

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

```
----- X
:
AMERICAN FEDERATION OF GOVERNMENT :
EMPLOYEES, AFL-CIO, et al.,      :
:                                : 25cv1237 (DLC)
Plaintiffs,                      :
:                                :
-v-                              :  OPINION AND
:                                :  ORDER
:                                :
U.S. OFFICE OF PERSONNEL MANAGEMENT, :
an agency of the United States, et   :
al.,                                :
:                                :
Defendants.                        :
:                                :
----- X
```

APPEARANCES:

For plaintiffs:

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

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

Andrew H. Warren
Norman L. Eisen
State 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:

Jeffrey Oestericher
 David E. Farber
 United States Attorney's Office, Southern District of New York
 86 Chambers Street, 3rd Floor
 New York, NY 10007

Table of Contents

Procedural History.....	4
Findings of Fact.....	14
I. Risks and Protections Applicable to OPM's Systems of Records	15
A. The Privacy Act	15
B. Dangers of Cybersecurity Breaches	18
C. Cybersecurity Standards and Practices	21
1. Vetting and Background Investigations	23
2. Training	23
3. Access Control Policies	27
D. Systems of Records at OPM	30
E. Efforts to Modernize Government Technology	33
II. Recent Events	36
A. The DOGE Executive Order	36
B. The Government-Wide Email System	38
C. Disclosure to Twenty Individuals	39
1. The Group of Seven	42
2. The Group of Ten	47
3. Use of Access to OPM Systems	48
4. Chronology of Disclosure	49
Conclusions of Law.....	52
I. Article III Standing	53
A. Injury in Fact	54
1. Onboarding Process	59
2. Access to OPM Systems	61

3.	Impending Risk of Harm	64
B.	Causation and Redressability	66
II.	Preliminary Injunction	67
A.	Likelihood of Success on the Merits	69
1.	Violations of the Privacy Act	69
i.	Illegal Disclosure.....	69
(a)	Disclosure.....	74
(b)	Employment Status.....	75
(c)	Need to Review.....	77
ii.	Lack of Appropriate Safeguards.....	83
2.	Availability of Review Under the APA	85
i.	Final Agency Action.....	87
ii.	Inadequacy of Alternative Remedies.....	90
3.	Ultra Vires Review	91
B.	Irreparable Harm	93
C.	Public Interest	98
	Conclusion.....	99

DENISE COTE, District Judge:

The U.S. Office of Personnel Management (“OPM”) maintains systems of records that contain the personal information of tens of millions of Americans, including past, current, and aspiring federal employees. Following President Trump’s inauguration, OPM granted broad access to many of those systems to a group of individuals associated with the Department of Government Efficiency (“DOGE”), even though no credible need for this access had been demonstrated. In doing so, OPM violated the law and bypassed its established cybersecurity practices.

Current and former federal government employees and their unions have sued OPM and other defendants for breaches of privacy. The plaintiffs have moved for a preliminary injunction that would stop disclosure of OPM records to individuals associated with DOGE and require the destruction of any copies of personal information that have been obtained through such disclosure. The plaintiffs have shown that they are entitled to a preliminary injunction that grants some of the relief they request.

Procedural History

This action was filed on February 11, 2025. 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 Administrative Procedure Act, 5 U.S.C. § 701 et seq. ("APA"); and an ultra vires claim. There are two sets of defendants: the "OPM Defendants," which consist of OPM and its 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.

The plaintiffs seek injunctive relief and a declaration that the decision to implement a system by which DOGE agents have access to OPM's records and the plaintiffs' personal

information contained in those records is unlawful. The plaintiffs do not seek damages. They request the following injunction:

(1) OPM Defendants are enjoined from disclosing to DOGE Defendants, including all DOGE agents,¹ 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 organizations;

(2) OPM Defendants are enjoined to ensure future disclosure of individual records will occur only in accordance with the Privacy Act and the Administrative Procedure Act;

(3) DOGE Defendants, including all DOGE agents, are enjoined to impound and destroy all copies of Plaintiffs' and union Plaintiffs' members' personal information that OPM has disclosed to them;

(4) OPM Defendants are enjoined 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; and

(5) Defendants are enjoined to file a status report within 48 hours of the issuance of this Order indicating whether any DOGE Defendants or agents continue to have access to any OPM systems that contain records and whether DOGE Defendants, including all DOGE agents, have destroyed all copies of Plaintiffs' and Plaintiffs' members' records.

¹ In requesting an injunction, the plaintiffs define DOGE agents as "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."

The plaintiffs are individuals currently or formerly employed by the federal Government and unions representing federal Government employees. The three named individual plaintiffs are a current federal employee working for the Brooklyn Veterans Affairs Medical Center and two former federal employees. The two union plaintiffs are the American Federation of Government Employees, AFL-CIO ("AFGE") and the Association of Administrative Law Judges, International Federation of Professional and Technical Engineers Judicial Council 1, AFL-CIO ("AALJ").

On February 14, the plaintiffs brought a motion for a temporary restraining order ("TRO"). That motion was accompanied by declarations from Everett Kelley, national president of AFGE; Sommattie Ramrup, president of AALJ; and Deborah Toussant, a retired federal employee who is one of the named individual plaintiffs. The plaintiffs sought a TRO that, among other things, would prohibit the disclosure of protected OPM records to "DOGE-affiliated agents." The defendants filed an opposition on February 19, which was accompanied by a declaration from Gregory Hogan, OPM's Chief Information Officer ("CIO"). In their opposition, the defendants requested that the motion for a TRO be converted into a motion for a preliminary injunction. Instead of filing a reply, the plaintiffs joined

that request on February 23 and indicated that they would seek expedited discovery.

Meanwhile, orders had been issued against the federal Government in other DOGE-related litigation, including in an action proceeding in the District of Maryland against OPM, the Department of the Treasury ("Treasury"), and the Department of Education ("DOE") for violations of the Privacy Act and the APA.² There, on February 24, the court issued a TRO enjoining OPM from disclosing the plaintiffs' personally identifiable information ("PII") "to any OPM employee working principally on the DOGE agenda who has been granted access to OPM records for the principal purpose of implementing the DOGE agenda," with the exception of Hogan. Am. Fed'n of Tchrs. v. Bessent ("Maryland OPM Action"), No. 25cv430, 765 F. Supp. 3d 482, 506 (D. Md. 2025). On March 24, the District of Maryland converted the TRO to a preliminary injunction.³ On April 7, the Fourth Circuit

² In an action brought against OPM and Treasury in the Eastern District of Virginia under the Privacy Act and the APA, a TRO was denied on February 21. Elec. Priv. Info. Ctr. v. OPM ("Virginia OPM Action"), No. 25cv255, 2025 WL 580596 (E.D. Va. Feb. 21, 2025).

³ The preliminary injunction enjoined OPM from disclosing PII "to any DOGE affiliates, defined as 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," with the exception of Hogan, Ezell, and then-Chief of Staff Amanda Scales. Maryland OPM Action, 2025 WL 895326, at *33.

stayed that injunction pending appeal. Am. Fed'n of Tchrs. v. Bessent, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025).⁴

The plaintiffs in the instant action filed a motion for expedited discovery on February 27, which became fully submitted on March 6. The defendants opposed the motion, arguing that it was premature for the plaintiffs to seek discovery before the administrative record had been produced. OPM had already been ordered to produce an administrative record in the Maryland OPM Action. Maryland OPM Action, ECF No. 46. This Court's Order of March 7 instructed the defendants to provide the plaintiffs with the administrative record and other relevant materials produced

⁴ Several actions have been brought under the Privacy Act and the APA that do not name OPM as a defendant. A preliminary injunction limiting access to records by individuals affiliated with DOGE was issued in New York v. Trump, No. 25cv1144, 2025 WL 573771 (S.D.N.Y. Feb. 21, 2025) (Treasury). Such an injunction was also issued in Am. Fed'n of State, Cnty., & Mun. Emps. v. SSA ("Maryland SSA Action"), No. 25cv596, 2025 WL 1141737 (D. Md. Apr. 17, 2025) (Social Security Administration ("SSA")). A stay pending appeal of the injunction issued in the Maryland SSA Action was denied by the Fourth Circuit and then granted by the Supreme Court. Am. Fed'n of State, Cnty., & Mun. Emps. v. SSA, No. 25-1411, 2025 WL 1249608 (4th Cir. Apr. 30, 2025); SSA v. Am. Fed'n of State, Cnty. & Mun. Emps., No. 24A1063, 2025 WL 1602349 (U.S. June 6, 2025). Preliminary relief has been denied in the following actions: Am. Fed'n of Lab. v. Dep't of Lab. ("D.C. DOL Action"), No. 25cv339, 2025 WL 542825 (D.D.C. Feb. 14, 2025) (Department of Labor ("DOL"), Department of Health and Human Services ("HHS"), and Consumer Financial Protection Bureau ("CFPB")); Univ. of Cal. Student Ass'n v. Carter, No. 25cv354, 2025 WL 542586 (D.D.C. Feb. 17, 2025) (DOE); All. for Ret. Ams. v. Bessent, No. 25cv313, 2025 WL 740401 (D.D.C. Mar. 7, 2025) (Treasury).

in the Maryland OPM Action. The Government produced the administrative record in the Maryland OPM Action on March 7 and supplemented that production on March 14; on both occasions, Hogan certified that the administrative record was complete and contained “non-deliberative documents and materials directly or indirectly considered regarding the OPM actions challenged in this case.” Maryland OPM Action, ECF Nos. 51, 64.

The defendants in the instant action filed a motion to dismiss the complaint on March 14, and that motion 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 (“April 3 Opinion”), No. 25cv1237, 2025 WL 996542 (S.D.N.Y. Apr. 3, 2025).⁵ The Opinion found, among other things, 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 who did not have a need for such access in the performance of their duties at OPM. Id. at *10-14.

⁵ A motion to dismiss was also largely denied in the D.C. DOL Action. 2025 WL 1129227 (DOL, HHS, and CFPB).

The Court then adopted the parties' proposed schedule for the defendants to produce supplemental administrative record materials and for the plaintiffs to move for a preliminary injunction. An Order of April 28 set a preliminary injunction hearing for May 29.

OPM filed an updated administrative record on April 23. Unlike in the Maryland OPM Action, Hogan did not certify the completeness of the administrative record in this action, and the Government has represented that it is not necessarily complete. The administrative record also does not provide information about events after March 6. The administrative record includes documents and emails related to the onboarding, vetting, and training of DOGE-related individuals at OPM; a copy of OPM's Cybersecurity and Privacy Awareness Training; spreadsheets reflecting access permissions to OPM systems; OPM regulations implementing the Privacy Act; and a February 28, 2025 Privacy Impact Assessment ("PIA") for OPM's creation of the Government-Wide Email System ("GWES").

The plaintiffs filed a motion for a preliminary injunction on April 25. The motion was accompanied by declarations of three witnesses with experience in information technology and cybersecurity: Ann Lewis, the former Director of Technology Transformation Services in the U.S. General Services

Administration ("GSA"); David Nesting, the former Deputy Chief Information Officer at OPM and the former Director of Engineering at the U.S. Digital Service; and Bruce Schneier, an author of various books and articles on cybersecurity who is currently, among other positions, a fellow at Harvard's Berkman Klein Center for Internet and Society. Exhibits attached to an attorney declaration included filings in other DOGE-related litigation, news articles, PIAs conducted by OPM, and letters to and from Government officials.

The defendants filed an opposition on May 16. It was accompanied by three declarations of OPM employees: a supplementary declaration from Hogan; a declaration from Everette R. Hilliard, OPM's Director of Facilities, Security, and Emergency Management; and a declaration from Carmen Garcia-Whiteside, OPM's Chief Human Capital Officer. Hogan's supplementary declaration provides additional information about access to and safeguarding of OPM's data systems. Hilliard describes OPM's processes for vetting and credentialing and how those processes were applied for certain DOGE-related individuals. Garcia-Whiteside provides information about the appointments and training of those individuals.

The plaintiffs filed a reply on May 23. It was accompanied by a second declaration from Nesting and more news articles.

In letters of May 14 and 21, the parties disagreed as to whether the plaintiffs were entitled to cross-examine Hogan at the preliminary injunction hearing. An Order of May 22 warned that, should Hogan not be present for cross-examination, the parties would be heard as to whether his declaration should be stricken or an inference should be drawn against the statements made therein. On May 23, the defendants gave notice that Hogan would be available for cross-examination..⁶

The preliminary injunction hearing was held on May 29. The declarations filed in support of and in opposition to the motion were received as direct testimony of the witnesses. Nesting and Hogan⁷ testified and were subject to cross-examination. The Government objected to questions that were beyond the scope of the administrative record that it had chosen to produce.

During the parties' summations, the Court observed that the parties agreed on many fundamental principles. There is no dispute that OPM has an obligation to safeguard its data

⁶ At a conference on May 27, the Government explained that it sought to cross-examine Schneier and Lewis about their reliance on press reports. The Government had not given timely notice of its desire to cross-examine these witnesses and they were not able to attend the May 29 hearing. The Court ruled that the hearing would proceed without them but the Government's objections regarding news reports would be heard at the hearing.

⁷ With consent of the plaintiffs, Hogan testified by video conference from Washington, D.C.

systems, and that a new President should be able to put his priorities into effect so long as there is compliance with the law. The parties agreed to confer until June 2 to determine whether any agreement could be reached. On the evening of June 2, the parties reported that they had not reached an agreement. Accordingly, this Opinion addresses the plaintiffs' motion for a preliminary injunction.

The findings of fact for this preliminary injunction appear throughout this Opinion but are set forth in detail in the following section. The findings are principally drawn from the administrative record compiled by the Government and the documents, including declarations, filed by the parties.

The Government has objected that some of the material submitted by the plaintiffs is inadmissible hearsay, including press accounts of DOGE activities at OPM. See Ezrasons, Inc. v. Travelers Indem. Co., 89 F.4th 388, 393 n.3 (2d Cir. 2023) (news reports are inadmissible hearsay when offered to prove the truth of what they state). The "admissibility of hearsay under the Federal Rules of Evidence goes to weight, not preclusion, at the preliminary injunction stage." Mullins v. City of New York, 626 F.3d 47, 52 (2d Cir. 2010). Thus, a court determining whether to grant a preliminary injunction may consider hearsay evidence in news reports, Havens v. James, 76 F.4th 103, 123 (2d Cir.

2023), or hearsay evidence in affidavits filed in other courts. We The Patriots USA, Inc. v. Hochul, 17 F.4th 266, 276 n.3 (2d Cir. 2021).

Nonetheless, news reports were not received into evidence for the truth of the matters contained in those reports, with two exceptions. This Opinion describes individuals' prior employers and the use of GWES, as reflected in news reports. The defendants have made no specific objection to drawing on news reports for those facts, which are not disputed. To the extent that the contents of news reports appear in this Opinion, they are identified as such.

Findings of Fact

The findings of fact are divided into two sections. The first section describes the risks to privacy and security that arise from the Government's creation of computerized databases and the protections that the Government has developed to mitigate those risks. There is no apparent dispute regarding the description of either the risks or the systems developed to protect against those risks. Indeed, much of this description is drawn from congressional reports and OPM's own documents. The second section describes events that have transpired since President Trump's inauguration, including the access that OPM gave to its systems to individuals working on the DOGE agenda.

I. Risks and Protections Applicable to OPM's Systems of Records

A. The Privacy Act

Many of the issues in this litigation hinge on an understanding of the Privacy Act of 1974. The Act recognizes both the Government's need for computerized systems containing private information and the risks to individual privacy associated with those systems.

In enacting the Privacy Act, Congress proclaimed that "[t]he right to privacy is a personal and fundamental right protected by the Constitution of the United States." Privacy Act of 1974, Pub. L. No. 93-579 ("Privacy Act"), § 2(a)(4), 88 Stat. 1896. The House Report explained that the Fourth Amendment to the Constitution confers "as against the Government, the right to be let alone" and bars "unjustifiable intrusion by the Government upon the privacy of the individual." H.R. Rep. No. 93-1416, at 10 (1974) (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). Although the Privacy Act confers a modern right to privacy with respect to information in Government computer systems, Congress viewed the Act as building on a long constitutional history of protecting individual privacy:

The broad principles involved in what is conveniently called "the individual right of privacy" are deeply rooted in our history and derived from the Bill of

Rights of the United States Constitution. The fourth amendment to the Constitution was written as the result of the American colonial experience with warrants and writs issued under King George III of England which often gave his officers an excuse to search anyone, anywhere, any time.

Id. at 9.

In crafting the Privacy Act, Congress was concerned by the federal Government's abuse of technology for surveillance of individuals. The "McCarthy Era" of the 1950s had involved "numerous examples of privacy invasion affecting Federal employees and the public in their dealings with Federal agencies." Id. at 5. Later, investigations related to Watergate had revealed the existence of "White House enemies' lists," wiretapping of Government employees and news reporters, and other acts of political surveillance. Id. at 8-9. In Congress' view, these events and others had raised the specter of "Big Brother" Government monitoring. Id. at 4, 7.

The Privacy Act reflects these concerns and applies them to the computerization of Government recordkeeping. Its preamble states that the "privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and that the "increasing use of computers" had "greatly magnified the harm to individual privacy that can occur." Privacy Act, § 2(a)(1)-(2). Congress deemed it necessary "to regulate the collection,

maintenance, use, and dissemination of information collected by . . . agencies.” Id. § 2(a)(5). As explained in the Senate Report,

a special status must be accorded to the issue of individual privacy, that is, the right of an individual to have such gathering of personal information as may be collected by the Government confined to that for which there is a legitimate use, and then secondly, after it is gathered, to have access to that information confined to those who have a governmental end in view for its use, and thirdly, to be assured by government that there is as little leakage as possible to unauthorized persons.

S. Rep. No. 93-1183, at 15 (1974).

Congress recognized at the same time that “the increasing use of computers and sophisticated information technology” is “essential to the efficient operations of the Government.” Privacy Act, § 2(a)(2). The Senate Report acknowledged that computers are “absolutely essential to the proper transaction of many government programs, and that the collection of information from the individual is absolutely necessary to carry out those programs.” S. Rep. No. 93-1183, at 15 (1974). Thus, the Privacy Act “strikes a balance between governmental needs and the personal freedoms of the individual.” Id.

That balance is reflected in a prohibition against agency disclosure of records that is at the heart of the Privacy Act. The Act states:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains[.]

5 U.S.C. § 552a(b). That provision is followed by a series of exceptions. The exception of importance to the parties in this litigation permits disclosure “to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” Id. § 552a(b)(1) (emphasis supplied). These provisions of the Privacy Act are discussed in more detail below.

B. Dangers of Cybersecurity Breaches

The Government recognizes at least three types of cybersecurity breaches that can occur in systems like OPM’s that contain sensitive data. These risks are explained to OPM employees in OPM’s Cybersecurity and Privacy Awareness Training.

First, a confidentiality breach occurs if private data is improperly accessed or copied. The possible consequences of a confidentiality breach include identity theft, stalking, retaliation, loss of assets, and blackmail. Because it may be impossible to claw back stolen data, the harm to an individual stemming from a confidentiality breach can be permanent.

Second, an integrity breach occurs if data is improperly modified or destroyed. Integrity breaches in OPM systems could,

for example, disrupt benefit payments or impact promotions and job security. An integrity breach can also consist of a malicious actor creating a "backdoor" that facilitates their future access to a system.

Third, an availability breach occurs if access to data is disrupted. This could occur either if specific data is deleted, even on a temporary basis, or if an entire system is made unavailable. An availability breach of OPM systems could, for example, interrupt the regular payment of federal retirement annuities, which would affect three million households who rely on those payments.

OPM experienced a serious cybersecurity breach in 2015. That breach resulted in attackers obtaining security clearance background information for over 21 million individuals, which has grave implications for espionage and national security. The breach also affected the personnel files of over four million individuals employed by the Government. The direct federal costs resulting from the breach exceeded \$500 million for remediation and identity protection services.

In 2016, the House Committee on Oversight and Government Reform published a report about the 2015 OPM breach, titled "The OPM Data Breach: How the Government Jeopardized Our National

Security for More than a Generation" ("2016 House Report").⁸ It described the breach as an "unthinkable event" for which "tens of millions of federal employees and their families paid the price." It stated that "the damage done to the Intelligence Community will never be truly known."

The 2016 House Report explained that at least two hackers were involved. OPM was able to detect that the first hacker had moved data out of its network, and kicked that hacker out of its system. But a second hacker used a contractor's credentials to log in to OPM's network. The second hacker installed malware that created a backdoor to the network and obtained administrative credentials, all the while evading detection.

The 2016 House Report concluded that the breach had been made possible by a lack of "basic, required security controls." It blamed the breach on a "longstanding failure of OPM's leadership to implement basic cyber hygiene," and stated that this was ultimately "a failure of culture and leadership, not technology." The report also listed actions that OPM had begun to take in an effort to enhance its cybersecurity, including deploying the use of two-factor authentication, creating a team of cybersecurity specialists who reported to the Chief

⁸ Available at <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>.

Information Security Officer ("CISO"), and enhancing its cybersecurity training.

C. Cybersecurity Standards and Practices

Federal agencies are required to uphold standards for reducing the risk of cybersecurity breaches. In particular, OPM's Cybersecurity and Privacy Awareness Training instructs its staff to be aware of the Federal Information Security Management Act ("FISMA") and Circular A-130. OPM describes these as "key laws and regulations significant to OPM information security."

FISMA makes the head of each agency responsible for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" agency information. 44 U.S.C. § 3554(a)(1)(A). It requires each agency to "develop, document, and implement an agency-wide information security program" approved by the Director of the Office of Management and Budget ("OMB"). Id. § 3554(b).

FISMA also requires the head of each agency to ensure the agency's compliance with cybersecurity standards that are promulgated by the Department of Commerce's ("DOC") National Institute of Standards and Technology ("NIST"). Id. § 3554(a)(1)(B)(i); 40 U.S.C. § 11331. NIST standards for

reducing the risk of cybersecurity breaches are documented in NIST Special Publication 800-53 ("NIST SP 800-53"), titled "Security and Privacy Controls for Information Systems and Organizations."⁹ OPM's CIO is tasked with ensuring compliance with NIST standards and designating an information security officer who has "information security duties as that official's primary duty." 44 U.S.C. § 3554(a)(3), (a)(3)(A)(iii).

Required cybersecurity standards are also set forth in Circular A-130, titled "Managing Information as a Strategic Resource,"¹⁰ which is issued by OMB pursuant to the Paperwork Reduction Act, 44 U.S.C. § 3501 et seq. Appendix I to Circular A-130 establishes requirements for information security and privacy programs at agencies. Appendix II to Circular A-130 sets forth agency responsibilities for managing PII. Circular A-130 also reiterates that agencies are required to implement security controls that satisfy NIST SP 800-53.

Three areas of cybersecurity are particularly relevant to this litigation: vetting and background investigations, training, and access control policies. The following describes Government standards and OPM practices in each of these areas.

⁹ Available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

¹⁰ Available at <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>.

1. Vetting and Background Investigations

Circular A-130 requires agencies to “[i]mplement access control policies for information resources that ensure . . . that the appropriate level of identity proofing or background investigation is conducted prior to granting access.” The Hilliard declaration describes OPM’s background investigation and security clearance vetting practices, which Hilliard has overseen since March 2020.

A background investigation is not required for new hires who are appointed for less than 180 days, although the agency “must conduct such checks as it deems appropriate to ensure the suitability or fitness of the person.” 5 C.F.R. § 731.104(a)(3). New hires submit a resume and fingerprints for a criminal history check.

2. Training

Circular A-130 requires agencies to “[d]evelop, maintain, and implement mandatory agency-wide information security and privacy awareness and training programs for all employees and contractors” and “ensure that measures are in place to test the knowledge level of information system users.” Agencies must also provide role-based training “before authorizing access to Federal information or information systems.”

Likewise, OPM's own regulations require it to "develop a plan for Federal information systems security awareness and training." 5 CFR § 930.301. It must also provide information on cybersecurity of federal information systems based on NIST guidance "to all new employees before allowing them access to the systems." Id. § 930.301(b) (emphasis supplied).

Relatedly, Circular A-130 requires that agencies "[e]stablish rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems." Agencies must then "[e]nsure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access." (Emphasis supplied.)

The Garcia-Whiteside declaration explains that all new OPM employees are required to complete its Cybersecurity and Privacy Awareness Training when they are appointed. According to PIAs conducted by OPM, OPM employees must also complete this training on an annual basis thereafter, and are specifically required to complete it prior to gaining access to at least two of OPM's

data systems, eOPF or EHRI.¹¹ This training is generally made available through OPM's Cybersecurity Learning Management System and accompanied by a quiz.

OPM's Cybersecurity and Privacy Awareness Training explains that employees are its "first line of defense" and states that "[o]ur technology and information are only as secure as the weakest link." Among many other topics, it discusses how OPM employees should handle PII. It instructs as follows: "Limit your access to only the PII that you have a need to know and do not disclose or provide access to others unless they also have a need to know for a legitimate business purpose." It includes an overview of the Privacy Act.

The Cybersecurity and Privacy Awareness Training also catalogues types of threats, including social engineering, malicious code, hacking, and denial-of-service attacks. It explains that OPM insiders, including current or former

¹¹ Under the E-Government Act of 2002, an agency must prepare a "privacy impact assessment" before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." E-Government Act of 2002, Pub. L. No. 107-347, § 208(b)(1), 116 Stat. 2899. PIAs are generally "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information." Id. § 208(b)(III)(2)(B)(i). The requirement that agencies conduct PIAs is intended "to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." Id. § 208(a).

employees, can be a threat to cybersecurity. Insider threats can arise due to "malicious insiders," who intentionally abuse their credentials to steal information, or "accidental insiders," who do not have malicious intent but nonetheless "cause[] harm or substantially increase[] the probability of future serious harm to an organization's information or information systems." The training states that threats from "accidental insiders" usually occur because of "an action or activity contrary to organization security guidance or security best practices."

The Cybersecurity and Privacy Awareness Training includes Rules of Behavior, which the training states OPM employees must acknowledge if they are granted access to an OPM information system. OPM also states in multiple PIAs that it ensures appropriate data use by having its employees agree to these Rules of Behavior.

Among other things, the Rules of Behavior describe precautionary measures for protecting PII and admonish employees that they "must not share their access rights with others." The Rules instruct employees that they may not introduce any "unauthorized software or data," "modify any configurations," or "connect to other computer systems or networks without the authorization of OPM's Chief Information Security Officer." The

Rules also require employees to “protect all sensitive information residing in OPM computer systems by preventing unauthorized access, use, modification, disclosure, or destruction of that information.” At the end of the Cybersecurity and Privacy Awareness Training, employees acknowledge that they must comply with the Rules and that the possible consequences for noncompliance may include, among other things, dismissal and civil or criminal penalties.

3. Access Control Policies

Federal agencies are required to follow access control policies intended to safeguard the confidentiality of their computerized records. One of these is the principle of least privilege, which is codified as NIST 800-53 AC-6. This principle holds that any person using a system should have the minimum level of access that is necessary for them to complete the tasks for which they are responsible. Circular A-130 requires agencies to “[i]mplement policies of least privilege at multiple layers -- network, system, application, and data so that users have role-based access to only the information and resources that are necessary for a legitimate purpose.” The principle of least privilege is also recognized as a fundamental tenet of cybersecurity by IT professionals in the private sector. In PIAs conducted for OPM systems, OPM has reported

that it uses role-based restrictions on user access that are consistent with the principle of least privilege.

The principle of separation of duties, codified as NIST 800-53 AC-5, is closely related to the principle of least privilege. The principle of separation of duties requires "two-person control" so as to ensure that a single person does not have the ability to make critical changes to a system. Circular A-130 requires agencies to "[i]mplement a policy of separation of duties to address the potential for abuse of authorized privileges and help to reduce the risk of malicious activity without collusion."

In managing access to systems containing sensitive information, organizations normally distinguish between administrators and other users. Administrators are tasked with ensuring the deployment and normal functioning of an existing system. They often require elevated privileges in a system and are normally subject to a high standard of vetting. In contrast, developers are tasked with enhancing a system or building new systems altogether, and do not normally need the same level of access to an existing system. For example, developers may be able to understand a system's data model using anonymized data in a test environment, as opposed to the live "production" environment, or through partial access to the data.

Developers normally rely on administrators to deploy any necessary code changes.

The term "administrative access" lacks an exact definition, but in industry parlance it is understood to be a very powerful level of access to a system. Administrative access often refers to the most powerful level of access to a system, although in some systems there are different "levels" of administrative access. Privileged actions that may be possible with administrative access include, for example, the ability to access, edit, and delete any data within a system, to deploy code changes to a system, and to grant or revoke access to any other user -- including the ability to grant administrative access to a different user. A user with administrative access may also be able to delete system backups, which can cause any data loss to be permanent. Users with administrative access may also be able to delete audit logs, thereby allowing an administrative user to conceal their actions.

OPM's use of the term "administrative access" is broadly aligned with the term's use in industry parlance. Hogan explains that granting a user "administrative access" means "allowing them to perform certain functions that a regular user would not be able to perform," although "the types of functions authorized vary depending on the particular role at issue."

OPM's Cybersecurity and Privacy Awareness Training describes administrators as users with "advanced system permissions."

Hogan states that a user with administrative access does not "necessarily" have the ability to take the following actions: "(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." He does not explain, however, which users at OPM with administrative access do or do not have those abilities. He adds that he is "not aware" of anyone at OPM taking these actions, but does not indicate that there has been an effort to determine whether such actions have been taken.

Hogan testified that once administrative access is requested, the amount of time it takes for it to be granted "could vary greatly based on the system and if someone facilitated rapidly executing that request." If fully expedited, it "could be on the order of minutes."

D. Systems of Records at OPM

OPM describes itself as the "chief human resources agency and personnel policy manager for the Federal Government."¹² In that role, it maintains systems of records containing the

¹² OPM, About Us, <https://www.opm.gov/about-us>.

personal information of tens of millions of Americans, including past, current, and aspiring federal employees and their family members.

These systems contain PII such as social security numbers, banking information, and health care information, including information about family members' health care. The information in OPM systems can be used to find federal employees who work in roles that make them vulnerable to threats of retaliation, such as Administrative Law Judges. OPM systems also contain security clearance data that could reveal intelligence connections of federal employees in sensitive undercover roles.

Individuals do not have the ability to opt out of having their private information in OPM systems. Some OPM systems retain information permanently. This means, for example, that information about federal employees will continue to be stored indefinitely in some OPM systems even after they stop working for the federal Government.

The parties agree that on January 20, 2025 and shortly thereafter, OPM gave individuals working on the DOGE agenda access to at least fourteen OPM systems. There is no dispute that most of those systems contain PII. Those systems include the following:

- The Electronic Official Personnel Folder ("eOPF") stores personnel files for federal employees. According to a

PIA of April 9, 2025, eOPF contains social security numbers, bank account information, dates of birth, addresses, and PII regarding family members.

- The Enterprise Human Resources Integration Data Warehouse ("EHRI") collects human resources, payroll, and training data from several dozen sources outside of OPM, including other federal agencies. According to a PIA of July 11, 2019, EHRI contains social security numbers, job descriptions of Government workers, employment histories, contact information, and payroll information.
- USA Performance is a job performance review site. According to a PIA of May 13, 2020, it contains social security numbers, various other PII, and information related to employee performance reviews, such as individual development plans and work plans.
- USA Staffing is a platform for federal agencies to recruit and onboard employees. According to a PIA of July 28, 2021, it contains social security numbers, demographic information, and any information agencies using the platform choose to collect, which may include banking information.
- USAJOBS is the federal Government's official hiring site. It stores personal information that is provided by applicants to federal Government jobs, regardless of whether they go on to work in those jobs.
- Federal Employee Health Benefits ("FEHB") is a system administered by OPM that is used to manage the healthcare of federal Government employees.
- Postal Service Health Benefits ("PSHB") is a program within FEHB that provides health benefits plans to eligible Postal Service employees, Postal Service annuitants, and their eligible family members.
- OPM Data is a system used for analytics that is built on the Azure Databricks platform. It combines data from other OPM systems and contains PII.

E. Efforts to Modernize Government Technology

There have been many initiatives to modernize the Government's use of technology. For example, the E-Government Act of 2002 was intended, among other things, to "promote interagency collaboration in providing electronic Government services" and "transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations." E-Government Act of 2002, Pub. L. No. 107-347, § 2(b)(3), (10), 116 Stat. 2901. As another example, Congress enacted amendments to FISMA in 2014 to bolster the Government's cybersecurity practices. 44 U.S.C. § 3551.

The U.S. Digital Service was established in 2014 to assist in modernizing technology in the Government. It was described as a "small team of America's best digital experts" who would "work in collaboration with other government agencies to make websites more consumer friendly, to identify and fix problems, and to help upgrade the government's technology infrastructure."¹³ Among other priorities, the U.S. Digital Service was to focus on:

¹³ President Barack Obama's White House Archive, 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>.

Establishing standards to bring the government's digital services in line with the best private sector services;

Identifying common technology patterns that will help us scale services effectively;

Collaborating with agencies to identify and address gaps in their capacity to design, develop, deploy and operate excellent citizen-facing services; and

Providing accountability to ensure agencies see results.

The U.S. Digital Service created "a playbook of 13 key 'plays' drawn from successful practices from the private sector and government that, if followed together, will help government build effective digital services."¹⁴ These include using "an incremental, fast-paced style of software development to reduce the risk of failure," "bringing in seasoned product managers, engineers, and designers," and "us[ing] data to drive decisions."

By 2024, the U.S. Digital Service had collaborated with 31 federal agencies.¹⁵ It "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." It worked on projects that "touched a

¹⁴ U.S. Digital Service, Digital Service Playbook, available at <https://playbook.usds.gov/>.

¹⁵ U.S. Digital Service, Impact Report at 2 (2024), available at <https://www.usds.gov/resources/USDS-2024-Impact-Report.pdf>.

majority of the United States population,” such as delivering COVID-19 tests to the public.

According to a PIA of October 28, 2020, the U.S. Digital Service collaborated with OPM on an “SME Assessment Review Prototype” project. This consisted of enhancements to USA Staffing that enabled subject matter experts to be involved in assessing the qualifications of job applicants. As part of this project, members of the U.S. Digital Service had access to data in USA Staffing. Nesting testified at the hearing that access was given only to a “small team.” He also testified that OPM was “very careful to limit what personal data went into this system,” such that the data was limited to names and possibly email addresses.

OPM has acknowledged the need to improve its IT infrastructure. A report issued in 2023 set forth a detailed modernization plan, stating 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.”¹⁶ A 2024 report by the Government Accountability Office (“GAO”) identified sixteen “priority recommendations” for improving

¹⁶ OPM, Information Technology Strategic Plan, Fiscal Years 2023-2026 at 7 (June 2023), available at <https://www.opm.gov/about-us/reports-publications/2023-2026-information-technology-strategic-plan.pdf>.

OPM's operations, including "[s]trengthening IT security and management."¹⁷

II. Recent Events

A. The DOGE Executive Order

On January 20, 2025, the day of his inauguration, President Donald J. Trump signed Executive Order 14,158 (the "DOGE Executive Order"). The DOGE Executive Order established the "Department of Government Efficiency" to implement the President's "DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity." It renamed the U.S. Digital Service as the United States DOGE Service and moved it from OMB to the Executive Office of the President. It also established within USDS the U.S. DOGE Service Temporary Organization, which it stated shall "terminate" on July 4, 2026.

The DOGE Executive Order instructed each executive agency to establish a "DOGE Team" in consultation with USDS. Each DOGE Team is to consist of at least four employees, who may include Special Government Employees hired or assigned within thirty days of the DOGE Executive Order. Each DOGE Team should

¹⁷ GAO, Priority Open Recommendations: Office of Personnel Management at 2, (May 28, 2024), available at <https://www.gao.gov/assets/gao-24-107323.pdf>.

"typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney."

The DOGE Executive Order also instructed the USDS Administrator to commence "a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." Among other things, this initiative was to "promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization."

The DOGE Executive Order 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."

According to a February 25 letter from USDS employees to President Trump's Chief of Staff, on January 21 the White House conducted interviews of employees who had worked for the U.S. Digital Service before January 20. These interviews included

questions about political loyalties. The letter also states that on February 14, the employment of approximately one third of these individuals was terminated, including the employment of technologists who had been working to modernize various aspects of the federal Government.

B. The Government-Wide Email System

Immediately after President Trump's inauguration, OPM created GWES as a new OPM system. It was created to send mass emails to Government employees. GWES was built using Government email addresses and names that were stored in eOPF and EHRI. Hogan explains that this information was extracted by OPM career staff.

The plaintiffs have submitted exhibits that provide context as to how GWES was used, including a May 22, 2025 article in Wired. On January 24, millions of federal employees began to receive emails from the email address hr@opm.gov. They received several test emails before receiving an email titled "Fork in the Road," which included a resignation offer. Federal workers subsequently received emails from GWES requiring them to list accomplishments over the past week.

On February 4, members of the House Committee on Oversight and Government Reform wrote to Ezell to express their concern that a PIA had not been conducted for GWES. OPM completed a PIA

for GWES on February 28. OPM-2¹⁸ was listed as the "Contact Point" for the PIA, while Hogan was listed as the "Reviewing Official."

C. Disclosure to Twenty Individuals

The following individuals have been appointed to leadership positions at OPM since President Trump's inauguration:

- Charles Ezell was designated Acting Director on January 20. Ezell previously served as a career OPM employee.
- Gregory Hogan is OPM's CIO. He previously served as Vice President of Infrastructure at comma.ai. He was designated as the Acting CIO on January 20, and assumed the CIO position on a permanent basis on February 11.
- Amanda Scales was appointed as Chief of Staff to the OPM Director on January 20. She no longer occupies that role, and it does not appear that she works at OPM any longer. According to a February 3, 2025 Musk Watch article, Scales had been a human resources staffer at xAI, an artificial intelligence firm led by Elon Musk.

Ezell, Hogan, and Scales have requested and facilitated access to OPM data systems for other individuals working on the DOGE agenda. They have also obtained access to OPM data systems themselves.

The administrative record contains two audits of the access to OPM systems given on January 20 and shortly thereafter, which were initially prepared for the Maryland OPM Action. At the

¹⁸ The DOGE-related individuals discussed in this Opinion who are not in public-facing roles are referred to by anonymized monikers, such as OPM-2.

hearing, the defendants principally relied on an audit prepared by a team working for OPM's CISO. That team undertook a review of OPM account access of those individuals who were identified by Hogan as "DOGE affiliates," which had been defined in the Maryland OPM Action to mean personnel "who are working on the DOGE agenda and have been granted access to records containing PII." Maryland OPM Action, ECF No. 38 at 5 n.2; ECF No. 64. This audit consists of a single page, OPM-103 ("March Audit"), and identifies twenty DOGE-affiliated individuals who were granted access to OPM systems, including Ezell, Hogan, and Scales, during the period January 20 to March 6, 2025.¹⁹ It also identifies whether the access granted to each system was administrative access, and whether the individuals logged in to the systems at issue. Each of the individuals listed in the March Audit was granted administrative access to at least one system.

The administrative record also contains an earlier audit. Pages OPM-89 through OPM-102 contain what the Government has labeled as an "account creation audit" for the period between January 20 and February 12 ("February Audit"). The February

¹⁹ Unless otherwise noted, this Opinion uses the term "DOGE agents" to refer to the seventeen individuals listed in the March Audit other than Ezell, Hogan, and Scales. They are OPM-2 through OPM-7, James Sullivan (formerly known as OPM-8), and OPM-9 through OPM-18.

Audit was requested by Hogan on February 16 and consists of two spreadsheets.²⁰ There are unexplained discrepancies between the February Audit and the March Audit. For instance, the February Audit indicates that Ezell, Hogan, and OPM-2 through OPM-5 were granted access to USA Staffing, but that access is not reflected in the March Audit.²¹ Hogan's May 16 declaration relied on the March Audit to state that most DOGE agents did not log in to OPM systems. (While the March Audit indicates whether individuals logged in to systems to which they had been given access, the February Audit does not.)

The Government's submissions in opposition to this motion contain almost no information regarding ten of these individuals, OPM-9 through OPM-18. The Government explains that it has not included onboarding, vetting, and credentialing documents and information for OPM-9 through OPM-18 because the

²⁰ Pages OPM-89 through OPM-91 identify individuals for whom accounts were created, the systems for which accounts were created, dates when accounts were created, and dates when accounts were removed. Pages OPM-92 through OPM-102 appear to be a log of individuals being added to and removed from groups or roles with preset permissions.

²¹ At the hearing, Hogan did not offer any explanation for such discrepancies other than to suggest that the requests could have been "asked in different ways that resulted in different output."

March Audit does not reflect that as of March 6 those ten individuals had logged in to OPM systems.²²

Thus, the DOGE agents will be considered in two groups: a group of seven consisting of OPM-2 through OPM-7 and Sullivan, and a group of ten consisting of OPM-9 through OPM-18. Information regarding the group of seven and then the group of ten is provided next.

1. The Group of Seven

Seven individuals, OPM-2 through OPM-7 and Sullivan, were given access to OPM systems between January 20 and February 3. Individuals in this group were appointed to OPM, as reflected in their Appointment Affidavits (Standard Form 61). Most of these individuals have a background in the technology industry, although some have minimal employment experience. All entered with temporary appointments, and several have since been converted to permanent Government employees. As detailed below, at least OPM-3 through OPM-6 have performed work for other

²² The Government's brief adds that these individuals do not have a "principal role" to further the "DOGE agenda" of "modernizing federal technology" and "were not granted access permissions for that purpose." It appears, therefore, that they are working on DOGE-related agenda items not related to IT modernization.

agencies, and OPM-2, OPM-3, OPM-4, and OPM-7 do not receive paychecks from OPM.²³

The following is relevant background regarding OPM-2 through OPM-7 and Sullivan:

- OPM-2 was appointed on January 20 as an expert in the Office of the Director, for a temporary appointment not to exceed 180 days. On March 18, clearance was requested to convert him to permanent appointment. Because another agency had initiated a background investigation, OPM-2's conversion to a permanent appointment must await adjudication of that investigation. OPM-2 does not receive a paycheck from OPM. According to the February 3 Musk Watch article, he previously worked at the Boring Company, which is owned by Musk.²⁴
- OPM-3 was appointed on January 20 as an expert in the Office of the Director, with a temporary appointment not to exceed 180 days. He has also been appointed to SSA, which pays his salary, and DOE. He does not receive a paycheck from OPM. This arrangement is detailed in an inter-agency memorandum of understanding executed on February 12 and 13 by OPM, SSA, and DOE.²⁵ OPM-3 is 21 years old. According to the February 3 Musk Watch article, he previously interned at Meta and Palantir.
- OPM-4 was appointed on January 24 as an expert in the Office of the Director, with a temporary appointment not to exceed 180 days. He has also been appointed to GSA and has been detailed to USDS and HHS. He obtained

²³ As discussed below, there is a multi-factor test to determine which federal agency is the employer of an individual working for the Government. Appointment to an agency and receipt of a paycheck from an agency are facts to consider in that analysis.

²⁴ The Government did not object at the hearing to the use of news reports to identify where DOGE agents were previously employed.

²⁵ Although several of the individuals listed here have done work for other agencies, this is the only inter-agency memorandum of understanding contained in the administrative record.

access to sensitive systems at HHS in March 2025, and that access has since been disabled. He does not receive a paycheck from OPM. OPM-4 is 19 years old. Press reports indicate that he is known online as "Big Balls." The February 3 Musk Watch article states that he interned at Neuralink. According to a February 7, 2025 New York Times article, he was fired from a cybersecurity firm after, according to that firm, "an internal investigation into the leaking of proprietary information that coincided with his tenure." The administrative record does not indicate that the February 7 article prompted a background check or additional vetting of OPM-4.²⁶

- OPM-5 was appointed on January 20 as a Senior Advisor to the Director for Information Technology, with a temporary transitional appointment. On January 29, it was requested that his position be converted to a permanent appointment. He became a permanent employee on February 18, the requirement of completing a pre-appointment background investigation having been waived. A background investigation was completed on March 18 and favorably adjudicated on March 21. He has also been detailed to GSA, the Internal Revenue Service, the U.S. Agency for International Development ("USAID"), the Department of Agriculture ("USDA"), and the U.S. Agency for Global Media. He is also a member of the DOGE team at Treasury. He has been identified by courts as having been involved in workforce reductions at USAID and CFPB. Does 1-26 v. Musk, No. 25cv462, 2025 WL 840574, at *7 (D. Md. Mar. 18, 2025) (USAID); Nat'l Treasury Emps. Union v. Vought, No. 25cv0381, 2025 WL 1144646, at *3 (D.D.C. Apr. 18, 2025) (CFPB). Emails contained in an administrative record produced by USDA in separate litigation indicate that he has also been involved in workforce reductions at that agency. OPM-5 was 25 years old when appointed to OPM. According to the February 3 Musk Watch article, he previously worked at Twitter.
- OPM-6 was appointed on January 24 as an expert in the Office of the Director, with a temporary appointment not to exceed 180 days. He has been detailed from OPM to

²⁶ This Opinion has not received the substance of the report regarding the termination of OPM-4's prior employment for its truth, but rather for the fact of the reporting and its impact, if any, on the defendants.

USDS, DOC, and CFPB, and was also appointed to SSA. In separate litigation, the Government has admitted that he was granted permission to access "sensitive systems" at CFPB in February 2025.

- OPM-7 was appointed on January 20 as an expert in the Office of the Director, with a temporary appointment not to exceed 180 days. Pursuant to a request made on January 29, he became a permanent employee on January 31. A previous background investigation was reviewed in lieu of completing a new background investigation. He does not receive a paycheck from OPM. According to the February 3 Musk Watch article, he spent 21 years at SpaceX, and led its human resources department for the last 10 years.
- James Sullivan, formerly referred to as OPM-8, was appointed as Senior Advisor to the Director on January 20, and was vetted for a temporary appointment not to exceed 180 days. Pursuant to a request made on January 30, he became a permanent employee on February 12, the requirement of a pre-appointment background investigation having been waived. A background investigation was completed on March 3 and favorably adjudicated on March 4. On March 28, Sullivan became Chief of Staff to the Director, a public-facing role.

The Hilliard declaration details the vetting and background checks that were conducted for the above individuals. For each of them, an interim eligibility determination was made between January 14 and January 24, at the time of their initial appointments. Because they were vetted for interim positions, they were subject at that time to a criminal history fingerprint check but no background check. OPM-5, OPM-7, and Sullivan have been converted to permanent positions. OPM waived pre-appointment background investigations for OPM-5 and

Sullivan, and relied on a previous background investigation for OPM-7.

The Garcia-Whiteside declaration details the training process for these individuals. While incoming OPM employees are ordinarily required to complete its Cybersecurity and Privacy Awareness Training through OPM's Cybersecurity Learning Management System, that system was unavailable in January 2025 because it was being updated. Thus, OPM provided this training in the form of a document and waived the required quiz. OPM then accepted emails from incoming employees acknowledging that they understood the training document's contents. Hogan, OPM-2, OPM-5, and OPM-7 sent such emails acknowledging that they completed the training by January 20, before they obtained access to OPM systems. OPM-3, OPM-4, and OPM-6 did not send such emails, and only acknowledged their completion of the training on February 19, weeks after each of them had been given access to OPM systems. February 19 is the date of Hogan's first declaration in this action. In it, he states in reference to OPM-2 through OPM-6 that they "have completed" this training. (Emphasis supplied.) There is no indication in the

administrative record that Sullivan has acknowledged completion of the training.²⁷

2. The Group of Ten

Ten individuals, OPM-9 through OPM-18, were also given administrative access to OPM systems between January 24 and February 7. With a single exception, however, they were only given administrative access to USA Performance, a job performance review site containing PII.²⁸ The exception is OPM-9, who was given administrative access to USA Performance, FEHB, PSHB, and OPM Data. As noted, the defendants have not provided any evidence as to whether these individuals were appointed to OPM, vetted, or trained.

The record contains background information about two of these ten individuals.

- OPM-14 is detailed from OPM to USDS and CFPB. According to a declaration by Elisabeth Feleke, the Chief Program Officer at the United States African Development Foundation ("USADF"), he has been involved in the termination of the employment of individuals at USADF, work that was initially portrayed to USADF employees as an IT modernization initiative. He has also been identified in other litigation as having been involved in workforce reductions at CFPB. Nat'l Treasury Emps. Union v. Vought, No. 25cv0381, 2025 WL 942772, at *5 (D.D.C. Mar. 28, 2025).

²⁷ At the hearing, the Government represented that Sullivan has since completed the training.

²⁸ Hogan has explained that access to USA Performance is automatically revoked after 60 days of inactivity.

- OPM-16 is a lawyer associated with DOGE. Similar to OPM-14, he is identified in the Feleke declaration as having been involved in the termination of the employment of individuals at USADF.

3. Use of Access to OPM Systems

The administrative record reflects that, beginning on January 20, OPM gave administrative access to its data systems to seventeen individuals working on the DOGE agenda, as well as to Ezell, Hogan, and Scales. The administrative record suggests that few of these individuals had used that access as of March 6.

As noted, the March Audit was compiled by OPM's CISO team and represents a review of login access to OPM's systems by individuals at OPM working on the DOGE agenda. That review reflects that the following individuals who had been given administrative access to OPM systems had logged in to those systems between January 20 and March 6:

- Hogan logged in to USA Performance.
- OPM-6 logged in to OPM Data.
- Scales, Sullivan, and OPM-6 logged in to USA Staffing. Hogan stated in his May 16 declaration that this access was needed for "several reasons," including to "make system changes in connection with automated hiring/onboarding and job posting processes" and "develop and implement a data-driven Federal Hiring Plan." At the hearing, the defendants provided evidence that the changes made to USA Staffing included the creation of popup screens that remind users of the hiring freeze.

The March Audit may not be an entirely reliable record of access, however. For instance, the February audit indicates that Ezell, Hogan, and OPM-2 through OPM-5 were granted access to USA Staffing, but that access is not reflected in the March Audit.²⁹

In addition, employees working on the DOGE agenda had access to data in OPM systems through career OPM staff. As noted above, Government email addresses and employee names appearing in eOPF and EHRI were used to create GWES. That data was extracted by OPM career staff and made available to DOGE agents, which is why the March Audit does not reflect that DOGE agents logged in to either eOPF or EHRI. At the hearing, Hogan testified that OPM career staff may have extracted data for DOGE agents on other occasions, specifically for a retirement services modernization project.

4. Chronology of Disclosure

A chronology of the disclosure of OPM systems to individuals working on the DOGE agenda begins on the evening of January 20, the day of President Trump's inauguration, with a "911-esque call" requesting that a "political team" composed of

²⁹ Another error in the March Audit is that it incorrectly indicated that OPM-7 logged in to USA Staffing. Hogan's May 16 declaration stated this as well. Hogan corrected the record at the hearing, stating that OPM-7 had not logged in to USA Staffing.

six individuals be given access to OPM systems. OPM's IT staff did not receive the usual documentation for this request until more than a week later. Internal emails indicate that, pursuant to this emergency request, OPM granted Ezell, Hogan, Scales, OPM-3, OPM-5, and OPM-7 administrative access to USAJOBS, USA Staffing, and USA Performance. This access was described as "administrator accounts with super user permissions" and "comprehensive access."

On January 27, Ezell stated that OPM-2, OPM-4, and OPM-6 "urgently" needed access. Ezell explained that "[r]ight now we don't have immediate plans to change anything but if we need to we might need to move quickly." He added that "[t]hey won't have a lot of time to go through a lot of presentations on what the systems are and what the program officers feel about the programs, etc." He suggested, instead, that if there was "an architecture level engineering perspective that could be shared that might be helpful if it could be done at some point." Internal emails indicate that on January 28, OPM granted OPM-2, OPM-4, and OPM-6 administrative access to USAJOBS, USA Staffing, USA Performance, eOPF, and EHRI. Their access included "[c]ode read and write permissions."

James Sullivan was given administrative access to USA Performance on January 31. On February 3, Amanda Scales

requested that Sullivan also be given administrative access to USA Staffing, and that access was granted the same day.

In addition, between January 28 and February 4, access to FEHB and PSHB was given to Hogan, Scales, Sullivan, OPM-2, OPM-4, OPM-5, OPM-6, and OPM-9. OPM-9 through OPM-18 were given administrative access to USA Performance between January 24 and February 7.

An article about DOGE-affiliated individuals accessing OPM records was published in the Washington Post on February 6. That same day, Hogan began an effort to roll back access to OPM systems for the "DOGE Engineers," a descriptor that Ezell and Hogan have used for OPM-2 through OPM-6. Hogan explained "we have never needed access to ERHI/eOPF so if any access was granted there it can be removed immediately." On February 6, OPM removed access to eOPF and EHRI from OPM-2 through OPM-6. It confirmed that none of them had logged in to these systems, although accounts had been created for OPM-2, OPM-4, and OPM-6. In Hogan's February 19 declaration, without disclosing that access had been given and then revoked, he stated, in reference to OPM-2 through OPM-6, that "[n]one of these individuals has access to EHRI." (Emphasis supplied.)

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

The Maryland OPM Action and Virginia OPM Action were filed on February 10, and this action was filed on February 11. On February 12, at Hogan's request, OPM began a review of all internal OPM user accounts created between January 20 and February 12. At the hearing, Hogan testified that the goal of this audit was to collect access requests and approvals in preparation for future audits. On February 16 Hogan requested the February Audit, which contains the same type of information that he requested on February 12.

Conclusions of Law

This section begins with the threshold issue of Article III standing, finding that the plaintiffs have carried their burden to establish standing. Next, this section turns to the elements of a preliminary injunction, analyzing the plaintiffs' likelihood of success on the merits, irreparable harm, and the public interest. As explained below, the plaintiffs have shown that they are entitled to a preliminary injunction.³⁰

³⁰ Much of the law set forth in this Opinion appears as well in the decision largely denying the defendants' motion to dismiss. April 3 Opinion, 2025 WL 996542.

I. Article III Standing

A plaintiff's burden to establish Article III standing for the purpose of obtaining preliminary relief "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) (citation omitted). This burden "is more onerous than the burden at the pleading stage." Id. To establish standing for a preliminary injunction, a plaintiff must set forth by affidavit or other evidence specific facts, which "will be taken to be true." Id. (citation omitted).

Article III of the U.S. Constitution requires a plaintiff to have "a personal stake in the case -- in other words, standing." TransUnion LLC v. Ramirez, 594 U.S. 413, 423 (2021) (citation omitted). A plaintiff must show "(1) an injury in fact, defined as an invasion of a legally protected interest that is concrete, particularized, and actual or imminent; (2) a sufficient causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury will be redressed by a favorable decision." Citizens United to Protect Our Neighborhoods v. Village of Chestnut Ridge, 98 F.4th 386, 391 (2d Cir. 2024) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)).

A union may assert standing to bring claims either in its own right or as a representative of its members. See id. at 395-96. Here the plaintiff unions assert their members' injuries. Consequently, under the doctrine of associational standing, the plaintiff unions must demonstrate that their members would have standing to sue in their own right. Id.³¹

A. Injury in Fact

An injury in fact must be concrete, such that it is "real and not abstract." FDA v. All. for Hippocratic Med., 602 U.S. 367, 381 (2024). It must also be particularized, meaning that it must affect the plaintiff "in a personal and individual way and not be a generalized grievance." Id. (citation omitted). Moreover, the injury "must be actual or imminent, not speculative -- meaning that the injury must have already occurred or be likely to occur soon." Id. "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury

³¹ The other elements of associational standing are satisfied. That is, the members' interests that the union plaintiffs seek to represent are "germane to the organization's purpose" and "neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." Citizens United to Protect Our Neighborhoods, 98 F.4th at 391. As reflected in the Ramrup and Kelley declarations submitted on February 14, the purpose of the plaintiff unions is to represent the interests of their members, who are current or former federal employees.

is not too speculative for Article III purposes -- that the injury is certainly impending." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (citation omitted).

An injury in fact may be tangible or intangible. TransUnion, 594 U.S. at 425. For instance, it may be physical, monetary, an injury to property, or an injury to rights. FDA, 602 U.S. at 381. To assess whether a harm is a concrete injury in fact for purposes of Article III standing, "courts should assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." TransUnion, 594 U.S. at 424 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)). While the asserted injury must have "a close historical or common-law analogue," the analogue need not be an "exact duplicate in American history and tradition," id., and a plaintiff need not "plead every element of a common-law analog to satisfy the concreteness requirement." Salazar v. Nat'l Basketball Ass'n, 118 F.4th 533, 542 n.6 (2d Cir. 2024).

Concrete, intangible harms "include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." TransUnion, 594 U.S. at 425. Traditional, concrete intangible injuries also include "harms specified by the Constitution." Id. In addition, when

identifying concrete, intangible harms, “Congress’s views may be instructive.” Id. (citation omitted). “Courts must afford due respect to Congress’s decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant’s violation of that statutory prohibition or obligation.” Id. Even where a statute grants a person a statutory right to sue, however, courts must independently assess whether the plaintiff has shown a concrete injury because of a defendant’s violation of law. Id. at 426.

The Supreme Court has explained that harms analogous to those underlying the tort of intrusion upon seclusion may be concrete for purposes of Article III standing. Id. at 425; see also Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (“The common law has long recognized actions at law against defendants who invaded the private solitude of another by committing the tort of intrusion upon seclusion.” (citation omitted)).

Intrusion upon seclusion is defined as follows:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 625B (Am. L. Inst. 1977); see Melito v. Experian Marketing Sols., Inc., 923 F.3d 85, 93 (2d

Cir. 2019) (citing § 652B in support of Article III standing analysis). The comments to this section of the Restatement explain that liability depends not “upon any publicity given to the person whose interest is invaded or to his affairs,” but rather on “[t]he intrusion itself.” Id. § 652B cmt. a, b. The tort covers intrusion upon private records but not “the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection.” Id. § 652B cmt. c. The interference with the plaintiff’s seclusion must be “substantial.” Id. § 652B cmt. d.

Citing these comments to the Restatement, the Second Circuit has emphasized that intrusion upon seclusion

is a tort that occurs through the act of interception itself. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the information outlined. Nothing more is required after the interception is made for liability to attach based on this tort.

Caro v. Weintraub, 618 F.3d 94, 101 (2d Cir. 2010) (citation omitted). In Caro, the Second Circuit held that liability could arise from a defendant setting up a recording device, pressing “record,” and doing nothing more -- that is, the “simple act of the recording itself” -- without listening, publishing, sharing,

copying, or any other act that might harm the plaintiff, sufficed to establish intrusion upon seclusion. Id.

The plaintiffs have demonstrated a concrete injury analogous to intrusion upon seclusion. The records at issue concern the plaintiffs' most sensitive private affairs. They include social security numbers, health care information, banking information, and information about family members. OPM records can be used to reveal intelligence connections regarding federal employees in sensitive undercover roles or to find federal employees who may be subject to threats of retaliation, such as Administrative Law Judges. The plaintiffs have no ability to opt out of having their information in OPM systems, and some OPM systems permanently retain information. The plaintiffs have every reason to expect that such information will be carefully safeguarded, and that is in fact what the Privacy Act requires.

The plaintiffs have also demonstrated that, beginning on January 20, OPM gave access to records containing PII to seventeen DOGE agents, as well as to three individuals in leadership positions at OPM. Collectively, OPM gave these individuals access to at least fourteen OPM systems, and the access it gave them was almost always administrative access. As explained in detail below, the plaintiffs have shown that in

doing so OPM violated the Privacy Act and the APA, including because the DOGE agents did not have a sufficient need for the access they were given. OPM also disregarded its cybersecurity standards and protocols.

The defendants argue that the plaintiffs have failed to establish their standing. The defendants contend that the administrative record, supplemented by the declarations they have submitted, shows that OPM “properly vetted, credentialed, and appointed” each of the DOGE agents; that no intrusion has occurred since few of the DOGE agents actually accessed OPM systems; and that the plaintiffs have not shown any impending risk of harm. These arguments fail.

1. Onboarding Process

The defendants argue that the plaintiffs cannot show that any violations of the Privacy Act and the APA that arose from giving the DOGE agents unrestricted access to the plaintiffs’ records would be “highly offensive to a reasonable person,” as required to establish an intrusion upon seclusion, because OPM adhered to its regular onboarding process and properly vetted, credentialled, and appointed each of the DOGE agents. But that is not what the record shows. While sparse, the administrative record reflects a chaotic, irregular, and risky onboarding process. Given the sensitivity of data within OPM systems and

OPM's legal obligations to keep its systems confidential and secure, the plaintiffs have shown that OPM's legal violations would be highly offensive to a reasonable person.

The defendants have not provided any record at all of vetting, credentialling, or training for ten of the DOGE agents, OPM-9 through OPM-18.³² Four of the other seven DOGE agents -- Sullivan, OPM-3, OPM-4, and OPM-6 -- did not complete OPM's Cybersecurity and Privacy Awareness Training, which is supposed to be mandatory for all newly appointed employees, before they were given access to OPM systems. Sullivan and OPM-6 also logged in to OPM systems before completing that training. These facts alone would give a reasonable person cause for grave concern.³³

The plaintiffs have also shown that based on the current state of the administrative record, OPM did not act to ensure

³² The defendants state that they have not included such information as to OPM-9 through OPM-18 because those individuals did not log in to OPM systems before March 6 and are not working primarily on technology modernization efforts. But, as is explained below, whether DOGE agents logged in to OPM systems does not determine whether the plaintiffs have standing or whether the defendants violated the Privacy Act. It is also not the case that DOGE agents fall outside the scope of this action if they are not principally working on technology modernization.

³³ New OPM employees are also required to complete ethics training within three months of their appointment. As of May 16, OPM had no record that OPM-4 or OPM-7 had completed that training at OPM.

the fitness of OPM-4 for employment at OPM and access to PII. While no background investigation is required for newly hired temporary employees, when OPM is put on notice of risk it is required to do what "it deems appropriate to ensure the suitability or fitness of the person." 5 C.F.R. § 731.104(a)(3). The record is barren of any additional scrutiny OPM gave to OPM-4 after the February 7 New York Times report that he had been fired from a cybersecurity firm after, according to that firm, "an internal investigation into the leaking of proprietary information that coincided with his tenure." Instead, in opposing this motion, the defendants argue that nothing in the resume OPM-4 submitted to OPM or in his fingerprint check "warranted any additional review or investigation."

The gravity of the gaps in the onboarding process is amplified by the sweeping access OPM gave to its data systems. That topic is addressed next.

2. Access to OPM Systems

The defendants next contend that the plaintiffs have not demonstrated an actual injury because they have not shown that data within OPM's systems was actually accessed by more than a few DOGE agents. While the defendants admit that OPM granted access to fourteen OPM systems, they again emphasize that the

March Audit reflects that as of March 6 only four relevant individuals had logged in to OPM systems. They acknowledge that Hogan logged in to USA Performance and that Scales, Sullivan, and OPM-6 logged in to USA Staffing. The defendants overlook that, according to the March Audit, OPM-6 also logged in to OPM Data, which also contains PII. Even assuming that to establish standing based on the violations of the Privacy Act and the APA at issue here the plaintiffs must show that the relevant individuals logged in to OPM systems, the plaintiffs have shown that these four did so, and that neither Sullivan nor OPM-6 had completed their security training before obtaining access.

A further weakness in the defendants' argument is that the March Audit is not entirely reliable. It indicates that OPM-7 logged in to USA Staffing, which the Government reports is an error. The Government has not explained why the February Audit, but not the March Audit, indicates that Ezell, Hogan, and OPM-2 through OPM-5 had access to USA Staffing. The March Audit also provides no information past March 6.

The defendants' argument also rests on a flawed assumption that DOGE agents could not have viewed or used the data stored in a system without personally logging in. That assumption is contradicted by the record. OPM-2 is listed as the "Contact Point" on the February 28 PIA for GWES, but apparently did not

log in to either EHRI or eOPF, the two systems from which Government employee names and email addresses were obtained to create GWES. Instead, those data elements were extracted by career OPM staff. Hogan testified that career OPM staff may also have extracted data and provided it to DOGE agents on other occasions, including for a retirement services modernization project. It is hardly surprising that data requests would be facilitated by career OPM staff who have familiarity with the operation of OPM systems. While the defendants suggest that there can be no violation of the Privacy Act when data is accessed from OPM systems by exploiting a career employee's access permissions, that is clearly wrong.

The defendants next argue that the plaintiffs have failed to show that DOGE agents personally reviewed the plaintiffs' PII. This argument fails. The plaintiffs do not have to make that showing to establish their standing, or even a likelihood of success on the merits. It is the intrusion and not the misuse of the data that constitutes the violation. Granting improper access to legally protected data is sufficient to demonstrate a harm resembling intrusion upon seclusion, and no further use or review of the data is necessary. See April 3 Opinion, 2025 WL 996542, at *7. The "exposure of [a plaintiff's] personally identifiable information to unauthorized

third parties,” without further use or disclosure, is analogous to harm cognizable under the common law right to privacy. Salazar, 118 F.4th at 541. Courts have found standing to exist when an unauthorized third party was granted access to a plaintiff’s legally protected data, due to the resulting harm’s resemblance to intrusion upon seclusion. E.g., Persinger v. Southwest Credit Sys., L.P., 20 F.4th 1184, 1192 (7th Cir. 2021) (an “unauthorized inquiry” into credit information sufficient to confer standing); Nayab v. Cap. One Bank (USA), N.A., 942 F.3d 480, 491-92 (9th Cir. 2019) (same); Perry v. Cable News Network, 854 F.3d 1336, 1340-41 (11th Cir. 2017) (same).

3. Impending Risk of Harm

Finally, the defendants argue that the plaintiffs have failed to establish their standing because they have not demonstrated any “impending” risk of harm. Not so. In addition to having shown concrete harm based on the improper access that has already been granted to OPM records, the plaintiffs have also demonstrated a risk of future harm. There has been no acknowledgement by the Government of past errors, nor any assurance that from this point on access will not be given to OPM systems containing PII to those who are not authorized to have access under the Privacy Act. And where unnecessary and improper access is given, cybersecurity risks are magnified.

The "need to review" requirement of the Privacy Act, which is discussed in detail below, overlaps with FISMA standards and basic cybersecurity hygiene. The record shows that instead of following the principles of least privilege and separation of duties, the OPM Defendants adopted a principle of maximum privilege for DOGE agents, routinely granting them administrative access. There has been no showing of need for such access. Quite the contrary. On January 27 Ezell requested administrative access for OPM-2, OPM-4, and OPM-6 despite noting that "we don't have immediate plans to change anything." Weeks later, Hogan reported that "we have never needed access to ERHI/eOPF." The fact that there is no record that most of the relevant individuals had logged in to OPM systems as of March 6 is strong evidence that they did not need access to OPM systems, much less the administrative access that they were granted.

The Government does not dispute that a retreat from basic cybersecurity safeguards increases the risk of confidentiality breaches, integrity breaches, and availability breaches. Indeed, that is what OPM teaches its own employees in the Cybersecurity and Privacy Awareness Training. Generally speaking, the longer broad and unnecessary access continues, the greater the risk that cybersecurity breaches will occur. As Nesting and Schneier have explained in their declarations,

giving more people unnecessary access increases OPM's "attack surface" with respect to malicious actors who seek to compromise credentials to OPM systems.

OPM's careless approach toward cybersecurity is reminiscent of the failures that contributed to the 2015 data breach. At the hearing, the Government took the view that the 2015 data breach was caused by the absence of multi-factor authentication, which OPM has now deployed. As the 2016 House Report makes clear, however, that was not the only cybersecurity failure that contributed to the 2015 data breach, and deploying multi-factor authentication was only one among many steps necessary to mitigate cybersecurity risks in the future. Other steps mentioned in the 2016 House Report include, for example, adopting a "zero trust IT security model" and making improvements to cybersecurity training.

B. Causation and Redressability

The final elements of an injury in fact, causation and redressability, "are often flip sides of the same coin," and can be quickly addressed. FDA, 602 U.S. at 380 (citation omitted). "If a defendant's action causes an injury, enjoining the action or awarding damages for the action will typically redress that injury." Id. at 381.

The OPM Defendants, who are responsible for the safekeeping of the plaintiffs' records, disclosed them to multiple government employees without requiring those employees to be adequately vetted or trained, and without limiting their access in the ways required by law and OPM's own procedures. This harm is redressable through an injunction, which can prohibit improper disclosure from continuing and, to the extent that any information from OPM records has been improperly copied, order that the information be impounded and destroyed.

II. Preliminary Injunction

Ordinarily, when a preliminary injunction will affect a government defendant, "the moving party must demonstrate (1) irreparable harm absent injunctive relief, (2) a likelihood of success on the merits, and (3) public interest weighing in favor of granting the injunction." Kane v. De Blasio, 19 F.4th 152, 163 (2d Cir. 2021) (citation omitted); see also id. ("When the government is a party to the suit, our inquiries into the public interest and the balance of the equities merge." (citation omitted)).

The defendants claim, however, that the preliminary injunction sought by the plaintiffs is "mandatory" rather than "prohibitory." If that were true, the plaintiffs would be subject to a more demanding standard requiring them to "show a

clear or substantial likelihood of success on the merits and [to] make a strong showing of irreparable harm.” Daileader v. Certain Underwriters at Lloyds London Syndicate 1861, 96 F.4th 351, 356 (2d Cir. 2024) (citation omitted). An injunction is prohibitory if it seeks to stay government action rather than “alter the status quo by commanding some positive act.” Mastrovincenzo v. City of New York, 435 F.3d 78, 89 (2d Cir. 2006) (citation omitted). The Second Circuit has explained that “[t]he ‘status quo’ in preliminary-injunction parlance is really a ‘status quo ante,’” which “shuts out defendants seeking shelter under a current ‘status quo’ precipitated by their wrongdoing.” N. Am. Soccer League, LLC v. U.S. Soccer Fed’n, Inc., 883 F.3d 32, 37 n.5 (2d Cir. 2018) (citation omitted).

The injunction the plaintiffs seek is prohibitory. They seek a return to the status quo as it existed at OPM before the DOGE agents were onboarded and given sweeping access to PII in disregard of the limitations imposed by the Privacy Act. They seek a return to good order and compliance with the dictates of the Privacy Act, as well as OPM’s own cybersecurity protocols. Thus, the more demanding standard for a mandatory injunction does not apply here. But even if that heightened standard applied, the plaintiffs have carried that burden as well.

A. Likelihood of Success on the Merits

The plaintiffs have shown a likelihood of success on the merits of their APA claims. As explained below, they have demonstrated that two violations of the Privacy Act have occurred and that the APA provides for judicial review of the defendants' actions.

1. Violations of the Privacy Act

The plaintiffs have shown violations of two provisions of the Privacy Act. These provisions are 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.

i. Illegal Disclosure

The Privacy Act restricts the disclosure of individuals' private data without their permission, subject to specific exceptions based on appropriate governmental needs. The Privacy Act provides:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains[.]

5 U.S.C. § 552a(b). That provision is followed by enumerated exceptions listed in § 552a(b)(1)-(13). The first exception,

and the one pertinent here, permits disclosure "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." Id. § 552a(b)(1) ("Exception (b)(1)").

The term "need" is not defined in the Privacy Act. In determining whether an official has a "need" for a record within the meaning of Exception (b)(1), courts consider "whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly." Bigelow v. Dep't of Def., 217 F.3d 875, 877 (D.C. Cir. 2000). The Senate Report explains the intent of § 552a(b) and Exception (b)(1):

The section envisions that if an employee dealing with official information about a person is requested to surrender that person's record to someone who clearly has no need for it, he should decline or seek to define the purpose of the requested disclosure. One of the results of this section may be to promote a sense of ethical obligation on the part of Federal officials and employees to ascertain when improper disclosure of information within the agency may be sought or promoted for personal, political or commercial motives unrelated to the agency's administrative mission.

S. Rep. No. 93-1183, at 51-52 (1974); see also Pilon v. U.S. Dep't of Just., 73 F.3d 1111, 1120-22 (D.C. Cir. 1996) (legislative history and purpose of the Privacy Act).

The Privacy Act and agency regulations contain definitions for other critical terms. There is no dispute that OPM is one

of the agencies to which the Privacy Act applies. See 5 U.S.C.

§ 552a(a)(1) (defining agency). A "record" is defined as

any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph[.]

Id. § 552a(a)(4). A "system of records" is defined as

a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual[.]

Id. § 552a(a)(5). The term "maintain" is defined to include

"maintain, collect, use, or disseminate." Id. § 552a(a)(3).

"Individual" is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence." Id. §

552a(a)(2).

OPM's regulations, enacted in 1988, govern the "maintenance, protection, disclosure and amendment of records" within the systems of records protected by the Privacy Act.

5 C.F.R. § 297.101. OPM's regulations define "disclosure" as "providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian." Id. § 297.102. Thus, "providing" access to another person for their

review of a record is a disclosure, even if that access is not used. This is consistent with the definitions other agencies have given to the term "disclosure" for purposes of their own compliance with the Privacy Act. For example, OMB states that "disclosure may be either the transfer of a record or the granting of access to a record," 40 Fed. Reg. 28948, 28953 (July 9, 1975), while the SSA defines "disclosure" as "making a record about an individual available to or releasing it to another party." 20 C.F.R. § 401.25. These definitions are also consistent with a holding by the D.C. Circuit that, under the Privacy Act, "disclose" includes "virtually all instances [of] an agency's unauthorized transmission of a protected record." Pilon, 73 F.3d at 24.

Thus, to demonstrate the violation of § 552a(b) at issue here, a plaintiff must establish that:

- (1) an agency covered by the Privacy Act maintains a system of records;
- (2) the agency disclosed to another person or agency a record contained in that system that pertains to the plaintiff;
- (3) the plaintiff did not submit a written request for the record's disclosure to the agency or give prior written consent to the disclosure; and
- (4) no exception under the Privacy Act applies, including Exception (b)(1).³⁴

³⁴ Because the plaintiffs succeed in proving each of these elements, it is unnecessary to decide whether the exceptions to

The plaintiffs have shown a likelihood of proving a violation of § 552a(b). There is no dispute that OPM maintains numerous systems that contain records pertaining to the plaintiffs, and that the plaintiffs did not consent to the disclosure of those records to the defendants in the ways at issue here. The plaintiffs have shown a likelihood of proving at trial that those 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.

The defendants argue that the plaintiffs have not shown a likelihood of success since OPM records were disclosed to only four relevant individuals -- Hogan, Scales, Sullivan, and OPM-6. They also argue that each of the four was a duly appointed OPM

§ 552a(b) should be treated as affirmative defenses that the defendants bear the burden of proving. Generally, “when a statutory prohibition is broad and an exception is quite narrow, it is more probable that the exception constitutes an affirmative defense.” Cunningham v. Cornell Univ., 86 F.4th 961, 975-76 (2d Cir. 2023) (citation omitted). In the context of claims alleging improper disclosure under the Privacy Act, however, courts appear to place the burden on plaintiffs to demonstrate that none of the exceptions apply. See, e.g., Chichakli v. Tillerson, 882 F.3d 229, 233 (D.C. Cir. 2018) (requiring a plaintiff seeking damages under the Privacy Act to plead the disclosure did not fall under the “routine use” exception, § 552a(b)(3)); Hill v. Dep’t of Def., 981 F. Supp. 2d 1, 5 (D.D.C. 2013) (“[t]he plaintiff bears the burden of proof” to show, among other elements, that “the agency improperly disclosed the information” (emphasis supplied)).

employee, and, relying on the presumption of regularity,³⁵ they argue that each of them had a need to access those records. These contentions are addressed next.

(a) Disclosure

The defendants argue that the plaintiffs have only shown that OPM "disclosed" records to Hogan, Scales, Sullivan, and OPM-6 because those are the only relevant individuals who are shown in the March Audit to have logged in to OPM systems as of March 6. This argument fails. As already explained, "disclosed" has a broader meaning under the Privacy Act than the defendants propose. OPM records were disclosed to all of the DOGE agents when they were given access to records, regardless of whether they actually logged in to OPM systems or reviewed the records.³⁶ In any event, the defendants concede that disclosure was made to these four individuals.

³⁵ The presumption of regularity in government proceedings is well established. "Unless the record includes clear evidence to the contrary, agency action is entitled to a presumption of regularity." Nat'l Lab. Rels. Bd. v. Newark Elec. Corp., 14 F.4th 152, 163 (2d Cir. 2021). The effect of that presumption, however, "is not to shield [agency] action from a thorough, probing, in-depth review." Citizens to Pres. Overton Park, Inc. v. Volpe, 401 U.S. 402, 415 (1971).

³⁶ While disclosure does not require review of records, the administrative record indicates that records were disclosed to and reviewed by DOGE agents who did not personally log in to OPM systems. Individuals working on the DOGE agenda in connection with the creation of GWES were given at least names and Government email addresses that were extracted from OPM systems

(b) Employment Status

The defendants next argue that the plaintiffs have not shown that these four individuals were not OPM employees at the time OPM records were disclosed to them. Their employment status is relevant since the Privacy Act permits disclosure to OPM employees "who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

The determination of whether a person was employed by OPM or elsewhere in the Government is not a straightforward task. In determining which agency employs a person who works for more than one agency, the D.C. Circuit applies a functional approach that includes an evaluation of all the circumstances of the relationship, such as what work they do, where they work, and who supervises them. Jud. Watch, Inc. v. Dep't of Energy, 412 F.3d 125, 131-32 (D.C. Cir. 2005). Federal employees can be "detailed" from one agency to another pursuant to the Economy Act when the "head of an agency . . . place[s] an order with . . . another agency for goods or services." 31 U.S.C. § 1535(a).³⁷ While an individual may be detailed to multiple

by career OPM employees. Hogan also testified that career OPM employees may also have disclosed OPM records to individuals working on the DOGE agenda in other contexts, including in connection with a retirement services modernization project.

³⁷ Title 31, which contains the Economy Act, defines an "agency" as "a department, agency, or instrumentality of the United

agencies, they cannot be deemed an employee of multiple agencies at the same time. See Jud. Watch, Inc., 412 F.3d at 131-32.

While the record suggests that Hogan, Scales, and Sullivan are OPM employees, the plaintiffs are likely to prove that at least OPM-6 was not. These four individuals were all appointed to OPM between January 20 and 24. OPM-6 was appointed to OPM for a 180-day term. He was also detailed to the USDS, DOC, and CFPB, and was also appointed to SSA. He obtained access to sensitive systems at CFPB in February 2025. In light of the significant DOGE-related work that OPM-6 has done with other agencies, it is likely that he took his direction from USDS and, under a holistic analysis, would not be considered an OPM employee. If OPM-6 was not an OPM employee, disclosure of OPM records to him violated the Privacy Act regardless of whether he needed that access to perform any duties that were assigned to him, whether by OPM or another agency.

For similar reasons, the plaintiffs are likely to succeed in showing that OPM-3 through OPM-5 are not OPM employees. Because the defendants have truncated the administrative record with respect to OPM-9 to OPM-18, their status is difficult to

States Government." 31 U.S.C. § 101. Courts have resisted further defining the term "agency" given "the myriad organizational arrangements for getting the business of the government done." Burch v. Pioneer Credit Recovery, Inc., 551 F.3d 122, 124 (2d Cir. 2008) (citation omitted).

predict. Nonetheless, there is reason to believe that at least OPM-14 and OPM-16 may have been employees of agencies other than OPM.

(c) Need to Review

Finally, the defendants contend that the plaintiffs have been unable to show that the relevant individuals did not have a need for access to the OPM systems in the performance of their duties. The Privacy Act allows a disclosure of OPM records to OPM employees when the employee has a "need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

The plaintiffs have pointed to clear evidence that the DOGE agents did not need access to the records disclosed to them, much less the administrative access that they were given. When Ezell requested access for OPM-2, OPM-4, and OPM-6 on January 27, he admitted that there was no need for access to the records at that time: "Right now we don't have immediate plans to change anything but if we need to we might need to move quickly."

(Emphasis supplied.) On February 6, Hogan explained "we have never needed access to ERHI/eOPF so if any access was granted there it can be removed immediately"; soon afterwards OPM removed access to eOPF and EHRI for OPM-2 through OPM-6. Hogan confirmed that OPM-2 through OPM-6 had never logged in to EHRI or eOPF, and OPM-3 and OPM-5 had not even completed the process

to create their accounts. More generally, the March Audit indicates that, as of March 6, most of the employees had not logged in to the systems to which the March Audit reflects they had been given access.

Hogan explained at the hearing that when access was granted to DOGE agents, "the intention" was that they "may have a need to use those permissions." (Emphasis supplied.) But a belief that there may be a need for access in the future does not qualify as a showing of need under Exception (b)(1). Moreover, there is ample evidence that an anticipatory grant of access is unnecessary. The record repeatedly shows OPM staff handling requests for access quickly, and Hogan testified that an expedited request for administrative access can be satisfied within minutes. The plaintiffs have shown that the DOGE agents would still have been able to "move quickly," as Ezell indicated they "might" need to do, without prematurely being given access they may never need.

The defendants have also objected that OPM should not be required to prepare a memorandum to justify each grant of access to its data systems. But the plaintiffs have neither argued nor implied that such a requirement exists under the Privacy Act, nor do they ask that OPM now implement such a process for the DOGE agents or anyone else. The conclusion that the DOGE agents

did not need access to the records disclosed to them is not based on a lack of formal documentation of purported need.

From their first submissions in this lawsuit, the defendants have argued that DOGE agents needed access to OPM records to effectuate the DOGE Executive Order and its mission of modernizing IT. For example, in his February 19 declaration, Hogan explained that, in addition to himself, the five DOGE Engineers were engaged with implementing the DOGE Executive Order. Hogan's declaration that access was needed to implement the DOGE Executive Order is not supported by the record evidence and is not credible. Indeed, while Hogan's testimony during the hearing was precise and responsive, his declarations filed in this action have left much to be desired. They have been incomplete and because of that misleading. Two examples suffice.

In his February 19 declaration, Hogan states that "to the best of my knowledge" all of the DOGE Engineers "have completed ethics trainings and training related to records management, cybersecurity, or data privacy." OPM-3, OPM-4, and OPM-6 only completed the latter training that very day, February 19, which was long after they were given access to OPM systems. Hogan's declaration omitted this troubling chronology and created the

false impression that there were no irregularities in the training.³⁸

Hogan also represented on February 19 that none of the DOGE Engineers “has” access to EHRI. But on January 27 Ezell had requested administrative access, including “code read and write permissions,” for all five DOGE Engineers to EHRI and several other OPM systems containing PII; OPM-2, OPM-4, and OPM-6 completed the process to obtain access. That access only began to be unwound on February 6, and it was only on February 16 that Hogan confirmed that their access had been removed. Again, the declaration did not reveal this history of access to EHRI, leaving the false impression that EHRI had never been at issue or at risk.

To be sure, the issue here is not whether OPM IT systems should be modernized. That is an entirely laudable goal and the plaintiffs do not suggest otherwise. Indeed, the Government has been engaged in IT modernization efforts for years. But, as the plaintiffs’ experts have explained, IT modernization does not necessarily require access to confidential PII. Individuals

³⁸ Hogan’s declaration that the DOGE Engineers had completed ethics training was also misleading. OPM-5 and OPM-6 are the only DOGE Engineers who completed that ethics training before February 19. OPM-2 and OPM-3 completed that training on February 19, the day of Hogan’s declaration. OPM-4 completed ethics training at GSA but not at OPM.

working on such projects generally act as developers tasked with enhancing a system or building a new system. For example, Nesting participated in modernization efforts at HHS and the Department of State without ever obtaining access to PII contained in the systems being modernized. Changes to the systems were tested without using real data, and whenever there were requests for confidential information they were handled by a limited set of authorized administrators. Nesting also testified that when the U.S. Digital Service assisted with enhancements to USA Staffing several years ago, limited access was given to some of the data in that specific system and only to a small team. Between this and the extensive evidence of the hasty and chaotic disclosures of OPM systems, the plaintiffs have rebutted any presumption of regularity on which the defendants seek to rely.

It is especially unlikely that any DOGE agents ever needed administrative access to any OPM systems. The defendants have not suggested that any of the individuals listed in the March Audit were tasked with primary responsibility for the deployment and normal functioning of an existing system, which is the type of work that normally necessitates administrative access. Underscoring the risks to the security of OPM's data systems that were created in the first three weeks of the new

administration, the plaintiffs have shown as well that in the process of giving the DOGE Engineers administrative access to OPM systems, database administrators who were responsible for the normal functioning of those systems had their access revoked. On February 6, Hogan reversed that decision and ordered that their access be restored immediately.

Finally, the defendants have to some extent switched gears and now argue that access to OPM systems was needed not to implement the DOGE Executive Order and its goal of IT modernization, but to implement the federal hiring freeze, pointing to Executive Orders 14,170 and 14,210. They explain that this is why Scales, Sullivan, and OPM-6 logged in to USA Staffing.³⁹ At the hearing, Hogan testified that these individuals were involved in a project to create popup screens to remind users of USA Staffing that a federal hiring freeze is in effect. While this provides some explanation as to why they were given access to USA Staffing, it still does not account for why all three of them needed the administrative access they were given. In any event, this limited explanation cannot account for the disclosure of records in other OPM systems to these individuals, or any disclosures to other DOGE agents.

³⁹ This argument also appears relevant in the defendants' eyes to the work done by OPM-9 through OPM-18.

ii. Lack of Appropriate Safeguards

The second Privacy Act claim asserts that the defendants violated § 552a(e)(10) of the Privacy Act, which creates a duty to safeguard the plaintiffs' records. This provision states:

Each agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

5 U.S.C. § 552a(e)(10); see Chambers v. U.S Dep't of Interior, 568 F.3d 998, 1007 n.7 (D.C. Cir. 2009).

The plaintiffs have shown a likelihood of prevailing on this claim as well. It is not disputed that OPM faces serious cybersecurity threats to the systems of records it maintains. OPM teaches about these threats in its Cybersecurity and Privacy Awareness Training. They include social engineering, malicious code, hacking, and denial-of-service attacks. OPM insiders, including current or former employees, can be a threat to cybersecurity through either malicious or accidental conduct. Cybersecurity threats can cause confidentiality breaches, integrity breaches, and availability breaches, all of which can substantially harm individuals on whom data is maintained in OPM systems. The 2015 OPM data breach is a reminder that such threats are not just theoretical. OPM has instituted a set of

safeguards to protect against these threats, including procedures for vetting and background investigations, training, and access control policies.

The plaintiffs have presented evidence that the defendants ignored many of OPM's safeguards in connection with the employees brought into OPM to pursue the DOGE agenda. For example, OPM employees are required to complete its Privacy and Cybersecurity Training when they join the agency. OPM has also relied on this training in PIAs for eOPF and EHRI to assure Congress that its employees will not misuse access to PII. This training contains the Rules of Behavior to which OPM employees must agree before OPM will give them access to its systems. Despite all of that, only Hogan, OPM-2, OPM-5, and OPM-7 completed the Privacy and Cybersecurity Training before OPM gave them access to OPM records.

Even more egregiously, the access control policies that OPM purports to follow fell by the wayside. DOGE Engineers and other DOGE agents were almost uniformly given administrative access without any need for that access. Such granting of maximum access is exactly the opposite of what the principle of least privilege requires, and was also inconsistent with the principle of separation of duties. OPM's departure from its basic cybersecurity practices, as well as the NIST standards and

Circular A-130, is reminiscent of the “failure of culture and leadership” that the 2016 House Report identified as having led to the 2015 OPM data breach.

In defending against this Privacy Act claim, the defendants argue only that OPM followed its established procedures for vetting and background checks. Even on this point, the record described above indicates otherwise.

2. Availability of Review Under the APA

The plaintiffs bring two claims under the APA. First, the plaintiffs assert that the defendants’ actions were contrary to law. Second, they assert that the OPM Defendants acted in an arbitrary and capricious manner because they failed to engage in reasoned decision-making when giving access to OPM records to individuals not authorized to have such access under the Privacy Act.

The APA enables a reviewing court to “hold unlawful and set aside agency action” that is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C.

§ 706(2)(A). Agency action is arbitrary and capricious

only if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Am. Cruise Lines v. United States, 96 F.4th 283, 286 (2d Cir. 2024) (citation omitted).

The plaintiffs have, as explained above, shown a likelihood of success in proving violations of the Privacy Act. Accordingly, the plaintiffs are likely to prove that the defendants' actions were "not in accordance with law" under 5 U.S.C. § 706(2) (A).

The plaintiffs have also shown that the OPM Defendants violated the APA by acting in an arbitrary and capricious manner. OPM's decision to give DOGE agents administrative access to multiple OPM systems containing PII was a gross departure from its obligations under the Privacy Act as well as its longstanding cybersecurity practices. The onboarding process was rushed and many of the relevant individuals did not complete required training before OPM gave them access to its systems. The DOGE agents' wide-ranging administrative access, which they were given without any credible need for access, violated the principles of least privilege and separation of duties. These departures from required security protocols that OPM claims to follow placed the security of OPM records at serious risk. OPM took these actions despite the instruction in the DOGE Executive Order that it "shall be implemented

consistent with applicable law" and that USDS shall "adhere to rigorous data protection standards."

The defendants argue that the plaintiffs' APA claims are not reviewable for two reasons. They contend that the plaintiffs fail to identify a final agency action, and that the plaintiffs cannot resort to the APA because they have "other adequate alternative remedies" under the Privacy Act. Neither argument succeeds.

i. Final Agency Action

The APA provides for judicial review only of "final agency action." 5 U.S.C. § 704. The APA defines "agency action" to include "the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act." 5 U.S.C. § 551(B). The word "action" is meant to "cover comprehensively every manner in which an agency may exercise its power." Whitman v. Am. Trucking Ass'ns, 531 U.S. 457, 478 (2001).

For an agency action to be "final," two conditions must be met: "First, the action must mark the consummation of the agency's decisionmaking process -- it must not be of a merely tentative or interlocutory nature. And second, the action must be one by which rights or obligations have been determined, or from which legal consequences will flow." Bennett v. Spear, 520

U.S. 154, 177-78 (1997) (citation omitted). Courts take a “pragmatic approach” in analyzing finality. U.S. Army Corps of Eng’rs v. Hawkes Co., 578 U.S. 590, 599 (2016). There is no requirement that there be a writing to memorialize a final agency action. See Brotherhood of Locomotive Eng’rs & Trainmen v. Fed. R.R. Admin., 972 F.3d 83, 100 (D.C. Cir. 2020).

The plaintiffs have shown that OPM engaged in a final agency action when it gave access to sensitive and legally protected records in violation of federal statutes, its own cybersecurity practices, and even the DOGE Executive Order. The decision to give access to DOGE agents was the “consummation” of OPM’s decision-making process; it was neither tentative nor interlocutory. OPM leadership demanded administrative access to multiple OPM systems for DOGE agents, beginning with a “911-esque call” on the evening of President Trump’s inauguration. Successive requests for access were couched as urgent and left no room for further deliberation. The usual training requirements for OPM employees were brushed aside.

It was also a decision from which legal consequences flow. As courts have emphasized, this prong must be assessed in a “pragmatic” fashion; the focus is on “the concrete consequences an agency action has or does not have.” Ipsen Biopharmaceuticals, Inc. v. Azar, 943 F.3d 953, 956 (D.C. Cir.

2019) (citation omitted). Here, the sensitive OPM records of tens of millions of Americans were disclosed to a cadre of individuals with no legal right to access those records and without adequate training. Their access was also inconsistent with cybersecurity principles that OPM is required to follow.

The defendants argue there was no final agency action because the events at issue here were "a series of discrete personnel decisions related to vetting, onboarding, and granting individual OPM employees access to OPM data systems." The administrative record indicates that this was not so. The decisions here were not discrete decisions as to individual employees. The actions taken do not reflect the application of customary agency procedures. Disclosure was not based on reasoned decisions about whose skills and talents were needed to modernize particular OPM systems and what training and access was necessary for that task with due regard to the security of those systems. For instance, the five DOGE Engineers were given access as a group, each was given administrative access to multiple systems, and their security training was an afterthought. The security training for three of the five was not completed until the date Hogan's declaration was due to be filed with the Court.

ii. Inadequacy of Alternative Remedies

The defendants next argue that the APA claims must be dismissed because the APA provides for judicial review only of agency actions “for which there is no other adequate remedy in a court.” 5 U.S.C. § 704. The “adequate remedy” requirement is “narrowly construed . . . to apply only in instances when there are ‘special and adequate review procedures’ that permit an adequate substitute remedy.” Sharkey v. Quarantillo, 541 F.3d 75, 90 n.14 (2d Cir. 2008) (quoting Bowen v. Massachusetts, 487 U.S. 879, 903 (1988)). An alternative remedy is not adequate if it provides only “doubtful and limited relief.” Bowen, 487 U.S. at 901. To be adequate, a remedy need not provide “identical” relief to that available under the APA “so long as it offers relief of the same genre.” Garcia v. Vilsack, 563 F.3d 519, 522 (D.C. Cir. 2009) (citation omitted).

As explained in the Opinion resolving the motion to dismiss, the Privacy Act does not provide an adequate remedy. See April 3 Opinion, 2025 WL 996542, at *18-19. In brief, while the Privacy Act provides monetary relief, it does not provide injunctive or declaratory relief for the claims at issue here. Monetary relief, which the plaintiffs do not seek in this action, cannot stop the illegal disclosures described here or mitigate any of the risks created by those disclosures. It

therefore would provide only “doubtful and limited relief.”

Bowen, 487 U.S. at 901.

3. Ultra Vires Review

The plaintiffs bring an ultra vires claim against the DOGE Defendants alone. The ultra vires right of action is a “nonstatutory” form of judicial review that derives from the inherent equitable powers of courts. Fed. Express Corp. v. U.S. Dep’t of Com., 39 F.4th 756, 765 (D.C. Cir. 2022). This doctrine is available when agency action is a clear departure from a statutory mandate or blatantly lawless. Id. at 764. Ultra vires claims are only available in the “extremely limited” circumstance where three requirements are met:

(i) the statutory preclusion of review is implied rather than express; (ii) there is no alternative procedure for review of the statutory claim; and (iii) the agency plainly acts in excess of its delegated powers and contrary to a specific prohibition in the statute that is clear and mandatory.

Yale New Haven Hosp. v. Becerra, 56 F.4th 9, 26-27 (2d Cir. 2022) (quoting DCH Reg’l Med. Ctr. v. Azar, 925 F.3d 503, 509 (D.C. Cir. 2019)).

The first of these requirements limits the availability of ultra vires review to situations where, on one hand, “Congress has not authorized statutory judicial review,” but, on the other hand, Congress “has not barred judicial comparison of agency action with plain statutory commands.” Fed. Express Corp., 39

F.4th at 765 (citation omitted). To satisfy the second requirement, plaintiffs must show that they have been “wholly deprived of a meaningful and adequate means of vindicating their alleged statutory rights.” Nat’l Air Traffic Controllers Ass’n AFL-CIO v. Fed. Serv. Impasses Panel, 437 F.3d 1256, 1264–65 (D.C. Cir. 2006) (quoting Bd. of Governors of Fed. Rsrv. Sys. v. MCorp Fin., Inc., 502 U.S. 32, 43 (1991)). The Supreme Court has suggested that ultra vires review is cabined to situations where it is needed to avoid “a sacrifice or obliteration of a right which Congress has given.” MCorp Fin., Inc., 502 U.S. at 43 (citation omitted). To satisfy the third requirement, plaintiffs must show that “the agency has plainly and openly crossed a congressionally drawn line in the sand.” Fed. Express Corp., 39 F.4th at 765.

As explained above, the plaintiffs have shown a likelihood of success under the APA and may obtain relief through an injunction targeted exclusively at the OPM Defendants. The plaintiffs have not shown, therefore, that they have a likelihood of success on their ultra vires claim, which pertains solely to the DOGE Defendants.

To be sure, the DOGE Defendants were likely participants in many of the illegal activities described in this Opinion. The plaintiffs have demonstrated that individuals affiliated with

DOGE obtained broad access to systems containing PII without an adequate showing of need, in contravention of both the Privacy Act and OPM's regular procedures and security standards. It is a fair inference that the DOGE Defendants instructed Ezell to expedite access to OPM systems for DOGE agents, leading to a "911-esque call" with OPM staff. Ezell and others at OPM have described the relevant individuals as "DOGE Engineers" and "DOGE employees," and Hogan has identified them as "DOGE affiliates." Many of the DOGE agents have done work on behalf of DOGE at multiple agencies, and at least some of them are likely to be USDS employees, or at least not OPM employees. The DOGE Defendants have no statutory authority with respect to OPM records, and by directing these activities they "plainly and openly crossed a congressionally drawn line in the sand." Fed. Express Corp., 39 F.4th at 765. Nonetheless, relief pursuant to the ultra vires claim is inappropriate because the APA already gives the plaintiffs meaningful relief for the violation of their rights.

B. Irreparable Harm

It is well established that a showing of irreparable harm "is the single most important prerequisite for the issuance of a preliminary injunction." JTH Tax, LLC v. Agnant, 62 F.4th 658, 672 (2d Cir. 2023) (citation omitted). "To satisfy their burden

to show irreparable harm, plaintiffs must demonstrate that absent a preliminary injunction they will suffer an injury that is neither remote nor speculative, but actual and imminent, and one that cannot be remedied if a court waits until the end of trial to resolve the harm.” Id. (citation omitted). It suffices for the plaintiffs to show “a threat of irreparable harm,” even if that harm has not yet materialized. Mullins v. City of New York, 626 F.3d 47, 55 (2d Cir. 2010). Irreparable harm may be found “where there is a threatened imminent loss that will be very difficult to quantify at trial.” Tom Doherty Assocs., Inc. v. Saban Ent., Inc., 60 F.3d 27, 38 (2d Cir. 1995).

The evidence that establishes the plaintiffs’ irreparable harm is largely the same as the evidence that establishes their standing. The plaintiffs have shown irreparable harm due to both the unlawful disclosure of OPM records to employees working on the DOGE agenda and the increased risk to cybersecurity because of the unlawful disclosure.

In brief, the OPM records at issue concern the plaintiffs’ most sensitive private affairs. They include social security numbers, health care information, banking information, and information about family members. For some people, disclosure of information in OPM systems could subject them to danger. The

defendants have not identified any credible need that the DOGE agents had for the access to OPM systems that they were given, and the plaintiffs have shown that it is exceedingly unlikely that there was any such need. OPM disclosed systems containing PII in violation of federal law and cybersecurity safeguards that OPM purports to follow.

As has been explained, such actions increased the risk of cybersecurity breaches, including confidentiality breaches, integrity breaches, and availability breaches. The 2015 OPM data breach is a reminder of how important it is for OPM to follow basic cybersecurity protocols and the serious impact that failure to do so has on individuals' lives. As explained in the Lewis declaration, the wide-ranging access that OPM granted to the DOGE agents would be considered a security risk in the private sector, including at leading technology companies.

The defendants argue that the plaintiffs have not shown irreparable harm because OPM abided by "appropriate safeguards" in controlling access to its data systems. But that is simply not what the record shows. Instead, OPM set aside its established safeguards, increasing the risk of cybersecurity breaches.

The defendants also argue that the plaintiffs have not shown irreparable harm because they have not identified the

occurrence of an unauthorized “public” disclosure. This argument has multiple flaws.

First, an improper disclosure within the Government is a serious and cognizable harm. Congress enacted the Privacy Act in light of government abuse, including improper searches by government authorities during the Colonial Era, government investigations of federal employees in the McCarthy Era, and government wiretapping during the Watergate Era. The plaintiffs have an interest in avoiding the “Big Brother” government monitoring that the Privacy Act is designed to prevent. Thus, as the Second Circuit found in Trump v. Deutsche Bank AG, disclosure within the Government can constitute irreparable harm even without a further disclosure to the public. 943 F.3d 627, 637 & n.21 (2d Cir. 2019), vacated on other grounds, Trump v. Mazars USA, LLP, 591 U.S. 848 (2020). There, President Trump and members of his family were found to face irreparable harm based on the risk of disclosure of financial records to Congress. The Court of Appeals recognized their “interest in keeping their records private from everyone, including congresspersons.” Id. at 637 (citation omitted).

As significantly, lax cybersecurity is an ongoing risk that can lead to public disclosure, and it has done so in the past. That its impact may not be apparent to the public for years does

not mean that this risk is not serious or that it does not exist.

The Government's defense of this action reinforces the finding that irreparable harm exists. The Government could have acknowledged that in its rush to accomplish a new President's agenda mistakes were made and established, important protocols were overlooked. It has not. The Government has defended this lawsuit by repeatedly invoking a mantra that it adhered to all established procedures and safeguards. It did not. Without a full-throated recognition that the law and established cybersecurity procedures must be followed, the risk of irreparable harm will continue to exist.

Moreover, there is no reason to believe that the risk of irreparable harm has lessened since March 6, the date at which the administrative record is truncated. The Government has offered no reassurance that it is returning to a regime in which the disclosure of OPM records containing PII is restricted to OPM employees, and to only those OPM employees who have a need for those records in the performance of their OPM duties. Nor is there any indication that the Government has done an adequate audit to identify and mitigate the risks that were created by OPM giving improper access to its records.

C. Public Interest

The final issue is the determination of the public interest. "There is generally no public interest in the perpetuation of unlawful agency action. To the contrary, there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." League of Women Voters v. Newby, 838 F.3d 1, 12 (D.C. Cir. 2016).

The public interest strongly favors injunctive relief. The plaintiffs have shown that the defendants disclosed OPM records to individuals who had no legal right of access to those records. In doing so, the defendants violated the Privacy Act and departed from cybersecurity standards that they are obligated to follow. This was a breach of law and of trust. Tens of millions of Americans depend on the Government to safeguard records that reveal their most private and sensitive affairs.

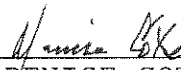
The defendants argue that an injunction will limit the Government's ability to effectuate the President's policy choices, in particular the need to modernize OPM IT systems. But this litigation does not challenge or undermine that policy. The modernization of IT systems has been an uncontroversial goal of the Government for years. The defendants have not shown that

a modernization effort will be hampered by compliance with the mandates of the Privacy Act or adherence to OPM's established cybersecurity protocols. Regardless, the defendants and the plaintiffs will be heard on the terms of the injunction to ensure that those terms do not interfere with a modernization effort.

Conclusion

The plaintiffs' April 25 motion for a preliminary injunction is granted. The scope of the injunction will be addressed in a separate Order.

Dated: New York, New York
June 9, 2025



DENISE COTE
United States District Judge