on February 17, 2025. A hearing on the TRO in that matter was conducted earlier today. In *EPIC v. OPM*, No. 25 Civ. 255 (E.D. Va.), OPM's opposition to an application for a TRO was filed on February 18, 2025. A hearing on the TRO in that matter is scheduled for February 21, 2025.

the absence of preliminary relief, [3] that ‘the balance of equities tips in his favor, and [4] that an injunction is in the public interest.’” *Gazzola v. Hochul*, 88 F.4th 186, 194 (2d Cir. 2023) (quoting *Winter*, 555 U.S. at 20); *see also Geller v. de Blasio*, 613 F. Supp. 3d 742, 746 (S.D.N.Y. 2020) (Cote, J.) (“The standard for determining whether to grant a motion for a temporary restraining order is the same as used in evaluating a motion for a preliminary injunction.” (citing *Local 1814, Int’l Longshoreman’s Ass’n, AFL-CIO v. N.Y. Shipping Ass’n*, 965 F.2d 1224, 1228 (2d Cir. 1992))). When “the Government is the opposing party,” the assessment of “harm to the opposing party” and “the public interest” merge. *Nken v. Holder*, 556 U.S. 418, 435 (2009).

Plaintiffs bear the burden of showing subject-matter jurisdiction. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Because “standing is not dispensed in gross,” Plaintiffs must “demonstrate standing for each claim that they press and for each form of relief that they seek.” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021).

ARGUMENT

I. Plaintiffs Lack Article III Standing

At the outset, the Court should deny the request for a temporary restraining order because Plaintiffs lack standing. *See, e.g., Manning v. City of New York*, No. 24 Civ. 4747 (LGS), 2024 WL 3377997, at *2 (S.D.N.Y. July 11, 2024) (“Before addressing the merits of the TRO Application, the Court must evaluate whether it has subject matter jurisdiction.” (citing *Branch of Citibank, N.A. v. De Nevares*, 74 F.4th 8, 15 (2d Cir. 2023))). At its “irreducible constitutional minimum,” Article III standing requires a plaintiff, as the party invoking the Court’s jurisdiction, to establish three elements: (1) a concrete and particularized injury-in-fact, either actual or imminent, and not conjectural or hypothetical (2) a causal connection between the injury and defendants’ challenged conduct, and (3) a likelihood that the injury suffered will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560.

As organizations, the union Plaintiffs representing employees (“Plaintiff Unions”) must demonstrate Article III standing either in their own right or as a representative of their members. *See NYCLU v. New York City Transit Auth.*, 684 F.3d 286, 294 (2d Cir. 2012). Here, the Plaintiff Unions do not rely on alleged injury to the organizations themselves but instead cite to the privacy interests of their members. *See* Pls’ Mem. at 13-14. As a result, the Plaintiff Unions must demonstrate that their members would otherwise have standing to sue in their own right. *See, e.g., Citizens United to Protect Our Neighborhoods v. Vill. of Chestnut Ridge, New York*, 98 F.4th 386, 395 (2d Cir. 2024) (where no individual plaintiff has standing, organization’s claim to representational standing also fails).

A. Plaintiffs Fail to Establish a Cognizable Injury-in-fact

To establish standing, Plaintiffs must establish that they have suffered an injury-in-fact—“actual or imminent, not speculative” harm, “meaning that the injury must have already occurred or be likely to occur soon.” *FDA v. Alliance for Hippocratic Med.*, 602 U.S. 367, 381 (2024) (“*Alliance*”). If the injury has not come to pass, it 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 it must be “concrete—that is, real, and not abstract.” *TransUnion*, 594 U.S. at 424 (citations omitted).

Plaintiffs first assert that Defendants’ alleged “ongoing Privacy Act violations are themselves enough to confer standing.” Pl’s Mem. at 12; *see also id.* at 20-21. But that is incorrect. Plaintiffs’ claim that OPM is illegally disclosing information protected by the Privacy Act to DOGE (Pls’ Mem. at 12-13), is untrue, and Plaintiffs offer no factual support for that assertion. Indeed, OPM has only granted access to its protected records systems to authorized OPM employees with a need to know, as discussed *infra* at 17-21. 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 unauthorized access to OPM's systems *and* intra-governmental disclosure, Plaintiffs still fail to establish standing. This is because *non-public* disclosure does not give rise to an actual, concrete harm sufficient to establish standing. The Supreme Court has made clear that a statutory violation is not, by itself, a cognizable injury. *See TransUnion*, 594 U.S. at 426-27 (“under Article III, an injury in law is not an injury in fact”). 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). Plaintiffs whose information has not been publicly disclosed to third parties lack a “concrete” injury for purposes of standing. *Id.* at 434; *cf. Salazar v. Nat’l Basketball Ass’n*, 118 F.4th 533, 541 (2d Cir. 2024) (an “intangible harm that readily qualifies as concrete is the public disclosure of private facts”). The same is true here—even assuming Defendants were engaging in the intra-governmental disclosure of OPM records in violation of the Privacy Act (they are not), Plaintiffs’ information has not been *publicly* disclosed to third parties outside of the government. Plaintiffs’ citation (Pls’ Mem. at 13), to *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015), is not to the contrary. There, the Second Circuit found plaintiffs’ allegations that the government had engaged in the widespread seizure of phone records in violation of the Fourth Amendment sufficient to confer standing. *Id.* at 801. Here, Plaintiffs allege no such Fourth Amendment violation. As a result, Plaintiffs lack the requisite concrete injury necessary to confer standing.³

³ Plaintiffs’ argument that they are harmed due to a violation of their “reasonable expectation” that their personal information will be securely held “in accordance with governing law,” Pls’ Mem. at 20, is simply a repackaged allegation that Defendants have violated the Privacy Act. As noted, those allegations are untrue. *See infra* at 19-23. But in any event, the Supreme Court’s decision in *TransUnion* forecloses Plaintiffs’ standing arguments based on a violation of the Privacy Act or their reasonable expectations of privacy, absent public disclosure.

Plaintiffs' alternative argument that they are exposed to a risk of future harm fares no better. To "establish a sufficient risk of future harm to support Article III standing," Plaintiffs must demonstrate a "sufficient likelihood" that OPM "would otherwise intentionally or accidentally release their information to third parties." *TransUnion*, 594 U.S. at 437-38. Plaintiffs cannot meet this burden.

Plaintiffs' claimed harms amount to an allegation that intra-governmental access could put their personal information "at risk of being accessed by bad actors," which exposes them to "security risk," or that "DOGE could use improperly disclosed records to retaliate against" them. *See* Decl. of Somnattie Ramrup, (ECF No. 29) ¶¶ 8, 11; Decl. of Everett B. Kelley (ECF No. 30) ¶¶ 10-11; Decl. of Deborah Toussant (ECF No. 31) ¶¶ 5-6. In support of their risk of future harm argument, Plaintiffs have alleged that "new access makes [OPM's] record vulnerable to other attackers," and point to "cybersecurity threats," including the hacking of OPM's databases a decade ago, *see* Pls' Mem. at 2, 10-11, 13, 21; *see also* Compl. ¶¶ 42-43. But the assertion that OPM's systems are *now* more vulnerable to hacking by malevolent actors simply because new OPM employees have access to OPM's records systems is entirely conclusory and speculative.⁴ *See, e.g., Doe v. OPM*, No. 25 Civ. 234 (RDM), 2025 WL 513268, at *6 (D.D.C. Feb. 17, 2025) ("Plaintiffs must do more than point to a decade-old failure to protect sensitive data; they must show that OPM computer systems [accessed by new OPM employees] are at imminent risk of

⁴ For example, Plaintiffs claim that "DOGE's access has compromised the cybersecurity of Plaintiffs' personnel records, significantly heightening the risk that their information will be far more vulnerable to hacking, or that their personnel file will be compromised," Pls' Mem. at 21. However, in support of this assertion, they cite a news article concerning the allegations in the Complaint they themselves filed. *Id.* at 21 n.49; ECF No. 37-37.

cyberattack and that this risk would be mitigated were the agency required” to implement measures mandated by the Privacy Act).

Plaintiffs also assert that “DOGE is looking into the net worth of federal employees, but did not reveal how DOGE acquired the data,” Pls’ Mem. at 13, but they do not connect this assertion with any risk of exposure of sensitive personnel data in OPM’s records systems, which do not contain employees’ net worth information.⁵ Plaintiffs further assert that “DOGE has posted other sensitive information online,” Pls’ Mem. at 13;⁶ however, they do not explain how DOGE’s further publication of already publicly-available OPM datasets translates into an increased risk that sensitive personal data in OPM’s protected records systems will be exposed or somehow used against them. At bottom, Plaintiffs fail to explain how granting access to a limited number of new federal employees—all of whom are subject to applicable privacy, ethics, and other requirements and have undergone appropriate trainings, *see* Hogan Decl. ¶¶ 9, 13—somehow makes exposure of their sensitive data more likely. Accordingly, “[b]ecause no evidence in the record establishes a

⁵ Moreover, such information for certain federal employees is already accessible through public financial disclosure reports. *See, e.g.*, U.S. Office of Government Ethics (“OGE”), “Public Financial Disclosure Guide,” available at <https://www.oge.gov/web/278eGuide.nsf> (last accessed Feb. 19, 2025); *see also* OGE, “Officials’ Individual Disclosures Search Collection,” available at <https://www.oge.gov/web/oge.nsf/Officials%20Individual%20Disclosures%20Search%20Collection?OpenForm> (last accessed Feb. 19, 2025).

⁶ Plaintiffs cite to the DOGE website’s publication of summary workforce data for the National Reconnaissance Office, *see* DOGE, *Meet the U.S. Government: National Reconnaissance Office*, <https://doge.gov/workforce?orgId=cef54cef-6e43-486d-aa0a-b1a7d5841a72> (last accessed Feb. 19, 2025), as well as a news article claiming such information constituted “classified personnel data,” *see* Pls’ Mem. at 13 n.34; ECF No. 37-34. However, the summary workforce information on the DOGE website—including for the National Reconnaissance Office—comes from an OPM dataset that has been publicly-available since March 2024. *See* DOGE, *Meet the U.S. Government*, <https://doge.gov/workforce> (“All workforce data from the U.S. Office of Personnel Management as of March 2024”) (last accessed Feb. 19, 2025); *see also* OPM, *Raw Datasets: Datasets Available from OPM: FedScope Employment Cube* (March 2024), <https://www.opm.gov/data/datasets/> (last accessed Feb. 19, 2025).

serious likelihood of disclosure, [the Court] cannot simply presume a material risk of concrete harm.” *TransUnion*, 594 U.S. at 438 (internal quotation and citation omitted).

Plaintiffs’ claim that DOGE could improperly use sensitive OPM information to retaliate against them is similarly unfounded. As an initial matter, “a presumption of regularity attaches to the actions of Government agencies,” and officials, *USPS v. Gregory*, 534 U.S. 1, 10 (2001), and “a plaintiff who contends that agency officials acted [or will act] in bad faith must overcome [that] presumption of regularity in agency conduct.” *Schneiter v. United States*, 159 Fed. Cl. 356, 376 (2022) (citation omitted). Here, Plaintiffs make no showing that DOGE, or any other government officials for that matter, will engage in retaliation against them. In any event, their subjective “fears of hypothetical future harm that is not certainly impending,” are insufficient to confer standing. *Clapper*, 568 U.S. at 416.

B. Plaintiffs Fail to Establish Causation or Redressability

Plaintiffs also fail to establish the necessary elements of causation and redressability—that any alleged harm or risk of future harm is traceable to OPM employees having access to OPM’s own records systems. *See Alliance*, 602 U.S. at 380-81 (“The second and third standing requirements—causation and redressability—are often ‘flip sides of the same coin.’” (quoting *Sprint Commc’ns Co. v. APCC Servs, Inc.*, 554 U.S. 269, 288 (2008))). As an initial matter, Plaintiffs’ claims of ongoing harm rest on the incorrect assumption that unspecified “DOGE agents”—presumably, they mean non-OPM employees—have access to protected OPM data and the ability to alter existing employee records. That is incorrect. *See infra* at 18-22. Moreover, Plaintiffs do not sufficiently allege that any purported risk of future harm due to the potential compromise of their sensitive personal information is fairly traceable to the challenged conduct of Defendants.

Plaintiffs do not explain how, and indeed cannot show, that intra-governmental access by OPM employees, versed in the privacy concerns of the systems they access, will lead to the disclosure of personal information to extra-governmental actors or allow DOGE to engage in retaliation against them. For Plaintiffs' "security risk" theory to be correct, they would have to demonstrate: (1) that unauthorized intra-governmental access to OPM's records systems (which again, is not occurring) is likely to materially increase the risk of hacking, notwithstanding OPM's existing internal security controls and mitigation efforts (*see* Hogan Decl. ¶¶ 9-14); (2) that there will be a cybersecurity incident that will compromise OPM's information; (3) that the individual Plaintiffs' information specifically will be compromised; and (4) that compromise will cause the Plaintiffs cognizable harm. This "chain of causation is simply too attenuated." *Alliance*, 602 U.S. at 392; *Murthy v. Missouri*, 603 U.S. 43, 57 (2024) ("The one-step-removed, anticipatory nature of [plaintiffs'] alleged injuries" fails to satisfy standing), *remanded*, 114 F.4th 406 (5th Cir. 2024). Similarly, under Plaintiff's "risk of retaliation" theory, they would have to demonstrate that (1) despite OPM's existing internal security controls and mitigation efforts, Plaintiffs' sensitive personal information contained in OPM's records systems is likely to be disclosed outside of OPM to DOGE (which has not occurred); and (2) that unspecified DOGE employees are willing, able, and likely to target them for retaliation based on that sensitive personal information. Relying on such a "speculative chain of possibilities[, however,] does not establish that injury based on potential future [action] is certainly impending or is fairly traceable." *Clapper*, 568 U.S. at 414.

Indeed, Plaintiffs' assertion that access to OPM information by a limited number of OPM employees will likely result in the information being compromised by third-party bad actors or disclosed to other, unauthorized government employees is simply unfounded. Plaintiffs'

conclusory assertions that Defendants' actions *might* put their information at increased risk or *could* lead to retaliation is insufficient to confer standing.

II. A Temporary Restraining Order Is Unwarranted

As discussed above, the Court need not consider the merits of Plaintiffs' claims and may deny Plaintiffs' request for a temporary restraining order based on a lack of standing alone. To the extent the Court does reach the merits of Plaintiffs' claims, however, it should deny their request for a TRO. The same type of Privacy Act-based claims concerning disclosures to "DOGE-affiliated" federal employees have already been rejected multiple times by courts in other districts. *See, e.g.*, Mem. Op. and Order (ECF No. 20), *Univ. of Cal. Student Assoc. v. Carter*, No. 25 Civ. 354, (D.D.C. Feb. 17, 2025) (Moss, J.); Mem. Op. and Order (ECF No. 34), *AFL-CIO v. DOL*, No. 25 Civ. 339, (D.D.C. Feb. 14, 2025) (Bates, J.). This Court should similarly decline to grant the injunctive relief requested here.

First, Plaintiffs' claims are not reviewable under the APA due to lack of final agency action, and they have an adequate, alternative remedy under private rights of action provided by the Privacy Act. *Second*, Plaintiffs' entire theory rests on the erroneous premise that the individuals carrying out the USDS E.O. in these agencies are not employees of these agencies. In fact, they are employees of these agencies. What is more, they require access to large datasets (including material that may be covered by the Privacy Act) to carry out their (again, Presidentially-directed) functions. Plaintiffs have thus not established a likelihood of success on their theory that Defendants are acting *ultra vires* or in violation of the Privacy Act. *Finally*, Plaintiffs fail to establish either irreparable injury or that the balance of equities is in their favor. For these reasons, a temporary restraining order is not warranted.

A. Plaintiffs' Claims Are Not Reviewable Under the APA

Plaintiff's claim under the APA for violation of the Privacy Act fails because they have not alleged the requisite final agency action and they have other adequate alternative remedies. The APA does not permit "judicial review over everything done by an administrative agency." *Fund for Animals, Inc. v. U.S. Bureau of Land Mgmt.*, 460 F.3d 13, 19 (D.C. Cir. 2006) (quotation omitted). Rather, the cause of action that statute provides, 5 U.S.C. § 704, is limited in two ways material here. Agency action must be "final" to be reviewable. *Id.* And if there is an adequate alternative remedy, including a distinct statutory cause of action, the plaintiff must sue under the alternative instead. *See id.* Because Plaintiffs' claims do not satisfy either condition, they lack a cause of action under the APA.

1. Plaintiffs have not identified the requisite final agency action.

APA review is limited to "final agency action." *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 61-62 (2004) (quoting 5 U.S.C. § 704) ("*SUWA*"). Agency action is final only when it (1) "mark[s] the consummation of the agency's decisionmaking process" and (2) 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)). "The second prong will be satisfied where the agency's action 'gives rise to direct and appreciable legal consequences.'" *Pearl River Union Free Sch. Dist. v. King*, 214 F. Supp. 3d 241, 258 (S.D.N.Y. 2016) (quoting *Hawkes*, 578 U.S. at 598) (internal quotation and citation omitted). "The Supreme Court has interpreted the finality element in a pragmatic way." *Salazar v. King*, 822 F.3d 61, 82 (2d Cir. 2016) (internal quotation and citation omitted).

Plaintiffs attempt to meet this requirement by arguing that "[a] decision by an agency to 'disclose' a plaintiff[s] records is a 'reviewable agency action' that the court can enjoin." Pls' Mem. at 18 (quoting *Chrysler Corp. v. Brown*, 441 U.S. 281, 318-19 (1979)). But as Plaintiffs

concede, the sole case they identify involved public disclosure pursuant to a statutory process (FOIA) that specifically provides a mechanism for reviewing agency disclosure decisions *to the public*—not intra-agency access and disclosure consistent with ordinary agency operations. *See Chrysler Corp.*, 441 U.S. at 318.

Plaintiffs fail to articulate how providing a new employee with system access necessary to her functions “consummat[es]” OPM’s decisionmaking 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) (citation omitted). Nor is it apparent how the decision to grant new employees access to systems and the data therein has “direct and appreciable legal consequences” for anyone at all. *Cf. Arizona v. Biden*, 31 F.4th 469, 478 (6th Cir. 2022) (“training [and] reprioritization of employees” do not amount to direct and appreciable legal consequences). Instead, OPM’s discretionary decisions regarding which of its own employees are given access to its own internal records systems are precisely the day-to-day operation of governmental programs that are not subject to APA review. *SUWA*, 542 U.S. at 63-64. And to the extent Plaintiffs challenge the OPM’s grant of systems access to any employees implementing the President’s priorities in the USDS E.O. as not “justified,” Pls’ Mem. at 15, such “broad programmatic attack” similarly falls outside the ambit of judicial review under the APA. *SUWA*, 542 U.S. at 64.

Plaintiffs’ assertion that OPM violated the Privacy Act by providing access to its own employees without “establish[ing] appropriate security safeguards or training for new agents,” and without “properly vet[ting]” new these new employees, Pls’ Mem. at 17 (citing 5 U.S.C. § 552a(e)(10)), is similarly beyond the scope of APA review. As an initial matter, these conclusory assertions are incorrect—all of the relevant employees have undergone appropriate ethics, records

management, cybersecurity, or data privacy training, Hogan Decl. ¶ 13, and OPM regularly reviews access permissions for OPM data systems to ensure they are appropriately limited, *id.* ¶ 12. Moreover, the statute’s requirement to “establish *appropriate* administrative, technical, and physical safeguards to insure the security and confidentiality of records,” 5 U.S.C. § 552a(e)(10) (emphasis added), commits the determination of which measures to adopt to agency discretion by law, and thus places those measures outside the scope of review under the APA. *See* 5 U.S.C. § 701(a)(2) (no review under the APA where “agency action is committed to agency discretion by law”); *Nat’l Sec. Sys., Inc. v. Iola*, 700 F.3d 65, 101 (3d Cir. 2012) (“[T]he term “appropriate” [] confer[s] discretion.”). In the end, “it is not the job of the federal courts to police the security of the information systems in the executive branch,” *Doe v. OPM*, 2025 WL 513268, at *5.

2. Plaintiffs have an adequate, alternative remedy under the Privacy Act.

Plaintiffs’ APA claims fail for the additional, independent reason that the APA does not grant a cause of action where there is “[an]other adequate remedy in any court.” 5 U.S.C. § 704. This statutory provision “makes it clear that Congress did not intend the general grant of review in the APA to duplicate existing procedures for review of agency action.” *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988). Accordingly, a plaintiff has adequate relief—and thus cannot avail herself of § 704—“where a statute affords an opportunity for *de novo* district-court review’ of the agency action.” *Garcia v. Vilsack*, 563 F.3d 519, 522-23 (D.C. Cir. 2009) (quoting *El Rio Santa Cruz Neighborhood Health Ctr. v. HHS*, 396 F.3d 1265, 1270 (D.C. Cir. 2005)). Stated differently, where an agency action is subject to review in some manner under a statutory review scheme, then the general rule is that action must be reviewed within the confines of that scheme. The mode of review established by the statutory review scheme is presumed exclusive. This is true even where a statutory review scheme only provides for review of issues by certain parties; other parties are

presumptively precluded from obtaining review of those issues under the APA. *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 349 (1984) (“[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded.”); *see also Dew v. United States*, 192 F.3d 366, 372 (2d Cir. 1999).

That is the case here. The Privacy Act establishes “a comprehensive and detailed set of requirements” for federal agencies that maintain systems of records containing individuals’ personal information, *FAA v. Cooper*, 566 U.S. 284, 287 (2012), and authorizes adversely affected individuals to bring suit for violations of those requirements, 5 U.S.C. § 552a(g)(1)(D). Relief under the Privacy Act is carefully circumscribed. Civil remedies are available—and thus the United States’ sovereign immunity has been waived—in four circumstances: (1) when the agency “makes a determination . . . not to amend an individual’s record in accordance with his request,” (an “Amendment Action”), 5 U.S.C. § 552a(g)(1)(A), (2) when the agency refuses to comply with an individual’s request for access to her records, (an “Access Action”), *id.* § 552a(g)(1)(B), (3), when the agency fails to maintain an individual’s records “with such accuracy, relevance, timeliness, and completeness” as is necessary for a government action and “consequently a determination is made which is adverse to the individual,” (a “Benefits Action”), *id.* § 552a(g)(1)(C), or (4) where the government “fails to comply with any other provision of this section . . . in such a way as to have an adverse act on an individual,” (an “Other Action”), *id.* § 552a(g)(1)(D). For Benefits Actions or Other Actions, a plaintiff may be entitled to “actual damages sustained by the individual as a result of the refusal or failure,” subject to a \$1,000 statutory minimum, but only if the “agency acted in a manner which was intentional or willful” and if that plaintiff could prove “actual damages,” which is “limited to proven pecuniary or

economic harm.” *Cooper*, 566 U.S. at 291, 299. Indeed, Plaintiffs have asserted such damages claims in their own complaint. *See* Compl. ¶¶ 47-59.

Beyond these monetary damages, the Act allows for injunctive relief in only two narrow circumstances: (1) to order an agency to amend inaccurate, incomplete, irrelevant, or untimely records of an individual, 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). Injunctive relief, as various courts have recognized, is not available for any other situation arising out of the Privacy Act. *See, e.g., 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))); *Doe v. Chao*, 435 F.3d 492, 504 (4th Cir. 2006) (“[S]ubsection (g)(1)(D) of the Privacy Act does not allow courts to grant injunctive or declaratory relief.” (collecting cases)).

Given the Privacy Act’s comprehensive remedial scheme, courts have repeatedly recognized that “a plaintiff cannot bring an APA claim to obtain relief for an alleged Privacy Act violation.” *Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014); *see also Tripp v. DOD*, 193 F. Supp. 2d 229, 238 (D.D.C. 2002); *Poss v. Kern*, No. 23 Civ. 2199, 2024 WL 4286088, at *6 (D.D.C. Sept. 25, 2024) (citing cases). That is consistent with the principle that “[w]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, 684 (10th Cir. 1980)⁷ (citing *Cell Assocs.*,

⁷ In *Parks v. IRS*, the Court noted that the government defendants could not rely on an executive order promoting savings bond programs to show that disclosure of employees’ nonparticipation in savings bond programs contained in personnel files “was necessary to the performance of their duties,” in light of the fact that “Congress expressly held out nonparticipation in savings bond programs as an example of information not needed in the performance of federal employees’ regular duties.” 618 F.2d at 681 & n.1. In contrast, there is no congressional pronouncement that employees’ access to agency data systems for purposes of their modernization is not necessary to

Inc. v. NIH, 579 F.2d 1155, 1161-62 (9th Cir. 1978)). This is especially true with respect to the Privacy Act because Congress “link[ed] particular violations of the Act to particular remedies in a specific and detailed manner[,]” which “points to a conclusion that Congress did not intend to authorize the issuance of [other] injunctions.” *Cell Assocs.*, 579 F.2d at 1158-59.

Indeed, as the Ninth Circuit concluded in *Cell Associates*, were injunctive relief available for violations of the Privacy Act generally, “the detailed remedial scheme adopted by Congress would make little sense. We think it unlikely that Congress would have gone to the trouble of authorizing equitable relief for two forms of agency misconduct and monetary relief for all other forms if it had intended to make injunctions available across the board.” *Id.* at 1160. Plaintiffs’ efforts to obtain an agency-wide injunction on information access by channeling Privacy Act claims through the APA would be an end-run around these common-sense principles and should be rejected.

B. Plaintiffs Cannot Establish a Violation of the Privacy Act

Even assuming an agency’s compliance with the Privacy Act is reviewable under the APA (it is not), Plaintiffs are also unlikely to succeed in establishing that Defendants are violating their rights (or the rights of their members). Plaintiffs’ claims rest on the incorrect premise that individuals at OPM advancing the President’s priorities set forth in the USDS E.O. are *not* employees of that agency. *See* Pls’ Mot. at 15. That is simply incorrect. Indeed, all of the relevant individuals who have access to OPM’s records systems are employees of OPM. *See* Hogan Decl. ¶ 12. Moreover, Executive Order 14,158 provides that these individuals have a need for access to “all unclassified agency records, software systems, and IT systems” to perform their duties.

the performance of their duties. Indeed, Congress has repeatedly encouraged the modernization of the government’s information technology systems. *See infra* at n.9.

90 Fed. Reg. 8,441, § 4. As a result, Plaintiffs have not established a likelihood of success on the merits to warrant the extraordinary remedy of a temporary restraining order.

1. All of the individuals with access to OPM's records systems who are advancing the USDS Executive Order are OPM employees.

The Privacy Act, 5 U.S.C. § 552a, applies to certain types of protectable records stored by an agency. *See id.* § 552a(a). The statute allows disclosure of records within system of records “to those officers and employees which maintains the record who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). All of the individuals with access to OPM's records systems advancing the USDS E.O. are “employees of the agency which maintains the record”—i.e., OPM. *Id.*

In their Motion, Plaintiffs assert that “the DOGE agents who obtained the records are not employees of OPM.” Pls' Mot. at 15. They are wrong. All individuals with access to OPM's sensitive data systems were hired and onboarded by OPM. *See Hogan Decl.* ¶ 13. Moreover, the relevant employees working at OPM to implement the USDS E.O. easily satisfy 5 U.S.C. § 2105(a)(1)'s definition of “employee.” For 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.” 5 U.S.C. § 2105(a)(1). 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). All of the relevant employees have been appointed to their positions under federal law as they were onboarded directly by OPM. *Hogan Decl.* ¶ 13. All are “engaged in the performance of a Federal function under authority of . . . an Executive act,” i.e.,

implementing Executive Order 14,158. *Id.* And all are ultimately subject to the supervision of the senior leadership of OPM, in which they serve. *Id.* ¶¶ 13-14.

Some of these OPM employees are also detailed or have dual appointments at other agencies, but that does not change the analysis as to whether they are acting as employees of OPM when accessing OPM's records systems. With respect to the employment status of detailed employees, the D.C. Circuit has adopted a functional approach, 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 weigh in favor of these workers' status as employees of OPM. They are working on advancing the USDS E.O. at OPM, Hogan Decl. ¶ 13-14; they are subject to the applicable privacy requirements in their handling of OPM data, *id.* ¶ 14; they are under the supervision of senior OPM leadership when performing work at OPM, *id.*; they perform their OPM-related work on an OPM-issued laptop, *id.*; and they are prohibited from sharing any OPM data with their other employing agency pursuant to a memorandum of understanding between the agencies, *id.*; see also *Judicial Watch*, 412 F.3d at 131-32; *Freeman v. EPA*, No. 02 Civ. 0387, 2004 WL 2451409, at *4-5 (D.D.C. Oct. 25, 2004) (finding that disclosure of plaintiffs' drug testing schedules and results by EPA OIG to an EPA-hired DOD investigator did not violate Privacy Act because "according to the OMB 1975 Guidelines, an agency that hires a member of another agency to serve in a temporary task force or similar, cross-designated function can share otherwise protected information with that hired person and still satisfy exception (b)(1)"). Accordingly, all of the relevant employees with access to OPM's data systems—detailed or not—are employees of OPM, the agency that maintains the records at issue.

2. All of the individuals with access to OPM's records systems who are advancing the USDS Executive Order have a need for access in the performance of their duties.

Contrary to Plaintiffs' assertions (Pls' Mem. at 15), all of the relevant OPM employees also have the requisite "need for the record" under the Privacy Act. *See* 5 U.S.C. § 552a(b)(1). Executive Order 14,158 directs all agencies, including OPM, with assembling DOGE Teams tasked with implementing the President's priorities, including "improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." 90 Fed. Reg. 8,441, §§ 3(c), 4. The OPM employees on OPM's DOGE Team have a need for "full and prompt access to *all* unclassified agency records, software systems, and IT systems" to perform those duties. *Id.* § 4 (emphasis added). Indeed, the relevant OPM personnel need access to OPM's records systems to execute the directive to modernize those systems pursuant to the USDS E.O., as well as to engage in mandated technology-based and data-driven workplace reforms pursuant to Executive Orders 14,170 and 14,210.⁸ *See* Hogan Decl. ¶¶ 6, 8, 13. *Cf.* Mem. Op. and Order (ECF No. 34), *AFL-CIO v. DOL*, No. 25 Civ. 339, at 3-4, 8 (D.D.C. Feb. 14, 2025) (federal employees carrying out DOGE's mission pursuant to the USDS E.O. have a need for access to agency records in the performance of their duties under the Privacy Act).

In response, Plaintiffs assert that these "types of employees" typically do not have access to sensitive personal records, and their access to sensitive data systems is "broader in scope than what occurred in the past." Pls' Mem. at 15. But "[t]he need to know exemption is not limited only to officers and employees within a certain office within an agency rather than to officers and

⁸ Executive Order 14,170 tasks the Director of OPM, among others, with developing a federal hiring plan which, among other things, "integrate[s] modern technology to support the recruitment and selection process, including the use of data analytics to identify trends, gaps, and opportunities in hiring." 90 Fed. Reg. 8,621, § 2(b)(vi). Executive Order 14,210 tasks each agency with, among other things, "develop[ing] a data-driven plan, in consultation with its DOGE Team Lead, to ensure new career appointment hires are in highest-need areas." 90 Fed. Reg. 9,669, § 3(b).

employees of the entire agency.” *Doe v. DOJ*, 660 F. Supp. 2d 31, 46 (D.D.C. 2009) (internal quotation and citation omitted). Furthermore, OPM’s granting of access to its record systems to new “types” of employees in furtherance of the policies articulated in the President’s Executive Orders is clearly a justifiable reason for access to these records—and access to such records was specifically authorized by the President. *Cf. Collins v. Yellen*, 594 U.S. 220, 252 (2021) (emphasizing that “because the President, unlike agency officials, is elected” Presidential control “is essential to subject Executive Branch actions to a degree of electoral accountability”).⁹ Although the President’s policy choices may not be Plaintiffs’, that alone cannot be the basis to invalidate their implementation.

C. Defendants’ Actions Are Not *Ultra Vires*

Plaintiffs also purport to raise a freestanding *ultra vires* claim against Defendants, premised on disclosure of records to DOGE employees in violation of the Privacy Act. *See* Pls’ Mem. at 18-19. Even assuming the common-law *ultra vires* doctrine still exists in suits against the federal government, *but see Apter v. HHS*, 80 F.4th 579, 593 (5th Cir. 2023) (“Under our precedent, Congress apparently did away with the *ultra vires* doctrine and other fictions surrounding sovereign immunity when it amended the APA in 1976.” (cleaned up)), Plaintiffs concede that their *ultra vires* claim is coextensive with their alleged violation of the Privacy Act. *See* Pls’ Mem. at

⁹ The relevant employees’ need for access to these systems to further the priorities of the USDS E.O. also comports with legislative mandates to modernize the federal government’s information technology systems. *See, e.g.*, 31 U.S.C. § 1120(a)(1) (requiring “agencies to develop priority goals to improve the performance and management of the Federal Government,” including “information technology management”); National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1587 (authorizing agencies to establish “information system technology modernization and working capital fund[s]” to be used “to improve, retire, or replace existing information technology systems in the covered agency to enhance cybersecurity and to improve efficiency and effectiveness”); Information Technology Modernization Centers of Excellence Program Act, Pub. L. 116-194, 134 Stat. 981 (2020) (agencies required to develop plans “encouraging the modernization of information technology used by an executive agency and how a customer interacts with an executive agency”).

19. As discussed *supra*, this argument is based entirely on Plaintiffs' incorrect assumption that OPM granted access to OPM record systems to non-OPM employees. As such, this claim is unlikely to succeed, as well.

D. Plaintiffs Have Not Shown Irreparable Injury

“A showing of irreparable harm is the single most important prerequisite for the issuance of a preliminary injunction.” *Faiveley Transport Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quotation and citation omitted). Plaintiffs' motion should be denied because they have not demonstrated the “actual and imminent” injury that this Circuit requires to demonstrate irreparable injury. *Id.* Moreover, where, as here, “there is an adequate remedy at law, such as an award of money damages, injunctions are unavailable except in extraordinary circumstances.” *Moore v. Consol. Edison Co. of N.Y.*, 409 F.3d 506, 510 (2d Cir. 2005); accord *New York ex rel. Schneiderman v. Actavis PLC*, 787 F.3d 638, 660 (2d Cir. 2015) (“Irreparable harm is injury that is neither remote nor speculative, but actual and imminent and that cannot be remedied by an award of monetary damages.”).

Plaintiffs cannot establish irreparable injury, for themselves or their members. Their claims of irreparable injury rest largely on the same claims as their standing arguments. *See* Pls' Mem. at 19-22. As detailed above, these claims fail. No public disclosure has occurred nor have plaintiffs established one is imminent, and any increased threat of hacking due to access alone is wholly speculative. *See supra* at 7-11. Indeed, another court faced with similar claims of irreparable injury premised on alleged Privacy Act violations due to data access by “DOGE-affiliates” concluded that such access alone—devoid of allegations of unauthorized public disclosure—is insufficient to show irreparable injury warranting the imposition of a TRO. *See* Mem. Op. and Order (ECF No. 20), *Univ. of Cal. Student Assoc. v. Carter*, No. 25 Civ. 354, at 10-12 (D.D.C. Feb. 17, 2025) (Moss, J.). Nevertheless, assuming Plaintiffs could show some actual harm, they have an

adequate remedy at law—a cause of action for damages under the Privacy Act—which they have specifically asserted in their Complaint. *See id.* at 13; *see also supra* at 16-18; Compl. ¶ 53. As a result, this case does not present the requisite “extraordinary circumstances” warranting preliminary injunctive relief.

E. The Balance of the Equities Favors Defendants

The balance of the equities and the public interest “merge when the Government is the opposing party.” *Nken v. Holder*, 556 U.S. at 435. Neither the balance of the equities nor the public interest favors Plaintiffs’ request for preliminary relief.

Plaintiffs arguments on this factor largely collapse into the merits, relying on their purported “overwhelming likelihood of prevailing on the merits,” of their Privacy Act-based claims in asserting that an injunction is in the public interest. Pls’ Mem. at 22. However, Defendants have not engaged in violations of the Privacy Act, for the reasons stated above. *Supra* at 19-23. Regardless, considering only likelihood of success is insufficient to justify injunctive relief. *See, e.g., Winter*, 555 U.S. at 376-77. Plaintiffs also make the specious claim that “Defendants’ actions threaten national security by making OPM’s systems more vulnerable to cyberattacks by foreign adversaries and intelligence services.” Pls’ Mem. at 23 (citing to a 2016 House Report on the OPM data breach which occurred over a decade ago). As noted above, Plaintiffs’ claims of heightened security risks and vulnerabilities are wholly speculative. *See supra* at 9-11.

Instead, it is the proposed injunction that would harm the public interest. At its core, it would limit the government employees’ ability to effectuate the policy choices of the President by limiting his advisors and other employees’ ability to access information necessary to inform that policy. It would also frustrate the ability to identify fraud, waste, and abuse throughout the federal government and engage in federal workplace reform, in keeping with the President’s executive

orders. Simply put, the requested injunction would prevent federal employees from lawfully doing their jobs.

III. Plaintiffs' Proposed Injunction Is Improper

Plaintiffs' proposed injunction is also patently overbroad. Plaintiffs request, among other things, that the Court temporarily enjoin Defendants from granting access to or disclosing *any* non-public OPM records to unspecified "DOGE-affiliated agents." Mot. at 1-2; *see also* ECF No. 32 ("Proposed Order"). Plaintiffs do not define the term "DOGE-affiliated agents" anywhere in their submissions or Proposed Order (running afoul of the requirement that an injunction or restraining order describe in "reasonable detail" the acts restrained or required, *see* Fed. R. Civ. P. 65(d)(1)(C)); however, to the extent Plaintiffs seek to prevent any OPM employee (including those detailed to other agencies) working in furtherance of the USDS E.O. from accessing OPM records systems, their request is clearly improper. A prohibition on disclosure or access to "DOGE-affiliated agents" goes well beyond the protections of the Privacy Act, and would effectively prevent *all* OPM employees from accessing OPM's records systems to the extent they are furthering the implementation of the USDS E.O. or related executive orders. "A plaintiff's remedy must be tailored to redress the plaintiff's particular injury," *Gill v. Whitford*, 585 U.S. 48, 72-73 (2018), and such a sweeping ban on access to *all* non-public data systems maintained by OPM is in no way tailored to Plaintiffs' purported injuries in this case and would constitute a substantial and unwarranted intrusion on the work of OPM's employees.

CONCLUSION

For all of the foregoing reasons, the Court should deny Plaintiffs' motion for a temporary restraining order.

Dated: New York, New York
February 19, 2025

Respectfully submitted,

MATTHEW PODOLSKY
Acting United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David E. Farber
JEFFREY OESTERICH
DAVID E. FARBER
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel: (212) 637-2695/2772

CERTIFICATE OF COMPLIANCE

Pursuant to Local Civil Rule 7.1(c), the undersigned counsel hereby certifies that this memorandum complies with the word-count limitation of this Court's Local Civil Rules. As measured by the word processing system used to prepare it, this memorandum contains 8,668 words.

/s/ David E. Farber
Assistant United States Attorney