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 PRELIMINARY INJUNCTION

JAY CLAYTON
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 OESTERICHER
DAVID E. FARBER
Assistant United States Attorneys
- Of Counsel -

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

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 Preliminary Injunction (ECF No. 83).

PRELIMINARY STATEMENT

Plaintiffs' suit was prompted by erroneous information contained in news reports claiming that OPM is improperly disclosing sensitive data to DOGE staffers. Subsequently, OPM produced the administrative record in this case—conclusively showing that all of Plaintiffs' claims are incorrect. The record shows that all of the individuals granted access to OPM's system were properly vetted and duly appointed as OPM employees. The record shows that OPM utilizes robust, appropriate, and established safeguards to control account and access management relating to OPM's sensitive data systems, and that OPM consistently followed these safeguards in connection with the granting of access permissions to OPM data systems to individuals who onboarded on or after January 20, 2025. And there is no evidence that any OPM employees have improperly disclosed sensitive personal information to "DOGE," in violation of the Privacy Act. Despite this record evidence, Plaintiffs now seek to enjoin OPM from granting access to its data systems for *any* individual that is implementing the President's executive order to modernize government technology and software.

As a threshold matter, Plaintiffs' submissions in support of their motion rely heavily on inadmissible evidence that cannot be considered in connection with their request for a preliminary injunction. Rather than develop admissible evidence or cite to the administrative record, Plaintiffs instead reuse the same hearsay within hearsay that forms the basis of their Complaint. As a result, none of the injunctive-relief factors weigh in favor of preliminary relief. *First*, Plaintiffs have not

shown the requisite clear likelihood of success on the merits because (1) they fail to demonstrate they have standing to pursue their claims, (2) their claims are not reviewable under the APA because they do not challenge final agency action, but rather the internal, day-to-day operations of OPM, (3) they have not demonstrated any underlying violation of the Privacy Act, and (4) Plaintiffs offer no evidence that the DOGE Defendants had any involvement in this case at all, let alone that their actions were *ultra vires*. *Second*, Plaintiffs have not made a sufficient showing that they likely face imminent irreparable harm. *Finally*, both the equities and the public interest favor Defendants and 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.

For all of these reasons, Plaintiffs' motion for a preliminary injunction 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 U.S. 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," and "promot[ing] inter-operability between agency networks and systems, ensur[ing] data integrity, and facilitat[ing] responsible data collection and synchronization." 90 Fed. Reg. 8,441, § 4 ("USDS E.O."). The USDS E.O. specifically describes the "President's DOGE Agenda" as "modernizing Federal technology and software to maximize governmental efficiency and productivity." *Id.* § 1. The USDS E.O. renamed the U.S. Digital Service as the U.S. Department of Governmental Efficiency Service, or U.S. DOGE Service. *Id.* § 3(a).[1] It also established a "U.S. DOGE Service Temporary Organization"

[1] The U.S. Digital Service was established in 2014 by President Obama within the White House as a "team of America's best digital experts [who] will work in collaboration with other

within the Executive Office of the President pursuant to 5 U.S.C. § 3161, which will terminate on July 4, 2026. *See* USDS E.O. § 3(b). Agency heads are directed under the USDS E.O. to establish within their respective agencies a DOGE Team of at least four employees to implement the President's DOGE agenda. *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 agency heads 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.* In this way, USDS's mission is no different than when it was named the U.S. Digital Service.[2] USDS's employees—both then and now—are subject to the same restrictions and cannot access another agency's protected systems without following the requirements of the Privacy Act.

---

government agencies to make websites more consumer friendly, to identify and fix problems, and to help upgrade the government's technology infrastructure." *See* Obama White House Archive Press Release, *Fact Sheet: Improving and Simplifying Digital Services* (Aug. 11, 2014), *available at* https://obamawhitehouse.archives.gov/the-press-office/2014/08/11/fact-sheet-improving-and-simplifying-digital-services (last accessed May 16, 2025). The U.S. Digital Service utilized the "Digital Services Playbook," which included using "an incremental, fast-paced style of software development to reduce the risk of failure," and using "data to drive decisions," including "measuring how well a system performs and how people are interacting with it in real-time." *See* U.S. Digital Service, *Digital Service Playbook, available at* https://playbook.usds.gov/ (last accessed May 16, 2025).

[2] A report published in 2024 by the U.S. Digital Service notes that the Service had "collaborated with 31 federal agencies," and "partner[ed] with agencies by assigning small, interdisciplinary teams to work hand-in-hand with agency staff and contractors to deliver critical programs through technology and design." U.S. Digital Service, Impact Report at 2 (2024), *available at* https://www.usds.gov/resources/USDS-2024-Impact-Report.pdf (last accessed May 16, 2025). Moreover, the Service's portfolio included "rapid response" projects: "In response to urgent situations, USDS deploys teams quickly across the interagency to solve critical problems." *Id.*

II. The Vetting, Credentialing, and Onboarding of Certain OPM Employees[3]

In January 2025, in connection with the incoming presidential administration, several individuals were appointed at OPM in various roles. On January 20, 2025, Charles Ezell, a career OPM employee, was designated as Acting Director of OPM. That same day Gregory Hogan, James Sullivan, OPM-2, OPM-3, OPM-5, and OPM-7, were also appointed as OPM employees.[4] *See* Declaration of Carmen Garcia-Whiteside ("Garcia Decl."), ¶¶ 5-7, 10, 14-15. On January 20, 2025, Ezell selected Gregory Hogan as the agency's acting Chief Information Officer ("CIO"), and Hogan later assumed that position on a permanent basis. *Id.* ¶ 5. In addition, Amanda Scales was appointed as Chief of Staff to the OPM Director. On January 24, 2025, OPM-4 and OPM-6 were

[3] Plaintiffs claim that these individuals are "DOGE agents"—a term they have now redefined yet again in connection with their motion for a preliminary injunction. The term "DOGE agents" is not defined in Plaintiffs' Complaint. *See* ECF No. 1. In Plaintiffs' Opposition to the Motion to Dismiss, they maintained that their Complaint uses the terms "DOGE" and "DOGE agents" interchangeably, to collectively refer to USDS, the DOGE Service Temporary Organization, agencies' DOGE Teams, and employees who work principally on the DOGE agenda. *See* ECF No. 67 at 3 & n.3. In connection with their current motion, Plaintiffs define the term "DOGE agents" (in their proposed order) as "refer[ring] to individuals whose principal role is to implement the DOGE agenda as described in Executive Order 14,158 and who were granted access to agency systems of records for the principal purpose of implementing that agenda." ECF No. 89 n.3. That definition is apparently lifted from the definition of "DOGE affiliates" in footnote 1 of the opinion in *Am. Fed'n of Tchrs. v. Bessent*, No. 25 Civ. 0430 (DLB), 2025 WL 895326, at *2 n.1 (D. Md. Mar. 24, 2025), *stayed pending appeal,* 2025 WL 1023638, at *1 (4th Cir. Apr. 7, 2025). However, Plaintiffs fail to note that the term "does not include OPM's CIO Greg Hogan, OPM Acting Director Charles Ezell, or OPM Chief of Staff Amanda Scales, because these individuals, by virtue of their positions at OPM, would otherwise have access to OPM systems and were not granted access for the principal purpose of implementing the President's DOGE agenda." *Id.* at *4 n.3.

[4] This memorandum uses the anonymized monikers for certain OPM employees (*e.g.*, "OPM-2") consistent with the Court's orders. *See* ECF Nos. 66, 81. Citations to the filed OPM administrative record (ECF No. 78-2) are denoted by the prefix "OPM-000XXX" throughout. James Sullivan (OPM-8) was converted to a noncareer appointment as the Chief of Staff to the OPM Director on March 28, 2025. *See* Garcia Decl. ¶ 15. Given his current public-facing role, Defendants no longer refer to him using an anonymized moniker.

also appointed as OPM employees. *Id.* ¶ 9, 12.[5] Each of the OPM employees at issue was duly appointed as an employee of OPM according to established procedures and not detailed from another agency. *See id.* ¶ 20.

Each of the above OPM employees was also appropriately vetted and credentialed according to established and required procedures. *See* Declaration of Everette R. Hilliard ("Hilliard Decl."), ¶¶ 4-24. At no point did the career OPM personnel who performed the vetting and credentialing of these employees deviate from any of these required procedures in connection with the vetting and credentialing of these employees. *Id.* ¶ 24. Furthermore, at no point did anyone direct the career OPM personnel who performed this vetting and credentialing to deviate from required vetting and credentialing procedures. *Id.*

III. Implementation of the USDS Executive Order at OPM

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 May 16, 2025). In its report, GAO stated that "[f]ully implementing

[5] Defendants have not included onboarding, vetting, and credentialing documentation and information for OPM employees designated as OPM-9 through OPM-18 in the OPM administrative record, because as of March 6, 2025, none of these individuals had logged into, and thereby accessed, an OPM data system that would be subject to the Privacy Act. *See* Declaration of Gregory Hogan, dated May 16, 2025 ("Second Hogan Decl.") ¶ 11; OPM-000103. Moreover, these individuals do not fall within Plaintiffs' definition of "DOGE agents," because their "principal role" is not to further the "DOGE agenda"—*i.e.*, modernizing federal technology—and they were not granted access permissions for that purpose. *See supra* at 4 n.3. In addition, Defendants have not included such information for Acting Director Ezell and former Chief of Staff Scales "because these individuals, by virtue of their positions at OPM, would otherwise have access to OPM systems." *Am. Fed'n of Tchrs.*, 2025 WL 895326, at *4 n.3.

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 (June 2023), at 7, *available at* https://www.opm.gov/about-us/reports-publications/2023-2026-information-technology-strategic-plan.pdf (last accessed May 16, 2025).

OPM plays a critical role in overseeing and managing the federal workforce. *See* Declaration of Gregory Hogan, dated February 19, 2025 (ECF No. 40, "First 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. As part of OPM's role in furthering these initiatives, various OPM employees have been granted access permissions to OPM data systems.

OPM utilizes robust, appropriate, and established safeguards to control account and access management to OPM's sensitive data systems, including by implementing best practices established by the National Institute of Standards and Technology ("NIST"). *See* Second Hogan Decl. ¶¶ 5-10. Access to the vast majority of OPM's data systems is only possible through Microsoft Entra ID, which provides for multi-factor authentication—requiring an individual to utilize an OPM-issued personal identity verification ("PIV") credential or similar temporary LAN card, along with their personal identification number, and utilizing a card reader on government-furnished equipment (*e.g.*, a laptop). *Id.* ¶¶ 5-6; *see also* OPM-000163. In addition, OPM utilizes

Entra ID to implement role-based access control, granting users varying levels of permissions to access its sensitive OPM data systems, based on the user's need for access. *Id.* ¶ 7. OPM has also adhered to NIST best practices by periodically reviewing access permissions to ensure that they are limited to those with a need to know. *Id.* ¶ 10.

OPM has consistently implemented these safeguards in connection with the granting of access permissions to OPM data systems to individuals who onboarded on or after January 20, 2025. *Id.* ¶ 15. The administrative record shows that Acting Director Ezell requested that the Associate CIO (a career OPM employee) provide administrative access permissions to six OPM employees—including himself, Scales, Hogan, OPM-2, OPM-5, and OPM-7—for several OPM data systems, including USAJOBS and USA Staffing, *see* OPM-000107-08. OPM's Associate CIO authorized the request and administrative access permissions were granted to those six individuals for those systems. *See* OPM-000108, OPM-000103. On January 27, 2025, Acting Director Ezell requested that the Associate CIO provide similar administrative access to three additional OPM employees—OPM-3, OPM-4, and OPM-6—for certain OPM data systems, including USAJOBS, USA Staffing, and EHRI; and the Associate CIO approved the request and administrative access permissions were granted to those three individuals for those systems. *See* OPM-000028-29, OPM-000103. On February 3, 2025, Chief of Staff Scales requested administrative access for James Sullivan for the USA Staffing system, OPM's Associate CIO similarly approved the request, and administrative access permission was granted to Sullivan. *See* OPM-000110, OPM-000103.[6]

[6] Seventeen individuals were also granted "admin access" permissions for the USA Performance System, including individuals identified as OPM-9 through OPM-18. *See* OPM-000103. But the granting of elevated permissions to an individual to access a specific system does not mean that such individual actually created an account or logged in and accessed any data in that OPM data system. *See* Second Hogan Decl. ¶ 9. None of these individuals (except for CIO Hogan) had actually logged into the USA Performance system as of March 6, 2025. *See id.* ¶ 13; OPM-000103.

Despite the grant of administrative access permissions—*i.e.*, account creation—to these individuals to various OPM data systems, the *only* OPM data system which any of the relevant individuals actually logged into prior to March 6, 2025, was the USA Staffing platform. *See* Second Hogan Decl. ¶ 14; OPM-000103 (showing only four individuals logged into USA Staffing—Scales, Sullivan, OPM-6, and OPM-7). The USA Staffing system, among other things, automates the hiring and onboarding process for many federal agencies and allows them to develop and post job opportunity announcements. *See* Noble Decl. (ECF No. 85), Ex. L at 2-3 (USA Staffing Privacy Impact Assessment). These individuals were granted administrative access to the USA Staffing system so that they could make system changes to automated hiring/onboarding and job posting processes, and develop a data-driven hiring plan, in furtherance of the President's executive orders. *See* Second Hogan Decl. ¶ 14.

IV. This Litigation

Plaintiffs filed their Complaint in this matter on February 11, 2025. *See* ECF No. 1. On April 23, 2025, Defendants filed the OPM administrative record in this matter. ECF No. 78-2 (redacted), and ECF No. 80 (unredacted, under seal). Plaintiffs have not sought leave to amend the Complaint or renew their request for expedited discovery. *See* ECF Nos. 75 & 77.

On April 25, 2025, Plaintiffs filed their Motion for a Preliminary Injunction, ECF No. 83 ("Mot."), and Memorandum of Law in Support of Plaintiffs' Motion for a Preliminary Injunction, ECF No. 84 ("Pls' Br."). Plaintiffs request, among other things, that the Court enjoin Defendants (1) "from disclosing to DOGE Defendants, including all DOGE agents, any OPM records, as defined by the Privacy Act; from granting DOGE Defendants, including all DOGE agents, access to OPM's records; and from allowing such Defendants and agents to obtain personal information contained in those records of Plaintiffs and members of Plaintiff organization"; (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 Plaintiffs' and union Plaintiffs' members' personal information that OPM has disclosed to [DOGE Defendants and DOGE agents]," and (4) "to establish appropriate safeguards to ensure the security and confidentiality of Plaintiffs' and union Plaintiffs' members' records and to protect against any anticipated threats or hazards to their security or integrity, including, but not limited to, the security risks created by DOGE agents' access." Mot. at 1-2.

STANDARD OF REVIEW

A preliminary injunction is an "extraordinary and drastic remedy" that "should not be granted unless the movant, by a clear showing, carries the burden of persuasion." *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) (per curiam); *accord Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008); *We The Patriots USA, Inc. v. Hochul*, 17 F.4th 266, 279 (2d Cir. 2021). To obtain preliminary injunctive relief, a plaintiff "'must establish [1] that he is likely to succeed on the merits, [2] he is likely to suffer irreparable harm in 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). When "the Government is the opposing party," the assessments of "harm to the opposing party" and "the public interest" merge. *Nken v. Holder*, 556 U.S. 418, 435 (2009).

Where, as here, a movant seeks "to modify the status quo by virtue of a 'mandatory preliminary injunction' (as opposed to seeking a 'prohibitory preliminary injunction' to maintain the status quo)," the "standard for obtaining preliminary injunctive relief is higher." *A.H. by & through Hester v. French*, 985 F.3d 165, 176 (2d Cir. 2021) (quoting *Yang v. Kosinski*, 960 F.3d 119, 127 (2d Cir. 2020)). "In this circumstance, the movant must . . . make a strong showing of

irreparable harm and demonstrate a clear or substantial likelihood of success on the merits." *Id.* (quotation marks omitted).

ARGUMENT

Plaintiffs are not entitled to preliminary injunctive relief because they do not make a clear showing that they are likely to succeed on the merits, that they will be irreparably harmed absent an injunction, or that the balance of equities and the public interest weigh in their favor.

I. Plaintiffs Do Not Demonstrate a Likelihood of Success on the Merits

Plaintiffs have not shown a substantial likelihood of success on the merits because they fail sufficiently to demonstrate they have standing to pursue their claims, the Court lacks subject matter jurisdiction because Plaintiffs do not challenge final agency action, they have not established any underlying violation of the Privacy Act, and Plaintiffs offer no evidence that the DOGE Defendants had any involvement in this case at all, let alone that their actions were *ultra vires.*

A. Plaintiffs Fail to Demonstrate Article III Standing[7]

At the outset, the Court should deny the request for a preliminary injunction because Plaintiffs have not demonstrated the requisite standing to pursue their claims. 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 v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992).

[7] The "likelihood of success on the merits" factor includes both the merits of the underlying claims and jurisdictional issues. *See Murthy v. Missouri*, 603 U.S. 43, 58 (2024); *see also Munaf v. Geren*, 553 U.S. 674, 690 (2008) (noting that when considering "likelihood of success on the merits" for a preliminary injunction, jurisdictional "impediments" "mak[e] such success more unlikely").

While this Court previously determined that the Complaint sufficiently alleged facts to establish standing in connection with Defendants' motion to dismiss, *see* ECF No. 72, at 17-25, Plaintiffs must demonstrate standing at each stage of the litigation with an increasing burden of proof. "When a preliminary injunction is sought, a plaintiff's burden to demonstrate standing will normally be no less than that required on a motion for summary judgment." *Do No Harm v. Pfizer Inc.*, 126 F.4th 109, 119 (2d Cir. 2025) (internal quotation and citation omitted). "Consequently, to establish standing for a preliminary injunction, a plaintiff cannot rest on such mere allegations as would be appropriate at the pleading stage but must set forth by affidavit or other evidence specific facts, which for purposes of the summary judgment motion will be taken to be true." *Id.* (internal quotation and citation omitted). Pursuant to Federal Rule of Civil Procedure 56(c)(4), a declaration filed in support of such a motion "must be made on personal knowledge, set out facts that would be admissible in evidence, and show that the affiant or declarant is competent to testify on the matters stated."

Plaintiffs have failed to meet their burden of demonstrating standing pursuant to this rigorous standard because most of their proffered "evidence" would not be admissible. The newspaper articles, blog posts, and various letters from Congressmen or former USDS employees, all of which form the basis for Plaintiffs' claim that OPM provided "sweeping and uncontrolled access to DOGE agents who were not properly vetted or trained," Pls' Br. at 12 (quoting ECF No. 72 at 23), may not be considered to demonstrate standing in connection with their motion for a preliminary injunction. *See, e.g.,* Noble Decl., Exs. G, H, M, N, P (attaching news articles and letters).[8] Similarly, Plaintiffs' purported expert declarations concerning the vetting, training,

[8] "It is well-established that newspaper articles offered for the truth of the matters asserted therein are inadmissible hearsay that may not be considered by the Court in deciding a motion for summary judgment." *Outerbridge v. City of New York*, No. 13 Civ. 5459 (AT)(DCF), 2015 WL 5813387,

access controls, oversight, and level of access they believe was granted to "DOGE agents,"—none of which cite to a single page of the OPM administrative record—are not based on personal knowledge and do not set out facts that would be admissible in evidence. *See, e.g.,* Lewis Decl. (ECF No. 86), ¶ 6; Nesting Decl. (ECF No. 87) ¶ 37; Schneier Decl. (ECF No. 88), ¶ 5.[9] Furthermore, Plaintiffs may not rely on the unsupported allegations in their Complaint to satisfy their burden to demonstrate standing, and thus their repeated citations to the Court's Order on the Motion to Dismiss (ECF No. 72) are similarly unavailing. *See, e.g.,* Pls' Br. at 10-13.

In contrast, the administrative record and OPM's declarants show that OPM properly vetted, credentialed, and appointed each of the OPM "DOGE agents" at issue. *See supra* at 4-5; Hilliard Decl. ¶ 24; Garcia Decl. ¶ 20. The record also shows that no "DOGE agents *demanded* immediate access to OPM records," Pls' Br. at 11 (emphasis added), but rather that new OPM officials requested access to relevant OPM data systems, and OPM career officials authorized that access, *see supra* at 7. Plaintiffs effectively concede as much. *See* Pls' Br. at 7 ("Amanda Scales requested that another DOGE engineer, OPM-8, receive 'admin access' . . ."), and 17 ("Ezell requested—and obtained—comprehensive access . . ."). The actual evidence in the record thus

---

at *4 (S.D.N.Y. Sept. 30, 2015) (cleaned up and citations omitted). Courts refuse to consider the content of news articles for their truth in connection with a motion for a preliminary injunction. *See, e.g., Aptive Env't, LLC v. Vill. of E. Rockaway*, No. 19 Civ. 3365 (SJF)(SIL), 2019 WL 3206132, at *2 n.2 (E.D.N.Y. July 16, 2019) (citations omitted).

[9] The Schneier Declaration embodies multiple levels of hearsay within hearsay by routinely citing to unverified and inadmissible news reports, letters, and other materials that themselves would be inadmissible. *See* ECF No. 88. For example, to support his assertion that "other DOGE engineers obtained access to OPM's records before the agency confirmed that they had government-issued computers and before they had been vetted in accordance with longstanding agency practices," Schneier cites to a blog post reporting on the filing of Plaintiffs' complaint in this action. *See* Schneier Decl. ¶ 10 n.2 (citing to TechCrunch blog post).

disproves the "core contention of the complaint that OPM did not adhere to its 'existing internal security controls'" when granting access to OPM "DOGE agents." ECF No. 72 at 26.

1. Plaintiffs Fail to Establish a Cognizable Injury-in-Fact Based on Intrusion Upon Seclusion

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). Plaintiffs have failed to demonstrate, under the more exacting standard required at this stage of the litigation, that Defendants' actions are similar to the common law tort of intrusion upon seclusion. In fact, the record evidence shows that the majority of the so-called "DOGE agents" did not actually access *any* sensitive OPM data systems, let alone review the sensitive personal information of the individual Plaintiffs.

Plaintiffs' claim that individuals were granted access "to at least 14 OPM systems," Pls' Br. at 11, is correct to the extent that several new OPM employees were granted access *permissions* to 14 OPM data systems. *See* OPM-000103. But the record shows that, other than CIO Hogan, *only four* of the OPM "DOGE agents"—all of whom were properly vetted, credentialed, and appointed at OPM—actually logged into *a single* OPM data system prior to March 6, 2025. *See supra* at 8; Second Hogan Decl. ¶¶ 13-14; OPM-000103 (showing only four individuals logged into USA Staffing). And there is no evidence that those individuals used that access to review Plaintiffs' or anyone else's sensitive personal information. Undeterred by this record evidence, Plaintiffs claim "there is evidence of actual use in further violation of the [Privacy Act]," pointing to inadmissible hearsay in Congressional letters, blog posts, and one of their expert declarations in support of this

claim. Pls' Br. at 14.[10] They also note that "OPM described using the EHRI and eOPF databases to create [the Government-Wide Email System ("GWES")]," Pls' Br. at 14 (citing OPM-000119), in support of the assertion of actual use. However, they ignore that none of the supposed "DOGE agents" at OPM even logged into EHRI or eOPF prior to March 6, 2025. *See* Second Hogan Decl. ¶ 11; OPM-000103. As CIO Hogan has explained, while the government email addresses and names in the GWES do come from EHRI and eOPF, these two data elements do not contain personal information about an individual beyond their name. Second Hogan Decl. ¶ 12. Accordingly, these data elements are not "records" within the meaning of the Privacy Act, and their use does not violate the statute. *See* 5 U.S.C. § 552a(a)(4) ("record" means any item or information "about an individual" that also "contains his name" or "other identifying particular"); *see also Bechhoefer v. U.S. Dep't of Just. D.E.A.*, 209 F.3d 57, 62 (2d Cir. 2000) (term "record" under the Privacy Act, means "any personal information about an individual that is linked to that individual through an identifying particular" (citation and quotation omitted)).[11] Furthermore,

[10] Plaintiffs cite to a letter from two Congressmen to the Acting Director of OPM, *id.* at 14 n.23 (Noble Decl., Ex. M), a blog post on the site "Musk Watch," *id.* at 14 n.24 (Nobel Decl., Ex. N), and their declarant Ann Lewis, *id.* at 14. But these sources represent *multiple* levels of hearsay within hearsay, and clearly cannot be used to carry their burden on this motion for a preliminary injunction. *See Do No Harm*, 126 F.4th at 119.

[11] The domain of government email addresses could be used to determine the agency at which an individual is employed (*e.g.*, @doj.gov)—however, that an individual is employed by a particular agency is not "personal information" about that individual comparable to, *e.g.*, their home address or personal contact information. *See, e.g., Bloche v. DoD*, 370 F. Supp. 3d 40, 59 (D.D.C. 2019) (suggesting "the domain part of a government email address" does not implicate personal privacy interests); *Cf. Bechhoefer*, 209 F.3d at 61 (federal civil service employees' home addresses are "records" within meaning of the Privacy Act). Even if a government email address were a "record" for purposes of the Privacy Act, disclosure in this instance would be permissible under 5 U.S.C. § 552a(b)(1) because the records were disclosed to OPM employees who had a need for the record in the performance of their duties—*i.e.*, to create the GWES. Moreover, the disclosure would arguably be permissible under 5 U.S.C. § 552a(b)(3) because it would be for a routine use listed in the GOVT-1 System of Records Notice. *See* 77 Fed. Reg. 73697 (routine use "s" provides that records may be used "by the OPM to locate individuals for personnel research or survey response"). OPM has utilized this same name and email information from EHRI, as well as

those data elements were supplied by career OPM staff who extracted them from the EHRI data warehouse—not by supposed "DOGE agents." *See* Second Hogan Decl. ¶ 12. Simply put, there is no evidence that OPM "DOGE agents" exploited access permissions to OPM data systems in violation of the Privacy Act.

Setting aside the fact that there is no evidence that any of the OPM "DOGE agents" actually used or reviewed any of the individual Plaintiffs' sensitive data, the tort of intrusion upon seclusion is not satisfied by the simple grant of access permissions, without any of those individuals actually logging into those systems. That is because the tort requires an actual "intrusion," not mere opportunity. *Cf.* ECF No. 72 at (finding complaint plausibly alleged that DOGE agents "entered six OPM systems").[12] The record shows that the only possible "intrusion" in this case was the actual access to the USA Performance system by CIO Hogan, and actual access to the USA Staffing system by four individuals—the former Chief of Staff (Scales), the current Chief of Staff (Sullivan), a Senior Advisor to the Director of OPM (OPM-7), and an expert engineer (OPM-6). *See* Second Hogan Decl. ¶ 13-14; OPM-000103.

The evidence in the record further shows that any "intrusion"—whether viewed as the grant of access permissions alone, or actual access by these five OPM employees to OPM data systems—

---

additional personal data such as social security numbers and birthdates, in the past to implement the Federal Employment Viewpoint Survey ("FEVS"), an annual survey sent by email to all federal government employees. *See, e.g.*, 82 Fed. Reg. 57489 ("In order to administer the FEVS, information about Federal employees is collected from OPM's Enterprise Human Resource Integration (EHRI) system, consistent with the OPM/Govt 1 General Personnel Records system of records.").

[12] Put another way, being granted access permissions without actually logging into those systems is akin to setting up a tape recorder, but never pressing "record." *Cf.* ECF No. 72 at 16-17 (for purposes of intrusion upon seclusion "liability could arise from a defendant setting up a recording device, pressing 'record,' and doing nothing more" (citing *Caro v. Weintraub*, 618 F.3d 94, 101 (2d Cir. 2010))).

was not "highly offensive to a reasonable person," as required to show an intrusion upon seclusion. *See* Restatement (Second) of Torts § 625B (Am. L. Inst. 1977). Contrary to Plaintiffs' assertion that access was granted "to DOGE agents in a rushed and insecure manner that departed substantially from OPM's normal practices," Pls' Br. at 11 (quoting ECF No. 72 at 17), the record shows that OPM properly vetted, credentialed, and appointed each of the relevant "DOGE agents" at issue. *See supra* at 4-5. The career OPM employees in OPM's Personnel Security Division implemented every required procedure in vetting and credentialing each of these new OPM employees, and "at no point did anyone direct [them] to deviate from these established vetting and credentialing procedures." *See* Hilliard Decl. ¶ 24. The record further disproves Plaintiffs' assertion that these individuals are not actually employees "of the" OPM. *See* Pls' Br. at 15-17. Each of these employees was duly appointed as an employee of OPM according to established procedures. *See* Garcia Decl. ¶ 20.

2. Plaintiffs Fail to Establish a Sufficient Risk of Future Harm

Plaintiffs have similarly failed to demonstrate standing based on a risk of future harm. 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 erroneously assert that "the current record also 'shows a risk of future harm exists and that the risk is substantial.'" Pls' Br. at 12 (quoting ECF No. 72 at 23). In support, they cite to their purported experts' declarations, *id.* at 13, but as noted above, those declarations represent inadmissible hearsay within hearsay, and as detailed below, these experts' opinions as to a risk of future harm are untethered to *any* evidence in the actual record.

Plaintiffs' expert Ann Lewis states that she "understand[s] that several DOGE personnel"—whom she does not identify—have "administrator access" to all OPM technology systems, which

she claims gives them the "highest and most powerful level of access to any system." Lewis Decl. ¶¶ 7-8. Lewis goes on to claim that these "DOGE personnel" at OPM thus "can not only export all data but can also disable tracking and audit logging critical to forensic analysis." *Id.* ¶ 17. None of these statements are supported by any citation to record evidence, and they are entirely incorrect. As OPM's CIO explains, the term "administrator access" means that an "individual was assigned to a role with permissions allowing them to perform certain functions that a regular user would not be able to perform—and the types of functions authorized vary depending on the particular role at issue." Second Hogan Decl. ¶ 10. That an individual was granted "administrator access" does not mean that individual has the "highest and most powerful level of access" to a data system. *Id.* And it does not mean that a user with such access can necessarily (1) permanently delete critical data owned by and affecting other users, (2) disable, modify, or destroy data backups, (3) disable logging or audit trails used to conduct forensic analysis, or (4) take OPM's data systems fully offline. *Id.* Furthermore, no one at OPM has taken the above actions, or even requested that they be taken. *Id.*

Plaintiffs' expert Bruce Schneier states that it is his opinion "that imminent risks of significant harm exist … as a result of the access to OPM systems given to personnel of the newly created Department of Government Efficiency (DOGE)." Schneier Decl. ¶ 5.[13] He claims, without citation, that "[p]eople associated with DOGE have been granted full administrative access to [OPM] systems, which allows them to make changes without the protection provided by a

[13] Schneier also claims, in conclusory fashion, that OPM CIO Greg Hogan does not have the necessary experience because he "has been at OPM less than four months and was not previously in governmental service," and "his familiarity with OPM systems is likely not deep." *Id.* ¶ 9. Schneier himself has never worked at OPM, appears to have no relevant knowledge of OPM's vetting, credentialing, onboarding, oversight, and account and access management procedures, and last worked for the government in 1990. *See* Schneier Decl., Ex. A (resume).

separation of duties protocol." *Id.* ¶ 32. He further states, based on inadmissible news articles, that "[r]eports indicate DOGE personnel have obtained persistent administrative access, bypassing [] controls," including "time-limited, audited privileged access through secure mechanisms." *Id.* ¶ 39. Moreover, he claims that "other DOGE engineers obtained access to OPM's records before the agency confirmed that they had government-issued computers and before they had been vetted in accordance with longstanding agency practices." *Id.* ¶ 10. And he asserts "DOGE" has "manipulated the OPM systems making them much more vulnerable to attack," and that "[r]eports also indicated that individuals associated with DOGE connected an unauthorized server into the OPM network," *id.* ¶ 40.[14] But all of these statements are based on inadmissible hearsay within hearsay, without citation to record evidence, and they exhibit a glaring lack of understanding of OPM's account and access management protocols. As CIO Greg Hogan explains, OPM utilizes FedRAMP-approved Microsoft Entra ID for account and access management for most of OPM data systems, thereby ensuring robust role-based access control—and no one has "bypassed" those controls. *See* Second Hogan Decl. ¶¶ 7-9. Furthermore, the record firmly disproves that "DOGE engineers" were granted access to OPM systems before they were vetted. *Id.* ¶¶ 5-6, 8; Hilliard Decl. ¶ 13. And CIO Hogan explains that no one has "bypassed controls" or "manipulated" OPM systems and thereby made them more vulnerable to attack. *See* Second Hogan Decl. ¶ 9-10, 12.

[14] For this assertion, Schneier cites a letter from Rep. Gerald Connolly and Rep. Shontel Brown, *see id.* ¶ 40 n.4, who wrote to Acting OPM Director Ezell "concerning numerous reports that a server of unknown nature and origin was brought into [OPM] last week, connected to federal government networks, and used to access sensitive government data without regard for crucial security and privacy protections." Noble Decl., Ex. M at 1. That letter is apparently based on news reports concerning the complaint in *Doe v. OPM,* No. 25 Civ. 234 (D.D.C.), filed by anonymous plaintiffs who alleged, based on further anonymous sources, that OPM had connected a private server to OPM systems in connection with developing the GWES. *See Doe v. OPM,* No. 25 Civ. 234 (RDM), 2025 WL 513268, at *1, 6 (D.D.C. Feb. 17, 2025). Schneier's statement thus represents *five levels* of hearsay. And as CIO Hogan has made clear, under penalty of perjury, that he is uninformed and incorrect. *See* Second Hogan Decl. ¶ 12.

The claim that a "private server" was connected to OPM systems in connection with the development of the GWES is based on erroneous and anonymous hearsay, categorically untrue, and contradicted by the record in this case. *Id.* ¶ 12; *see also* OPM-000120 ("The GWES is located within Microsoft applications and on secure government computers."). Moreover, another court has already concluded that such allegations are insufficient to show OPM's systems are at "imminent risk due to likely cyberattack." *Doe v. OPM*, 2025 WL 513268, at *6.

Plaintiffs' expert David Nesting served as a former Deputy CIO of OPM from 2019 to 2021, and as a Site Reliability Engineer in the U.S. Digital Service from 2014-2019. Nesting Decl. ¶¶ 6, 9. His declaration is based on his reading of the First Hogan Declaration, Defendants' brief in support of their motion to dismiss, and unspecified "public information" he reviewed—and does not cite to the OPM administrative record at all. *Id.* ¶¶ 3, 37. He states, based on his review of this unspecified public information, that he does "not believe the DOGE personnel that have obtained, or are seeking, full administrative access to OPM's IT systems have been sufficiently vetted." *Id.* ¶ 37. That is incorrect. The record shows that every OPM employee at issue was properly vetted, credentialed, and appointed at OPM. *See supra* at 4-5. And despite his years of experience as the former Deputy CIO at OPM, Nesting provides no explanation for what he means by "full administrative access." Nesting Decl. ¶ 37. As CIO Hogan explains, the term "administrator access" or "administrative access" means a user has elevated permissions, not full and total control over all OPM data systems. *See supra* at 17. Nesting states that when he worked on IT modernization projects for various federal agencies while employed at the U.S. Digital Service, he did not need access to underlying data. Nesting Decl. ¶ 9, 22-31.[15] But because he was not an

[15] Nesting is curiously silent concerning the level of his access to OPM's data systems, or the need for such access, while serving as Deputy CIO of OPM. *See* Nesting Decl. Of course, by virtue of

employee of these other agencies that maintained such data systems, it is not surprising that he was not granted access to the underlying data. *See* 5 U.S.C. § 552a(b)(1). In contrast, the record here shows that all of the individuals at issue were duly appointed as employees of OPM.

At bottom, Plaintiffs' assertion that OPM's systems are now more vulnerable to hacking by malevolent actors simply because new, properly appointed OPM employees have access to OPM's records systems is entirely conclusory and speculative. Indeed, Plaintiffs' continued argument that access to OPM information by a limited number of new OPM employees will likely result in that information being compromised by third-party bad actors or disclosed to other, unauthorized government employees is simply unfounded. Plaintiffs' erroneous theory—based on inadmissible hearsay—that Defendants' actions *might* put their information at increased risk or *could* lead to retaliation is insufficient to confer standing.

To the extent Plaintiffs assert, in perfunctory fashion, that their injuries are also analogous to claims for "disclosure of private information," "harms specified by the Constitution," or the common law tort of 'breach of confidence," Pls' Br. at 13, they have not developed those arguments, and they are thus deemed waived. *See Tolbert v. Queens Coll.*, 242 F.3d 58, 75 (2d Cir. 2001). In any event, they are unavailing for the reasons outlined in Defendants' briefing on their motion to dismiss. *See* ECF Nos. 62 at 8-9.

B. Plaintiffs' Claims Are Not Reviewable Under the APA

Plaintiff's claims under the APA for violations of the Privacy Act fail because they have not shown the requisite final agency.[16]

---

that position the need is readily apparent, and he would "otherwise have access to OPM's systems." *Am. Fed'n of Tchrs.*, 2025 WL 895326, at *4 n.3.

[16] Defendants acknowledge that the Court has already found that the Privacy Act's comprehensive remedial scheme does not provide another "adequate remedy," 5 U.S.C. § 704, that would prevent review under the APA. *See* ECF No. 72 at 50-53. Defendants incorporate their arguments on this

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). 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*"). Courts have long recognized that this definition of agency action "is not so all-encompassing as to authorize us to exercise judicial review over everything done by an administrative agency." *Indep. Equip. Dealers Ass'n v. EPA*, 372 F.3d 420, 427 (D.C. Cir. 2004) (cleaned up and internal quotation omitted). For example, courts do not oversee agency training programs, *see Jones v. U.S. Secret Serv.*, 701 F. Supp. 3d 4, 17 (D.D.C. 2023), or "the common business of managing government programs," *Fund for Animals*, 460 F.3d at 20. Put another way, judicial review under the APA does not reach the agency's "workaday" dealings. *Indep. Equip. Dealers Ass'n*, 372 F.3d at 427.

The evidence in the record shows that the "agency action" Plaintiffs challenge is actually a series of discrete personnel decisions related to vetting, onboarding, and granting individual OPM employees access to OPM data systems. *See supra* at 4-5, 7. Plaintiffs make this plain through their attempts to point out perceived deficiencies—none of which stand up to scrutiny—in the vetting and onboarding of particular individuals. *See* Pls' Br. at 16.[17] For instance, Plaintiffs

---

point from their prior briefing, *see* ECF No. 62 at 16-19, ECF No. 71 at 7-8, to preserve the issue, if necessary, for appeal.

[17] Plaintiffs' assertion that three OPM employees (OPM-4, OPM-6, OPM-7) "did not finalize their employee paperwork with OPM before obtaining the agency's records," Pls' Br. at 16, is demonstrably incorrect. Plaintiffs erroneously claim that "[g]overnment employees must generally complete a standard government form called a 'Notification of Personnel Action' (SF 50), which details a person's position and is signed by an authorized official at the agency." *Id.* However, an SF 50 form, as the name suggests, is a notification of personnel action *to* the employee documenting the personnel action after it is effective, not a form that the employee completes prior to appointment. *See, e.g., NTEU v. Reagan*, 663 F.2d 239, 244 (D.C. Cir. 1981) ("The SF-50, Notification of Personnel Action [], is the document used to record personnel actions after they are effective.... SF-50 simply documents the action."). While an SF 50 is indeed part of the "usual

claim that OPM-5 "obtained access to sensitive systems prior to completing a pre-appointment background investigation," Pls' Br. at 20 (citing OPM-000218), but the very waiver form they cite makes clear that "an individual may be appointed on a temporary-basis to a critical-sensitive position prior to the investigation's completion." OPM-000218; *see also* Hilliard Decl. ¶ 20. And an individual may have logical access to OPM's data systems when they are cleared for entrance on duty. *See id.* ¶ 13. Likewise, Plaintiffs' claim, based on inadmissible hearsay, that OPM-4 obtained access to OPM systems despite being fired by a cybersecurity firm, Pls' Br. at 20 & n.32, has no bearing on whether OPM-4 was properly vetted and granted access to OPM systems. *See* Hilliard Decl. ¶ 19. Contrary to Plaintiffs' continued assertions (Pls' Br. at 23), the evidence in the record shows that OPM's appropriate vetting, credentialing, onboarding, and decisions to grant access permissions to new OPM employees, *see supra* at 4-5, 7-8, were all "representative of its ordinary day-to-day operations," and they were not, "in sharp contrast to its normal procedures, illegal, rushed, and dangerous." *Cf.* ECF No. 72 at 47. The record is clear that the newly-appointed OPM officials followed established protocols for seeking access to these systems—they requested access to relevant OPM data systems, and OPM career officials authorized that access, *see supra*

---

indicia of civil service status," *Horner v. Acosta*, 803 F.2d 687, 694 (Fed. Cir. 1986), another "appointive document," evidencing an "an oath of office" is sufficient to effectuate the appointment, *id.*; *see also NTEU,* 663 F.2d at 246 (employees were duly appointed despite lack of completed SF 50s). Here, on January 24, 2025, OPM-4 completed an appointment affidavit (Standard Form 61), which includes the details of his appointment and an oath of office, sworn before an OPM Supervisory HR Specialist. OPM-000014. He also completed an Acceptance of Uncompensated Services agreement the same day evidencing that he "agree[s] to being appointed as an uncompensated employee of OPM." OPM-000015. And OPM's declarant has explained that an SF 50 could not be generated by OPM's HR system in connection with his appointment. *See* Garcia Decl. ¶ 9. As to OPM-6 and OPM-7, both of their SF 50 forms show an "effective date" of January 24, 2025, and January 20, 2025, respectively, and they also executed appointment affidavits on those dates. *See* OPM-000021 (SF 50 for OPM-6); OPM-000022 (appointment affidavit for OPM-6); OPM-000111 (SF 50 for OPM-7), OPM-000112 (appointment affidavit for OPM-7). All of these employees were duly appointed to OPM.

at 7.[18] The record evidence thus stands in stark contrast to Plaintiffs' allegations that OPM made the "decision to depart radically from its established safeguards and to give access to DOGE agents in violation of the law," ECF No. 72 at 49. Simply put, there is no evidence that *anyone* made the decision to disregard established vetting and security practices, throw out standard access controls, and grant "DOGE agents" unfettered access. The record shows the exact opposite occurred.

C. Plaintiffs Have Not Shown Likely Violations of the APA

To the extent the Court finds that that Plaintiffs APA claims are reviewable, Plaintiffs are unlikely to succeed in establishing that Defendants actions were not in accordance with the law—*i.e.*, the Privacy Act—or otherwise arbitrary and capricious.

As an initial matter, Plaintiffs have attempted to improperly shift the burden of proof to Defendants as to the merits of their APA claims—arguing that it is Defendants that bear the burden as to whether the exception to disclosure at Section 552a(b)(1) applies. *See* Pls' Br. at 15. In support of this novel contention, they cite to cases involving Privacy Act claims, noting that the 552a(b)(1) exception is likely an affirmative defense, and posit that Defendants thus must establish that it applies. *See id.* However, Plaintiffs' Privacy Act claims have been dismissed. *See* ECF No. 72 at 56. Plaintiffs are now pursuing claims under Section 706(2) of the APA, asserting that Defendants' actions were (1) "not in accordance with law," because they violated the Privacy Act, Pls' Br. at 21, and (2) arbitrary and capricious because Defendants "failed to consider an important aspect of the problem," and "failed to articulate a satisfactory explanation for [their] action," in granting access to "DOGE agents," *id.*

[18] In this regard, this case is readily distinguishable from other Privacy Act-related cases in which courts have found the grant of access to agency DOGE Teams constituted "final agency action." *See, e.g., Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, No. 25 Civ. 0596 (ELH), 2025 WL 1206246, at *51 (D. Md. Apr. 17, 2025) (describing agency head's "repeated and rapid approvals of access requests" as inconsistent with "ordinary business operations and procedures").

Under the APA, it is Plaintiffs who bear the burden of showing, by citation to evidence in the administrative record, that the agency's actions are arbitrary and capricious or otherwise not in accordance with law. *See Adueva v. Mayorkas*, No. 17 Civ. 03350 (DLI), 2021 WL 3492144, at *13 (E.D.N.Y. Aug. 9, 2021). Furthermore, "this standard of review is highly deferential and presumes the agency's action to be valid." *Adler v. DOJ*, No. 18 Civ. 2188 (PAC), 2018 WL 4571677, at *3 (S.D.N.Y. Sept. 24, 2018) (citation omitted). Furthermore, "[a] reviewing court may not itself weigh the evidence or substitute its judgment for that of the agency." *Islander E. Pipeline Co., LLC v. McCarthy*, 525 F.3d 141, 150 (2d Cir. 2008) (citation omitted). Accordingly, it is Plaintiffs who bear the burden of showing, with sufficient proof on their motion for a preliminary injunction, that OPM's actions violated the strictures of the Privacy Act—including both Section 552a(b)(1) and Section 552a(e)(10).

Plaintiffs have failed to meet their burden. At the outset, Defendants can only show that OPM "disclosed" agency records to four OPM "DOGE agents." *See supra* at 8, 13, 15. That is because the rest of the individuals at issue never logged into these systems prior to March 6, 2025, *id.,* and thus no "unauthorized transmission of a protected record" occurred. *See* ECF No. 72 at 34. Moreover, despite the clear factual record to the contrary, Plaintiffs continue to assert that the individuals at OPM who were granted access permissions to OPM's data systems are *not* employees of that agency—instead, Plaintiffs claim they are "functionally controlled and supervised by agencies other than OPM." Pls' Br. at 15. That is simply incorrect. Indeed, all of the relevant individuals who were granted access permissions to OPM data systems are duly appointed employees of OPM. *See* Garcia Decl. ¶ 20. And all of the OPM employees who actually logged into these systems had the requisite need for the records in performance of their duties. *See* First Hogan Decl. ¶ 12; Second Hogan Decl. ¶¶ 13-14. As a result, Plaintiffs have not established a

likelihood of success on the merits of their APA claims to warrant the extraordinary remedy of a preliminary injunction.

1. <u>All of the individuals granted access to OPM's records systems are OPM employees.</u>

All of the individuals at issue were appropriately vetted, credentialed, and duly appointed as employees of OPM, and thus are "employees of the agency which maintains the record." *See supra* at 4-5; Hilliard Decl. ¶ 24; Garcia Decl. ¶ 20.

Plaintiffs claim, without support, that many "DOGE agents," are not "of the" OPM because they are "are functionally controlled and supervised by agencies other than OPM, including DOGE itself." Pls' Br. at 15. In support of this assertion, Plaintiffs offer no actual evidence. Even if these individuals were hired in consultation with USDS and coordinate their work with USDS, that does not make them "functional" employees of USDS.[19] The idea that OPM employees' coordination and consultation with DOGE makes them *de facto* DOGE employees is without any support in the law. Plaintiffs similarly point to the fact that several OPM employees have been detailed or dual-appointed to other agencies, Pls' Br. at 16 & nn. 26-27, but that does not undermine the fact that these individuals were employees of OPM when they were granted access permissions to OPM data systems. *See* ECF No. 72 at 36 (noting that the relevant determination is "whether, at the time they were first given access to OPM records, the DOGE agents were OPM employees"). Furthermore, none of these individuals were "detailed from another component of the government [to OPM] at the time they were first given access." ECF No. 72 at 36; *Cf. Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA,* No. 25 Civ. 0596, 2025 WL 868953, at *60 (D. Md. Mar. 20,

[19] Such collaboration and coordination between agency employees and USDS is far from unprecedented or in "sharp contrast" to OPM's normal procedures. Indeed, prior to January 20, 2025, USDS (when it was named the U.S. Digital Service) routinely coordinated and worked on IT modernization projects at agencies across the federal government. *See supra* at 3-4 & nn. 2-3; *see also* Nesting Decl. ¶ 9.

2025) (discussing employees detailed to the Social Security Administration ("SSA") who may have accessed systems prior to having "finalized detailed agreements" from those other agencies to SSA (cited by Plaintiffs, Pls' Br. at 17)). The fact that some employees may have dual appointments at OPM and other agencies, *see* Garcia Decl. ¶¶ 7, 9 ,13, or were later detailed *from* OPM *to* other agencies, *see id.* ¶¶ 11, 13, does not make those individuals non-employees of OPM at the time they were granted access.

That some of these individuals have decided to forgo a paycheck pursuant to established and lawful procedures similarly does not make them non-employees of OPM. *See id.* ¶ 6; *see also* 5 C.F.R. § 304.104(c). Plaintiffs cite no authority to the contrary. Finally, Plaintiffs assert without *any* evidentiary support that "[t]he DOGE agents do not answer to OPM officials." Pls' Br. at 16. It remains unrebutted that employees with dual appointments, or on temporary details *from* OPM *to* other agencies, are still employees of OPM. Accordingly, all of the relevant employees who were granted access permissions to OPM's data systems are employees of OPM.

2. <u>All of the individuals granted access permissions to OPM's records systems have a need for access in the performance of their duties.</u>

Contrary to Plaintiffs' assertions (Pls' Br. 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 working to further the priorities of the USDS E.O. have a need for "full and prompt access to all unclassified agency records, software systems, and IT systems" to perform those duties. *Id.* § 4. Indeed, the relevant OPM personnel were granted access permissions 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.[20] *See* First Hogan Decl. ¶¶ 6, 8, 13; Second Hogan Decl. ¶ 14; *Cf. AFL-CIO v. Dep't of Lab.*, No. 25 Civ. 0339 (JDB), 2025 WL 542825, at *2 (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).

Plaintiffs decry the lack of formal justification for each employee's access to OPM data systems in the administrative record. *See* Pls' Br. at 17. But this case does not involve the "unauthorized disclosure of millions of records" that would be "unlawful" absent a "showing of why each employee needed to receive the information." Pls' Br. at 17 (quoting *Bessent*, 2025 WL 582063, at *11).[21] OPM does not have contemporaneous formal justifications for any of the hundreds of career and non-career OPM employees who were granted access permissions to various OPM data systems between January 20 and February 12, 2025. *See* OPM-000089-91 (Account Creation Audit spreadsheet showing over 300 access permission grants to hundreds of

[20] Executive Order 14,170 tasks the OPM Director, 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).

[21] Plaintiffs fail to note that their quotation from Judge Boardman's decision in *Bessent* granting a preliminary injunction preventing access to OPM's records systems—which has been stayed pending appeal—actually is a quotation from *Dick v. Holder*, 67 F. Supp. 3d 167, 178 (D.D.C. 2014), an inapposite case involving "agency-wide distribution" of records to DOJ employees. *See Dick v. Holder*, 67 F. Supp. 3d 167, 178 (D.D.C. 2014) ("[P]ermitting agency-wide distribution under § 552a(b)(1) without any showing of why each employee needed to receive the information would allow the exception to swallow the rule."). Here, OPM officials granted access to a limited number of properly vetted and appointed OPM employees in furtherance of the President's lawful executive order.

OPM employees, between 1/20/25 and 2/12/25). That is simply not how any federal agency operates, or is required to operate, when making decisions as to whether to grant an employee access to an agency database. That is because "the courts must presume that the government will exercise its powers responsibly and with due regard to affected individuals." *Univ. of California Student Ass'n v. Carter*, No. 25 Civ. 354 (RDM), 2025 WL 542586, at *6 (D.D.C. Feb. 17, 2025) (denying temporary restraining order enjoining Department of Education staffers from sharing student association's members' data with DOGE staffers) (internal quotation and citation omitted). This "presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties." *United States v. Chem. Found.*, 272 U.S. 1, 14-15 (1926). OPM employees (and DOGE employees) are obligated to use Plaintiffs' personal information for lawful purposes, within the mission of OPM, and to keep it confidential, in accordance with the Privacy Act. *See Carter*, 2025 WL 542586, at *6. In this case, there is no evidence that OPM employees have not abided by those obligations with respect to the personal information contained in OPM's systems.

Plaintiffs now concede, as they must, that the DOGE agenda of modernizing government IT is nothing new. *See* Pls' Br. at 19.[22] Rather, they claim that access to OPM data systems is

[22] 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").

unnecessary because it is "vastly preferable to modernize IT systems without access to the data." Pls' Br. at 18. On this point, Plaintiffs assert that the Court should trust their purported experts as to whether these OPM employees have a need for access to these OPM data systems. But even assuming that some outside observers might do things differently does not suffice to show that the relevant OPM employees do not have a need to access OPM data systems in furtherance of their duties. Plaintiffs' experts' opinions as to the "need for access" are properly excluded because they amount to "little more than improper second-guessing of [the agency]'s decision on the merits." *Safe Haven Home Care, Inc. v. HHS*, 130 F.4th 305, 324 (2d Cir. 2025) (affirming exclusion of extra-record expert declaration in matter under the APA); *see also Asarco, Inc. v. EPA*, 616 F.2d 1153, 1160 (9th Cir. 1980) ("Consideration of [extra-record] evidence to determine the correctness or wisdom of the agency's decision is not permitted.").

That OPM's CIO rolled back or removed access permissions for certain individuals where "it is currently unnecessary," OPM-000027, does not show that the OPM "DOGE agents" did not have a need for access to those systems when access was granted. *See* Pls' Br. at 17. As the record shows, after assuming his role as Acting Director on January 20, 2025, Charles Ezell requested access for these individuals because, while there were no immediate plans to make changes to these OPM systems, he wanted the agency to be prepared to move quickly to implement any changes. *See* OPM-000029 ("Right now we don't have immediate plans to change anything[,] but if we need to[,] we might need to move quickly."). The initial justification for granting access permissions was thus appropriate. CIO Hogan made the decision later in February 2025 to conduct a review of assigned user privileges to determine whether the rationale for assigning such privileges remained valid. *See* OPM-000023-26; Second Hogand Decl. ¶ 10 (discussing periodic review of assigned user privileges to implement principle of least privilege). As Plaintiffs' own

experts note, implementing the principle of least privilege, which includes a periodic review of user privileges, is a fundamental "best practice." Lewis Decl. ¶¶ 12, 14; Schneier Decl. ¶¶ 36-37. That CIO Hogan determined that those individuals "never needed" access to EHRI and eOPF—data systems that were not accessed by any of the relevant OPM employees prior to March 6, 2025, *see* OPM-000103—and made sure those access permissions were removed is thus appropriate.

Finally, Plaintiffs posit that the "mass resignation" of former USDS employees who "complained that DOGE agents"—though not *OPM* "DOGE agents"—were "firing technical experts, mishandling sensitive data and breaking critical systems," Pls' Br. at 18 (citing to an inadmissible letter downloaded from Politico, *see* Noble Decl., Ex. P), somehow shows a lack of need for access by OPM employees to OPM record systems. This contention is simply irrelevant, and there is no evidence in the record (or otherwise) that this type of conduct occurred at OPM.

3. OPM has adhered to appropriate safeguards to insure security and confidentiality of its data systems

OPM has established and adhered to appropriate safeguards to "insure the security and confidentiality" of it sensitive data systems. *See* 5 U.S.C. § 552a(e)(10). As detailed above, OPM has adhered to its established and appropriate vetting, credentialing, onboarding, and account and access management procedures. *See supra* at 4-5, 7-8. Each of the OPM employees "was appropriately vetted and credentialed according to [OPM's] established, rigorous, and required procedures." Hilliard Decl. ¶ 24. OPM did not "deviate from any of these required vetting and credentialing procedures," *id.*, and "at no point did anyone direct" the career staff of OPM's Personnel Security Division "to deviate from these established vetting and credentialing procedures." *Id.* Similarly, "each of the [relevant] employees was duly appointed as an employee of OPM according to established procedures." Garcia Decl. ¶ 20. And "OPM has consistently followed appropriate safeguards in connection with the granting of access permissions to OPM

data systems to individuals who onboarded on or after January 20, 2025." Hogan Decl. ¶ 15. Accordingly, Plaintiffs are highly unlikely to succeed in establishing that Defendants acted contrary to 5 U.S.C. § 552a(e)(10).

D. The DOGE Defendants Have Not Acted *Ultra Vires*

Plaintiffs' *ultra vires* claim against the "DOGE Defendants alone," asserts that "no law permitted them to access and administer OPM systems." Pls' Br. at 23. However, Plaintiffs have not cited to even a scintilla of evidence showing that any DOGE Defendants requested, demanded, or were granted access to OPM's data systems, let alone "administered" them. This section of Plaintiffs' brief (Pls' Br. at 23-24), is devoid of record citations—presumably because the OPM administrative record *never* even mentions any of the DOGE Defendants at all. Plaintiffs' conclusory assertion that "[t]he DOGE Defendants directed and induced" violations of the Privacy Act is simply unfounded. The record shows that Acting Director Ezell and Chief of Staff Scales requested that OPM's Associate CIO (a career employee) grant access permissions to the new OPM employees at issue, and the Associate CIO approved each of those requests. *See supra* at 7. All of these individuals were appropriately vetted and duly appointed employees of OPM. *See supra* at 4-5. As such, this claim is unlikely to succeed on the merits as well.

II. 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*.

Plaintiffs cannot establish irreparable injury. They rely solely on their purported experts' speculative opinions that "continued unrestricted access makes [] eventual recovery more difficult

and increases the risk of irreversible damage," Pls' Br. at 24 (quoting Schneier Decl. ¶ 78), that "sensitive information stored in [legacy systems] can be lost, altered or compromised in ways that cannot be remedied," *id.* at 24-25 (quoting Nesting Decl. ¶ 41), and 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," Pls' Br. at 27 (citing all three expert declarations). However, the record evidence shows that these concerns are unfounded. OPM has adhered to its appropriate safeguards in controlling access to its data systems. *See* Second Hogan Decl. ¶ 15. And Plaintiffs point to no evidence that would be admissible showing that a risk of public disclosure of their sensitive, private information is "actual and imminent." *See, e.g., Doe v. OPM*, 2025 WL 513268, at *6 ("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 cyberattack and that this risk would be mitigated were the agency required" to implement measures mandated by the Privacy Act). They simply have failed to carry their burden. Indeed, other courts faced with similar claims of irreparable injury premised on alleged Privacy Act violations due to data access by "DOGE agents" have concluded that such access alone—devoid of allegations of unauthorized public disclosure—is insufficient to show irreparable harm warranting the imposition of preliminary injunctive relief. *See Carter*, 2025 WL 542586, at *6. Plaintiffs' unfounded "fear that Defendants will use the information against them," Pls' Br. at 26, is similarly too speculative to show irreparable harm. As a result, this case does not present the requisite "extraordinary circumstances" warranting preliminary injunctive relief.

III. 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 rely on their purported "extremely high likelihood of prevailing on the merits," of their APA claims, and on the unremarkable proposition that "[i]ndividual privacy is an important public interest." Pls' Br. at 27-28. However, Defendants have not violated the APA or the Privacy Act, for the reasons stated above, *supra* at 23-30, and Plaintiffs have not shown that their personal privacy interests are at stake. Regardless, considering only likelihood of success is insufficient to justify injunctive relief. *See, e.g.*, *Winter*, 555 U.S. at 24. 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' Br. at 28 (citing to Schneier Decl. ¶¶ 43-47, which in turn cites the 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 16-20.

In contrast, the proposed injunction would harm the public interest. At its core, it would limit 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 OPM's ability to modernize critical IT infrastructure and engage in federal workplace reform, in keeping with the President's executive orders. Simply put, the requested injunction would prevent federal employees from doing their jobs.

IV. Plaintiffs' Proposed Injunction Is Improper

Plaintiffs' proposed injunction is also overbroad. Plaintiffs request, among other things, that the Court enjoin Defendants from granting access to or disclosing *any* non-public OPM

records—not specific OPM data systems—to unspecified "DOGE agents." ECF No. 89 at 1. The requested prohibition on disclosure or access to all "DOGE agents"—as expansively defined, *see* ECF No. 89 at 1 n.3—would include countless OPM employees working on IT modernization projects, and goes well beyond the protections of the Privacy Act. This definition could potentially include all of OPM's staff in the Office of the Chief Information Officer, OPM's entire CISO team, any outside contractors who perform work on OPM data systems, and countless others. Moreover, the record evidence shows actual access to a single OPM data system by four OPM employees—and on that slender reed, Plaintiffs ask the Court to grind the work of OPM's IT modernization to a halt. "A plaintiff's remedy must be tailored to redress the plaintiff's particular injury," *Gill v. Whitford*, 585 U.S. 48, 72-73 (2018). Such a sweeping ban on access to *all* OPM 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 preliminary injunction.

Dated: New York, New York
May 16, 2025

Respectfully submitted,

JAY CLAYTON
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: */s/ David E. Farber*
JEFFREY OESTERICHER
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 modified by the Court's Order. *See* ECF No. 94. As measured by the word processing system used to prepare it, this memorandum contains 11,987 words.

/s/ David E. Farber
Assistant United States Attorney