UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, et al.,		
Plaintiffs,	:	25cv1237 (DLC)
-v-	:	OPINION AND ORDER
U.S. OFFICE OF PERSONNEL MANAGEMENT, et al.,		
Defendants.	:	

APPEARANCES:

For plaintiffs:

Victoria Noble
F. Mario Trujillo
Cindy Cohn
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Rhett O. Millsaps II
Mark P. McKenna
Christopher J. Sprigman
Mark A. Lemley
Lex Lumina LLP
745 Fifth Avenue, Suite 500
New York, NY 10151

Norman L. Eisen
Andrew H. Warren
Democracy Defenders Fund
600 Pennsylvania Avenue SE #15180
Washington, DC 20009

Subodh Chandra
The Chandra Law Firm LLC
1265 W. 6th Street, Suite 400
Cleveland, OH 44113

For defendants:

Ilan Stein
Alyssa O'Gallagher
Jeffrey Stuart Oestericher
United States Attorney's Office, Southern District of New York
86 Chambers Street, 3rd Floor
New York, NY 10007

DENISE COTE, District Judge:

Following President Trump's inauguration on January 20, 2025, the U.S. Office of Personnel Management ("OPM") granted a group of individuals associated with the Department of Government Efficiency ("DOGE") broad access to systems of records containing the personal information of tens of millions of past, current, and aspiring federal employees, even though no credible need for this access had been demonstrated. In doing so, OPM violated the law and bypassed its established cybersecurity practices.

This action was filed on February 11, 2025 by current and former federal government employees and their unions. An Opinion of June 9, 2025 found that the plaintiffs were entitled to a preliminary injunction based on the defendants' violations of the Privacy Act, which were reviewable under the Administrative Procedure Act ("APA"). Am. Fed'n of Gov't Emps. v. OPM, 786 F. Supp. 3d 647, 657 (S.D.N.Y. 2025) ("June 9 Opinion"). A preliminary injunction was entered on June 20.

An Opinion of December 19, 2025 denied the defendants' motion to dismiss the case as moot and the plaintiffs' motion for extra-record discovery. Am. Fed'n of Gov't Emps. v. OPM, 820 F.Supp.3d 260 (S.D.N.Y. Dec. 19, 2025) ("December 19 Opinion"). The parties now cross-move for summary judgment. For the following reasons, the defendants' motion for summary judgment is granted as to the plaintiffs' ultra vires claim but otherwise denied; the plaintiffs' cross motion for summary judgment on their APA claims is granted.

Procedural Background

On February 11, 2025, current and former federal government employees and their unions sued OPM and other defendants for breaches of privacy.[1] The complaint includes five claims for relief: two claims under the Privacy Act of 1974, 5 U.S.C. § 552a ("Privacy Act"); two claims under the APA, 5 U.S.C. § 701 et seq.; and an ultra vires claim. The plaintiffs seek injunctive relief and a declaration that the decision to implement a system by which DOGE Agents have access to OPM's

[1] There are two sets of defendants: the "OPM Defendants," which consist of OPM and its former Acting Director Charles Ezell; and the "DOGE Defendants," which consist of the United States DOGE Service ("USDS"), its Acting Director, the U.S. DOGE Service Temporary Organization, and Elon Musk.

records and the plaintiffs' personal information contained in those records is unlawful.

On February 14, the plaintiffs brought a motion for a temporary restraining order. Before that motion was fully submitted, however, the parties requested that it be converted into a motion for a preliminary injunction. On February 27, the plaintiffs moved for expedited discovery. An Order of March 7 instructed the defendants to provide the plaintiffs with the administrative record and other relevant materials that had been produced in a related action in the District of Maryland, Am. Fed'n of Tchrs. v. Bessent, No. 25-cv-430 (D. Md.) ("Maryland OPM Action").

On March 14, the defendants filed a motion to dismiss the complaint pursuant to Rules 12(b)(1) and 12(b)(6), Fed. R. Civ. P., which became fully submitted on March 31. An Opinion of April 3 dismissed the two claims brought under the Privacy Act, except insofar as they serve as a predicate to the plaintiffs' other claims and otherwise denied the defendants' motion to dismiss. Am. Fed'n of Gov't Emps. v. OPM, 777 F. Supp. 3d 253 (S.D.N.Y. 2025) ("April 3 Opinion"). The Opinion found that the complaint adequately pleaded a violation of the Privacy Act and the APA based on the disclosure of OPM records to individuals who were not OPM employees or did not have a need for such

access in the performance of their duties at OPM. Id. at 271-77.

On April 23, OPM filed an updated administrative record that provided information about events that had occurred through March 6. The plaintiffs filed a motion for a preliminary injunction on April 25, and that motion became fully submitted on May 23. A preliminary injunction hearing was held on May 29. Gregory Hogan, who was then OPM's Chief Information Officer ("CIO"), testified on behalf of the defendants. David Nesting, a former Deputy CIO at OPM and a former Director of Engineering at the U.S. Digital Service, testified on behalf of the plaintiffs.

The June 9 Opinion found that the plaintiffs had shown that they were entitled to a preliminary injunction. 786 F. Supp. 3d at 657. The Opinion found first that the plaintiffs had carried their burden at that stage of the proceedings to establish Article III standing. Id. at 677-83. Next, the Opinion found that the plaintiffs had shown a likelihood of proving that the Privacy Act was violated on two grounds: (1) OPM records were disclosed to individuals affiliated with DOGE who were not OPM employees or did not have a need for the records in the performance of their duties at OPM, and (2) OPM had failed in its duty to safeguard the plaintiffs' records, having set aside

its established safeguards in connection with individuals brought into OPM to pursue the DOGE agenda. Id. at 683-90. The Opinion also found that these claims are reviewable under the APA. Id. at 690-92.

Pursuant to an Order of June 9, the parties offered proposed terms for a preliminary injunction on June 12. On June 13, the Court circulated a draft preliminary injunction and held a conference. After the parties proposed revisions to the Court's draft injunction on June 19, another conference was held on June 20. In their June 19 letter, the defendants argued that the Court does not have authority to order OPM to undertake a forensic audit but noted as well that any such audit would be "in addition to" three audits concerning "DOGE Access" that were already being conducted. These were an audit by the Government Accountability Office ("GAO"), an audit being conducted by OPM's Office of the Inspector General ("OIG"), and a regular annual audit conducted by OPM.

A preliminary injunction was issued on June 20. It required the Government to file two reports. The first report, which the Government filed on July 18, described the procedures OPM had put in place since March 6 to ensure adherence to the requirements of the Privacy Act with respect to any new grant of

access permissions by OPM to any records containing the plaintiffs' personally identifiable information ("PII").

The Government filed the second report on August 1 and a corrected version of the second report on September 30. This report provided information regarding access permissions that had been granted to "DOGE Agents," as defined in the preliminary injunction,[2] and were in effect as of the date of the preliminary injunction, June 20. Pursuant to an Order of June 27, the Government supplemented the administrative record on August 29.

In a joint letter of September 15, the parties proposed that, before proceeding to summary judgment, the plaintiffs would move for extra-record discovery, and the defendants would

[2] The definition of "DOGE Agents" in the preliminary injunction, which is also adopted in this Opinion, is the following:

> (1) the individuals listed on page OPM-103 of the administrative record; (2) any individuals employed by [USDS] and detailed to OPM; (3) any individuals employed by OPM and detailed to USDS; (4) any individuals employed by OPM who are detailed to any other federal agency for the principal purpose of implementing initiatives that are directed by USDS; and (5) any individuals who were not employees or contractors of OPM prior to January 20, 2025 and who have been given access to any OPM system of records containing PII for the principal purpose of implementing initiatives that are directed by USDS. Excluded from this definition are Charles Ezell, Gregory Hogan, Amanda Scales, and James Sullivan.

move to dismiss this action as moot. Delayed by the Government shutdown, the motions became fully submitted on December 17.

In their motion to dismiss, the defendants primarily argued that the plaintiffs' claims were moot because none of the five DOGE Agents left at OPM had access to the plaintiffs' PII in any OPM system, and because OPM had adopted new security protocols that would ensure compliance with the Privacy Act. The defendants also argued that, to the extent that there is reason to expect any future violation of the Privacy Act, such a violation is not currently ripe for review. The motion was accompanied by a declaration of OPM's Acting CIO Perryn Ashmore,[3] an excerpt of an updated OPM Cybersecurity and Privacy Policy released on November 18, and a supplemental administrative record.

The December 19 Opinion denied the motion. 820 F. Supp. 3d at 264. The Opinion first determined that, even with the updated protocols, the defendants had failed to establish that the challenged conduct could not reasonably recur, particularly given OPM's history of bypassing its security protocols, its refusal to concede that its prior grants of access violated the law, and its failure to offer any assurance that the DOGE

[3] Ashmore replaced Hogan, OPM's previous CIO, on September 2.

Agents' access to OPM systems would not be restored. Id. at 273-75. Moreover, the new protocols, even if strictly adhered to, only addressed the circumstances in which an individual could be given direct access to an OPM system, even though the record reflected instances of DOGE Agents accessing PII indirectly through career OPM staff. Id. at 274. The Opinion then concluded that the lawsuit was ripe for review because there was still a concrete dispute between the parties, and a continuing possibility of hardship to the plaintiffs because the defendants had not explained what happened to any data that was extracted directly or indirectly by DOGE Agents. Id. at 276. The Opinion also denied the plaintiffs' motion for extra-record discovery. Id. at 277.

In a letter of January 9, 2026, the parties proposed a briefing schedule for cross-motions for summary judgment. Also in that letter, the defendants advised the Court of the status of the three audits mentioned in their June 19 letter. At that time, the GAO and OIG audits were still pending, and the OPM annual audit, dated November 24, 2025, had been completed. That annual audit, performed pursuant to the 2002 Federal Information Security Modernization Act (FISMA), reviewed OPM's security practices according to metrics derived from the National Institute of Standards and Technology's (NIST) Cybersecurity

Framework. The report from that audit does not mention OPM's broad grants of access to the DOGE Agents at issue here and provides no indication that such grants were investigated as part of the audit.

On March 2, 2026, the plaintiffs filed a letter motion to unseal the names of the sixteen DOGE Agents who remained anonymized in this action.[4] The motion became fully submitted on March 19.

An Opinion of April 1 granted the plaintiffs' motion. Am. Fed'n of Gov't Emps. v. OPM, 827 F. Supp. 3d 513, 516 (S.D.N.Y. 2026) ("April 1 Opinion"). The Opinion determined that the identities of the relevant DOGE Agents were integral to the merits of the plaintiffs' claims, as well as the public's ability to understand the governmental conduct being challenged. The presumption of public access was therefore strong, and outweighed any countervailing interests asserted by the

[4] Throughout the litigation, the defendants had designated the identities of DOGE Agents as confidential under the Protective Order entered in this case, and their names were replaced with anonymized monikers (e.g., OPM-1) in public filings. The plaintiffs withheld consent to those sealing requests, reserving the right to challenge the confidentiality designation at a later date.

defendants. Thus, under both the common law and First Amendment standards, the DOGE Agents' identities had to be unsealed.[5]

Meanwhile, the defendants moved for summary judgment on March 20. They explained that the GAO and OIG audits, which "touch[] on 'DOGE access' to OPM's data systems," were still pending.[6] They also explained that only two DOGE Agents -- Riccardo Biasini (formerly OPM-2) and Noah Peters (formerly OPM-18) -- remained at OPM.

In their brief, the defendants primarily argued that the record does not support that Biasini and Peters -- who they contend are the only relevant individuals "at this juncture" because the plaintiffs seek prospective relief -- violated the Privacy Act because they were OPM employees with the requisite "need" for access to OPM's systems of records to perform their employment duties at the time.[7] They also sought summary

---

[5] The defendants filed a motion for partial reconsideration of the Court's April 1 Opinion on April 15, which became fully submitted on April 23. An Opinion of April 29 denied the motion. Am. Fed'n of Gov't Emps. v. OPM, No. 25-cv-1237 (DLC), 2026 WL 1162382, at *3 (S.D.N.Y. Apr. 29, 2026).

[6] The defendants also characterize the OPM annual audit, discussed above, as "touching on 'DOGE access' to OPM's data systems." As noted, however, the report from that audit does not mention OPM's broad grant of access to its systems of records to DOGE Agents and therefore does not "touch on" this litigation.

[7] Their employment status is relevant since the Privacy Act permits disclosure to OPM employees "who have a need for the

judgment on the plaintiffs' ultra vires claim against the DOGE Defendants, arguing that there is no record evidence showing any DOGE defendant requesting or being granted access to OPM data systems.[8]

On April 15, the plaintiffs opposed the defendants' motion and cross moved for summary judgment on their APA claims.[9] For a remedy, the plaintiffs sought an order that does the following:

1. Sets aside Defendants' misapplication of Privacy Act disclosure exceptions by:
   a. Prohibiting OPM from disclosing records to any OPM employee under § 552a(b)(1) based on a "need to be prepared" for future events; and
   b. Prohibiting OPM from disclosing records to the DOGE agency, or DOGE agents, under § 552a(b)(1).
2. Sets aside Defendants' ongoing unlawful records disclosure by:
   a. Requiring OPM to remove all DOGE agent access to OPM records systems; and
   b. Requiring Defendants to remove all DOGE agent access to OPM records that have been previously extracted from OPM records systems and moved elsewhere, including requiring the DOGE agency, DOGE agents, and any third party to delete or expunge such copies they possess,

---

record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

[8] The defendants also incorporated by reference their arguments from prior motions regarding standing, the reviewability of the plaintiffs' claims under the APA, and mootness to "preserve these issues for appeal."

[9] The plaintiffs did not move for summary judgment on their ultra vires claim, given the Court's prior ruling that the APA "already gives the plaintiffs meaningful relief for the violation of their rights." June 9 Opinion, 786 F. Supp. 3d at 693.

line with NIST SP 800-53 Revision 5.1, SI-14(2) ("Non-persistence").

3. Sets aside Defendants' ongoing cybersecurity threats and hazards by:
   a. Requiring OPM to create an accurate accounting of disclosures made to DOGE agents, in accordance with 5 U.S.C. § 552a(c)(1); and
   b. Requiring OPM to create and execute a plan to mitigate the ongoing effects of OPM's illegal practice of disclosing records to DOGE agents, regardless of need, employment status, training, or cybersecurity safeguards, in line with NIST SP 800-53 Revision 5.1, IR-8(1) ("Incident response plan, breaches").
4. Determines that Plaintiffs are entitled to attorney's fees and related costs, and reserve consideration of the amount of such fees for a subsequent motion filed under Fed. R. Civ. P. 54(d)(2).

The defendants then filed multiple joint requests for extensions of the briefing schedule to allow the parties to explore "a possible consensual resolution of this action," all of which were granted. The defendants' final letter request of June 16 asked for an additional three weeks to "finalize the settlement" and represented that the parties had reached an agreement "as to all issues except fees, costs, and expenses." On July 7, however, the defendants filed their brief in opposition to the plaintiffs' motion and reply in further support of their motion.

In that brief, the defendants shifted their focus to recent factual developments that they argue render the case moot or, alternatively, counsel against any need for prospective relief.

Those developments include additional updates to OPM's Cybersecurity and Privacy Policy, an internal investigation that OPM conducted into all previous grants of access to PII to DOGE Agents, and the agency's repudiation of the need-to-be-prepared justification for granting administrative access to systems containing PII. They also confirmed that, as contemplated by the DOGE Executive Order, the DOGE Temporary Organization ended its operations on July 4.

The plaintiffs filed their reply in further support of their motion for summary judgment on July 21. In it, they requested that the Court determine whether the plaintiffs are entitled to relief and then seek input from the parties regarding the "precise terms" of that relief.

An Order of July 23 granted the defendants leave to file a sur-reply. The defendants filed their sur-reply on July 28. The sur-reply and the declarations attached thereto revealed, among other things, that only one DOGE Agent -- Noah Peters -- remains at OPM; that OPM repudiates the need-to-be-prepared justification for any access to OPM systems containing PII, not just administrative access; and that OPM's investigation included review of account access, system use, and possible data movement by the DOGE Agents, and found no evidence of extraction, dissemination, or continuing unauthorized access

requiring further containment, eradication, recovery, or notification activity. The plaintiffs did not request an opportunity to further respond.

Factual Background

The relevant facts regarding the defendants' violations of the law were set forth in detail in the June 9 and December 19 Opinions, and familiarity with those Opinions is assumed.[10] The essential facts are recounted below, along with recent developments most salient to the parties' arguments.

I. OPM's Initial Grants of Access to OPM Data Systems to DOGE Agents

On January 20, 2025, President Donald J. Trump signed Executive Order 14,158 (the "DOGE Executive Order"). The DOGE Executive Order established the "Department of Governmental Efficiency" to implement the President's "DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity." It also renamed the U.S. Digital Service as the United States DOGE Service ("USDS") and moved it to the Executive Office of the President. It also

[10] The June 9 Opinion granting in part the plaintiffs' motion for a preliminary injunction was decided based on an administrative record that had been truncated at March 6, 2025. The December 19 Opinion denying the defendants' motion to dismiss incorporated additional information from the September 30 revised access report, the Ashmore declaration, and the supplemental administrative record.

established within USDS the U.S. DOGE Service Temporary Organization (the "DOGE Temporary Organization"), which was "dedicated to advancing the President's 18-month DOGE agenda" and would terminate on July 4, 2026.

The DOGE Executive Order instructed each executive agency to establish a "DOGE Team" consisting of at least four employees, who may include Special Government Employees hired or assigned within thirty days of the DOGE Executive Order. The DOGE Executive Order also instructed agency heads to ensure, "to the maximum extent consistent with law," that USDS has "full and prompt access to all unclassified agency records, software systems, and IT systems." USDS was instructed to "adhere to rigorous data protection standards." The DOGE Executive Order stated that it "shall be implemented consistent with applicable law" and should not "be construed to impair or otherwise affect . . . the authority granted by law to an executive department or agency."

Beginning on January 20, OPM gave individuals working on the DOGE agenda access to at least fourteen OPM systems, most of which contain PII. OPM conducted two early audits of this access, a "February Audit" and a "March Audit," which are inconsistent with each other. June 9 Opinion, 786 F. Supp. 3d at 672. According to the March Audit, twenty DOGE-related

individuals were granted access to OPM systems during the period January 20 to March 6. Almost all of that access was "administrative" access. Id. at 671-72. Meanwhile, internal OPM emails indicate that on January 20 or shortly thereafter, career database administrators in OPM's Office of the CIO had their access revoked.[11] Id. at 677.

DOGE Agents also gained access to data in OPM systems indirectly through career OPM staff. For example, Government email addresses and employee names appearing in certain systems were used to create a government-wide email service, and that data was extracted by OPM career staff and made available to DOGE Agents. Id. at 676. Hogan also testified that OPM career staff may have extracted data for DOGE agents for a retirement services modernization project. Id.

Three of the twenty DOGE-related individuals granted direct access to OPM systems were in leadership positions at OPM: Charles Ezell, the Acting Director; Hogan, the CIO; and Amanda Scales, the Chief of Staff to the OPM Director. Id. at 671. An additional seven -- referred to as the "Group of Seven," in the June 9 Opinion -- tended to have a background in the technology industry, and some were unusually young and inexperienced. Id.

[11] On February 6, Hogan directed that their access should be immediately restored.

at 672-75. Most individuals in the Group of Seven appeared not to work solely or even primarily for OPM, having either performed work for other agencies or not having received paychecks from OPM. Id. The record contains relatively little information regarding the remaining ten individuals, who were referred to as the "Group of Ten" in the June 9 Opinion.

The June 9 Opinion found that the plaintiffs were likely to succeed in showing that individuals working on the DOGE agenda did not need the access that OPM gave them. Id. at 686-90. The record reflects that few of the relevant individuals ever logged in to OPM systems, despite having administrative access to those systems. Id. at 687. Ezell and Hogan made statements indicating that access had been granted in anticipation that it might be needed, which does not qualify as a showing of need under the Privacy Act. Id. at 676, 687. Any "need" for such anticipatory grants of access was also undermined by Hogan's testimony that a request for access can be satisfied within minutes. Id. at 687.

OPM also ignored many of its privacy and cybersecurity safeguards in connection with DOGE Agents. While incoming OPM employees are ordinarily required to complete its Cybersecurity and Privacy Awareness Training, many DOGE Agents only acknowledged their completion of the training weeks after each

of them had been given access to OPM systems. Id. at 674-75, 689. In granting the DOGE Agents administrative access, OPM also violated core cybersecurity principles that it purports to follow, such as the principle of least privilege. Id. at 689.

II. DOGE Agents' Continued Access to OPM Data Systems

As of June 20, 2025, the date that the preliminary injunction was entered in this case, eight DOGE Agents remained at OPM. Four of those DOGE Agents -- Akash Bobba, Nihkil Rajpal, Riccardo Biasini, and Gavin Kilger -- still had mostly administrative-level access to certain OPM systems containing PII. Bobba, Rajpal, and Kilger logged into some of those systems between April and July. December 19 Opinion, 820 F. Supp. 3d at 270.

On multiple occasions, OPM removed permissions from these DOGE Agents shortly before filing reports in this litigation. Id. For example, access to multiple OPM systems was removed for Biasini, Bobba, and Rajpal between July 21 and July 30, not long before the August 1 report. As noted, the corrected September 30 report reflected other permissions that had been overlooked in the August 1 report. Those permissions were removed on August 8, September 22, and September 29. Id. These removals allowed the defendants to represent in their September 30 report

that no DOGE Agents had access to any OPM data systems containing PII, which they maintain remains true today.

By the time the defendants filed their mootness motion on December 5, five Agents remained at OPM. Ezell, Hogan, and Scales had also left OPM. Id. at 268-69. When summary judgment briefing began on March 20, 2026, two DOGE Agents, Peters and Biasini, remained at OPM. As of July 23, only Peters remains at OPM.[12]

Peters was appointed on January 20, 2025 as a Senior Advisor in the OPM Office of the Director. Peters had access to OPM systems containing PII beginning on January 24 and no longer had such access as of June 20, 2025. Peters did not complete OPM's cybersecurity training until April 5, 2026, nearly fourteen months after this case was filed and while summary judgment briefing was underway.

The defendants assert, through three separate declarations including one by Peters himself, that Peters has been an OPM employee at all relevant times and has never been detailed to or from DOGE or USDS.[13] The plaintiffs have submitted conflicting evidence. Such evidence includes a roster of DOGE employees,

[12] Biasini left OPM on July 23, 2026.

[13] The declarations are by Peters; Amy Gleason, Administrator of USDS; and Kimberly Sylke, Supervisory HR Specialist in the Office of the Chief Human Capital Officer.

contractors and detailees that the Government filed in a separate case -- Authors Guild v. National Endowment for the Humanities, No. 25-cv-3923 (CM), ECF No. 122-2 (S.D.N.Y.) -- identifying Peters as a "Detailee (NTEE) (Fixed Term)" to USDS beginning on January 24, 2025. It also includes an article titled "Elon Musk's Demolition Crew," published on February 6, 2025, which states that, according to internal government directories reviewed by ProPublica, Peters had an Executive Office of the President DOGE email address. Peters declares, however, that he has only ever had an OPM email address since joining OPM on January 20, 2025.

III. Additional Procedures Implemented by OPM

As noted, pursuant to the preliminary injunction, the Government filed a report on July 18, 2025 that described procedures that had been put in place by OPM since March 6 to ensure adherence to the requirements of the Privacy Act with respect to any new grant of access permissions by OPM to any records containing the plaintiffs' PII. First, since April, OPM documented "the applicable Privacy Act provision(s) which allow for access to PII in a specified OPM data system for individuals who will be granted access in connection with high profile initiatives, which include projects that could be construed as falling under the 'DOGE agenda.'"

Second, OPM adopted interim protocols "in response to this court's preliminary injunction opinion and order." These protocols were to be followed before granting new access to PII contained in OPM systems to "(1) any [USDS] employee, contractor, or detailee, or (2) any OPM employee, contractor, or detailee hired after January 20, 2025, and who requires access for the primary purpose of working on an initiative or project involving DOGE." The interim protocols were circulated to OPM officials by internal memoranda dated July 18 -- the same day as the defendants' report to the Court.

OPM then formalized the interim protocols described in the July 18 report by incorporating them into OPM's Cybersecurity and Privacy Policy and clarified "that they apply to all new employee[s] and contractors requiring access to OPM systems containing PII." The revised policy was approved by OPM Director Scott Kupor on November 18. An email announcing the policy, including a link to its full terms, was sent to all OPM employees on November 20, four days before the defendants' deadline to file their mootness motion.[14]

In denying that motion, the Court found that the new protocols, however admirable, did not prevent OPM from

[14] At the defendants' request, this deadline was later extended to December 5.

improperly invoking the need-to-be-prepared justification to satisfy the "need to know" criteria of the Privacy Act -- a justification that the Court explicitly rejected. December 19 Opinion, 820 F. Supp. 3d at 273-74. The new protocols also did not ensure that only individuals who are OPM employees within the meaning of the Privacy Act will be given access to OPM systems containing PII, nor did they address circumstances in which individuals may seek to gain indirect access to PII through career OPM staff. Id. at 274.

OPM has since made additional changes to its policies. On May 11, 2026, amidst summary judgment briefing and the parties' settlement negotiations, OPM again revised its Cybersecurity and Privacy Policy to clarify that: (1) only OPM employees and contractors -- not detailees -- may be granted access to OPM systems containing PII, and (2) the protocols apply with equal force to indirect access to PII extracted from OPM systems. That policy change was communicated to all OPM employees on May 15. The relevant section of OPM's Cybersecurity and Privacy Policy now reads:

> The following protocols shall be used for new employees and contractors requiring access to OPM systems containing PII who have a need for the record in performance of their duties and are approved for access pursuant to 5 U.S.C. 552a(b)(1). Only OPM employees and contractors who have a need for such access in the performance of their duties and are approved for access may access OPM systems containing

> PII. Before an individual is provided with access to an OPM system or systems containing PII, the SO [system owner] must take the following steps:
>
> > i. Confirm with CISO [the Chief Information Security Officer] that the person has completed Cybersecurity and Privacy Awareness training and completed [the] Rules of Behavior acknowledgement which are included as part of the training.
> >
> > ii. Confirm with CHCO [the Chief Human Capital Officer] that the individual has been properly appointed or detailed.
> >
> > iii. Confirm with FSEM [Facilities, Services, and Emergency Management] that the individual has been appropriately vetted and they have been cleared for entrance on duty.
> >
> > iv. Confirm with SAOP [Senior Agency Official for Privacy] that the above steps have been taken, provide an explanation for need to access the system(s), and receive written approval from the SAOP that the access fits within the "need to know" criteria of the Privacy Act.
> >
> > v. This policy applies to indirect access to information in systems of records covered by the Privacy Act as well as direct access. That is, employees and third parties who do not have a need for records containing PII in the performance of their duties and are not approved for such access may not seek to obtain such records indirectly.

Additionally, in declarations filed in connection with summary judgment, OPM's current CIO Adam Starr has repudiated the need-to-be-prepared justification for grants of access to OPM systems containing PII. In his declaration of July 6, Starr only repudiated the need-to-be prepared justification for grants of administrative access to OPM systems containing PII and

declared that "OPM will not invoke this justification in the future in granting such access." After the plaintiffs pointed out that his repudiation of the justification had not included grants of non-administrative access, Starr clarified in his declaration of July 28 that "OPM's repudiation of its previously-held 'need-to-be-prepared' rationale for PII access applies to all grants of access to OPM systems, not just administrative access."

Starr's declarations also describe an investigation conducted by OPM's Office of the CIO between May 18 and June 5, 2026 into all prior grants of access to PII to DOGE Agents.[15] The investigation was "undertaken for the purpose of ensuring compliance with Court's previous decisions," and included the following steps:

> (a) Review of system audit logs, access logs, and account-provisioning records for OPM records systems containing PII for the period from January 20, 2025 through June 5, 2026;
>
> (b) review of the accounts and credentials issued to personnel associated whose access is at issue in this litigation;
>
> (c) review of data-loss-prevention, network egress, and download/export logs for indications that records

[15] OPM's investigation was conducted after the plaintiffs pointed out in their April 15 brief that DOGE affiliates at the Social Security Administration (SSA) mishandled the PII to which they had been given access.

> were copied, extracted, or transmitted outside OPM systems; and
>
> (d) verification of the current status of all such accounts and credentials.
>
> According to Starr,
>
> OPM's review did not reveal evidence that [DOGE Agents] used system access to export, copy, transfer, or transmit OPM records containing Plaintiffs' PII outside OPM systems. OPM's review likewise did not identify any OPM records or datasets extracted from OPM systems and made available to DOGE-affiliated personnel outside authorized OPM environments.

As part of the review, "OPM also confirmed that any access inconsistent with OPM's current access protocols has been removed, disabled, or otherwise addressed." As a result of these findings, OPM determined that no remediation was warranted.

Discussion

The parties cross-move for summary judgment on the plaintiffs' claims arising from OPM's decision to grant the DOGE Agents access to systems containing the plaintiffs' PII. In addition to arguing the merits, the defendants renew several threshold arguments previously addressed by the Court, including that the plaintiffs lack standing, subsequent developments have rendered this case moot, the plaintiffs have not challenged a final agency action, and the Privacy Act provides an adequate

alternative remedy. These threshold arguments are addressed first.

I. Jurisdiction

A. Standing

"[B]ecause subject-matter jurisdiction is a 'threshold question,' it must be answered before any treatment of a case's merits can be undertaken." Molecular Dynamics, Ltd. v. Spectrum Dynamics Med. Ltd., 143 F.4th 70, 80-81 (2d Cir. 2025) (citation omitted). Article III of the Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies," U.S. Const. art. III, § 2, "which requires, among other things, that a plaintiff sustain the burden of establishing standing." Marcavage v. City of New York, 689 F.3d 98, 103 (2d Cir. 2012) (citation omitted). The doctrine of standing generally assesses whether, at the outset of the litigation, the parties have a legally cognizable interest in the outcome of the case. Stafford v. Int'l Bus. Machines Corp., 78 F.4th 62, 67 (2d Cir. 2023).

The June 9 Opinion held that, at the preliminary injunction stage, the plaintiffs had standing because the challenged access to their sensitive PII caused a concrete injury analogous to intrusion upon seclusion, which could be redressed by an injunction prohibiting further improper disclosures and

requiring the impoundment and destruction of any improperly copied information. 786 F. Supp. 3d at 682–83; see also December 19 Opinion, 829 F. Supp. 3d at 276 (incorporating that reasoning). The defendants do not seriously contest the Court's prior standing holding, incorporating their prior arguments only to preserve them for appeal. The Court therefore adheres to its prior ruling for the reasons contained therein.

B. Mootness

The defendants do contend, however, that recent developments have mooted this case. "Mootness is 'standing set in a time frame.'" Stafford, 78 F.4th at 67 (2d Cir. 2023) (quoting Arizonans for Off. Eng. v. Arizona, 520 U.S. 43, 68 n.22 (1997)). While the doctrine of standing generally assesses whether the parties have a legally cognizable interest in the outcome "at the outset," the "doctrine of mootness considers whether it exists throughout the proceedings." Id. (quoting Uzuegbunam v. Preczewski, 592 U.S. 279, 282 (2021)). A case therefore becomes moot "when the issues presented are no longer live or the parties lack a legally cognizable interest in the outcome, making it impossible for a court to grant any effectual relief whatever to the prevailing party." Doe v. McDonald, 128 F.4th 379, 385 (2d Cir. 2025) (citation omitted).

As a general matter, a defendant's "voluntary cessation of a challenged practice does not deprive a federal court of its power to determine the legality of the practice." Mhany Mgmt., Inc. v. Cnty. of Nassau, 819 F.3d 581, 603 (2d Cir. 2016) (citation omitted). Otherwise, a defendant could strategically alter its conduct to prevent or undo an adverse ruling. Exxon Mobil Corp. v. Healey, 28 F.4th 383, 395 (2d Cir. 2022). To establish mootness based on voluntary cessation, a defendant must demonstrate both that "(1) there is no reasonable expectation that the alleged violation will recur and (2) interim relief or events have completely and irrevocably eradicated the effects of the alleged violation." Neurological Surgery Prac. of Long Island, PLLC v. HHS, 145 F.4th 212, 223 (2d Cir. 2025) (citation omitted). This is a "formidable burden." FBI v. Fikre, 601 U.S. 234, 241 (2024) (citation omitted). The defendants have not carried it.

The developments since December when the Court last ruled that this case was not moot have been significant. All but one DOGE Agent has left OPM, and no DOGE Agent has had access to OPM systems containing PII since September 2025. The DOGE Temporary Organization's 18-month term has expired. OPM has revised its policies and repudiated the need-to-be-prepared rationale for granting any type of access to OPM systems of records containing

PII. But several considerations prevent a finding that the issues being litigated here are moot.

First, OPM continues to maintain that all DOGE Agents who received access permissions to OPM's systems of records containing PII were "OPM employees who had a need for that access in the performance of their duties." That includes the argument, drawn from Am. Fed'n of Tchrs. v. Bessent, 152 F.4th 162, 176 (4th Cir. 2025), vacated, 172 F.4th 361 (4th Cir. 2026) (en banc), that the breadth of the DOGE mandate itself justified broad access. A defendant's "insistence on the validity of the challenged practice" makes recurrence reasonable to expect. Ahrens v. Bowen, 852 F.2d 49, 53 (2d Cir. 1988); see also June 9 Opinion, 786 F. Supp. 3d at 694 ("Without a full-throated recognition that the law and established cybersecurity procedures must be followed, the risk of irreparable harm will continue to exist.").

Second, the timing of OPM's revisions to its policies closely tracks this litigation's deadlines, suggesting that they are driven more by a desire to resolve this case than by a genuine departure from its prior conduct. Compare Neurological Surgery Prac., 145 F.4th at 224 (noting that the government action that mooted the claim was "wholly unrelated to th[e] litigation"). OPM repeatedly removed access permissions for the

DOGE Agents shortly before court reports were due. OPM circulated its November 2025 policy days before its mootness motion was due. It revised its policies again amid summary judgment briefing and settlement negotiations. And Starr, OPM's third CIO since this case began, at last repudiated the need-to-be-prepared justification for granting any type of access to OPM's systems of records containing PII in a declaration attached to the defendants' sur-reply. He had repudiated the justification for administrative access only in a declaration submitted just two weeks prior. "To the extent that the voluntary cessation doctrine exists primarily to keep parties from acting strategically to avoid judicial review," Ruesch v. Comm'r of Internal Revenue, 25 F.4th 67, 71 (2d Cir. 2022), OPM's behavior, while undoubtedly commendable, appears designed to do just that.

The same cannot be said about the termination of the DOGE Temporary Organization, as its July 4, 2026 end date was fixed by the DOGE Executive Order rather than adopted in response to this litigation. This development therefore carries particular weight in the mootness analysis. That said, the DOGE Executive Order provides that the Organization's termination does not "imply the termination, attenuation, or amendment of any other authority or provision of this order." USDS continues to

operate within the Executive Office of the President, and the Executive Order's directive that agencies give USDS "full and prompt access" to their records remains in effect. The termination thus narrows, but does not eliminate, the circumstances in which the challenged conduct could recur.

Lastly, Peters remains at OPM. The parties dispute whether he was an OPM employee or detailed from USDS during the relevant period. Although Peters currently does not have access permissions to any of OPM's systems of records containing PII, OPM has committed only that it will not grant him access "except in conformity with" its policies and applicable law. That assurance carries little weight, given that the defendants engaged in the challenged conduct notwithstanding the existence of policies and law prescribing their actions. And even though OPM has strengthened their access protocols considerably in response to this litigation, "it is ultimately no more difficult for OPM to ignore these new protocols than to ignore its old procedures." December 19 Opinion, 820 F. Supp. 3d at 273.

This conclusion does not diminish OPM's admirable efforts during this litigation to strengthen its protocols. But the misconduct at issue in this litigation was not attributable to deficient procedures or a lack of clarity regarding the law. Rather, it resulted from the failure of particular individuals

to abide by the Privacy Act and to honor the safeguards already in place at OPM. The effectiveness of any law and such government safeguards ultimately depends on the fidelity of those entrusted to observe and enforce them, and even the most rigorous procedures cannot secure compliance by those willing to disregard them.

Whether a case is moot and whether an injunction should issue, however, are "analytically distinguishable" questions governed by different burdens. SCM Corp. v. F.T.C., 565 F.2d 807, 812 (2d Cir. 1977). To obtain an injunction, the burden is on the plaintiff to show that relief is needed. That requires "some cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive." Id. (quoting United States v. W.T. Grant Co., 345 U.S. 629, 633 (1953)). The developments described above fall short of mooting the case. Whether they defeat the plaintiffs' request for a permanent injunction, however, is a separate issue.

II. Reviewability under the APA

The defendants incorporate their arguments that the plaintiffs have not challenged final agency action and that the Privacy Act provides an adequate alternative remedy. The Court previously rejected both. June 9 Opinion, 786 F. Supp. 3d at 690–92; April 3 Opinion, 777 F. Supp. 3d at 279–82. The

defendants do not seriously contest the Court's prior rulings, incorporating their prior arguments only to preserve them for appeal. The Court therefore adheres to its prior rulings for the reasons explained therein.

III. The Merits

A. APA Claims

Under the APA, a court must "hold unlawful and set aside agency action" that is "not in accordance with law." 5 U.S.C. § 706(2)(A). The June 9 Opinion concluded that the plaintiffs were likely to succeed in showing that OPM's broad grant of access to DOGE Agents to its systems of records containing PII violated two provisions of the Privacy Act -- 5 U.S.C. § 552a(b), which prohibits certain disclosures of records, and 5 U.S.C. § 552a(e)(10), which imposes a duty to establish appropriate safeguards to ensure the security and confidentiality of records. 786 F. Supp. 3d at 683–93. At this point, there is no meaningful dispute concerning the underlying conduct. The defendants barely defend its legality, relying instead on what has happened since to argue that the case is moot and that prospective relief is unnecessary. The Court therefore reaches the same conclusions on the merits of the plaintiffs' APA claims for the reasons stated in the June 9 Opinion, which are incorporated here. Id. OPM's decision to

grant DOGE Agents broad access to its systems of records containing PII without a demonstrated need was unlawful; because all the access permissions have been rescinded, those permissions need not be set aside.

In their briefing, the defendants reiterate their argument that the nature of the DOGE Agents' modernization responsibilities under the DOGE Executive Order provided the necessary justification for access to OPM records systems. But the June 9 Opinion already concluded that "IT modernization does not necessarily require access to confidential PII," much less administrative access. 786 F. Supp. 3d at 688. In fact, one of the plaintiffs' experts, former OPM CIO David Nesting, testified to participating in modernization efforts at two federal agencies without ever obtaining access to PII contained in the systems being modernized. The defendants do not explain why modernization efforts by the DOGE Agents at OPM needed to proceed differently. The record also provides no support for a finding that it was the pursuit of a modernization agenda that prompted OPM to grant sweeping and expedited access to a score of DOGE Agents to its systems of records containing PII.

The defendants also rely on Am. Fed'n of Tchrs. v. Bessent, which reasoned at the preliminary injunction stage that an employee with broad and open-ended duties may need

correspondingly broad access to its employer's systems. 152 F.4th at 176–77. Even accepting that premise, need still depends on the duties actually being performed. Id. at 176. The record here contains no contemporaneous explanation connecting any DOGE Agent's duties to the access granted. Instead, the record contains testimony from OPM's then-CIO explaining that access was only granted in case it might be needed.[16]

Lastly, the defendants argue that because the plaintiffs seek prospective relief, only the DOGE Agents who remain at OPM -- now just Peters -- are "relevant at this juncture." The defendants therefore urge the Court to rule only on the legality of OPM's decision to grant Peters access to its systems of records containing PII. But the defendants' argument conflates liability with remedy. Which individuals remain at OPM today

[16] The defendants also briefly mention OPM's organic statute, which requires the OPM Director to "advis[e] the President on actions which may be taken to promote an efficient civil service," 5 U.S.C. § 1103(a)(7), and OPM to "design a set of systems, including appropriate metrics, for assessing the management of human capital by Federal agencies," id. § 1103(c)(1), to further justify the access provided to DOGE Agents. This argument is a post hoc rationalization offered for the first time in summary judgment briefing. See Dep't of Com. v. New York, 588 U.S. 752, 780 (2019) ("[I]n reviewing agency action, a court is ordinarily limited to evaluating the agency's contemporaneous explanation in light of the existing administrative record."). Nonetheless, the defendants fail to explain how the statute justifies giving the DOGE Agents administrative access to the confidential PII at issue here.

bears on what relief is appropriate, not on whether OPM's decision to grant DOGE Agents access to its systems of records containing PII violated the law.[17]

Because OPM's grants of access violated §§ 552a(b) and (e)(10) of the Privacy Act, they were "not in accordance with law." 5 U.S.C. § 706(2)(A). The plaintiffs' motion for summary judgment is therefore granted as to their APA claims, and the defendants' cross-motion as to this claim is denied.

B. Ultra Vires Claim

The defendants move for summary judgment on the plaintiffs' ultra vires claim against the DOGE Defendants. Non-statutory ultra vires review is a narrow doctrine, unavailable where "a statutory review scheme provides aggrieved persons 'with a meaningful and adequate opportunity for judicial review.'" NRC v. Texas, 605 U.S. 665, 682 (2025) (citation omitted). The APA has afforded the plaintiffs review and relief here. June 9 Opinion, 786 F. Supp. 3d at 693. The defendants' motion for summary judgment is therefore granted as to this claim.

IV. Remedy

In their opening brief, the plaintiffs sought an order "vacat[ing] and set[ing] aside OPM's systematic practice of

[17] The defendants reiterate other arguments that they made in connection with the preliminary injunction, and they are rejected for the reasons contained in the June 9 Opinion.

disclosing records to DOGE agents, regardless of need, employment status, training, or cybersecurity safeguards, and an injunction and declaration doing the same." By the time of their reply, the plaintiffs requested that the Court decide whether the plaintiffs are entitled to relief and then seek input from the parties regarding the precise terms of relief.

By virtue of the Court's summary judgment ruling, OPM's decision to grant DOGE Agents broad access to its systems of recordings containing PII has been held unlawful. As noted above, because all the access permissions have been rescinded, that access need not be vacated or set aside.

Although the Court issued a preliminary injunction in June 2025, that determination does not establish whether permanent injunctive relief is appropriate. Accordingly, the Court must independently assess what, if any, permanent injunctive relief is warranted in light of the record now before it, including material developments occurring since the preliminary injunction was entered. Voluntary cessation may be insufficient to establish mootness, but it remains an "important factor" in determining whether an injunction is warranted. Friends of the Earth, Inc. v. Laidlaw Env't Servs. (TOC), Inc., 528 U.S. 167, 193 (2000) (citation omitted). The Court will therefore solicit the parties' views on what relief, if any, is appropriate under

the circumstances. In the meantime, the parties are encouraged to confer and explore whether they can reach an agreement on an appropriate resolution.

Conclusion

The defendants' March 20, 2026 motion for summary judgment is granted as to the ultra vires claim and otherwise denied. The plaintiffs' April 15, 2026 cross-motion for summary judgment on their APA claims is granted. The scope of relief, if any, will be addressed by separate order.

Dated: New York, New York
October 20, 2026

DENISE COTE
United States District Judge