

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	:	
STATE OF NEW YORK, et al.,	:	
	:	
Plaintiffs,	:	25-CV-01144 (JAV)
	:	
-v-	:	<u>OPINION AND ORDER</u>
	:	
DONALD J. TRUMP, <i>in his official capacity as</i>	:	
<i>President of the United States</i> , et al.,	:	
	:	
Defendants.	:	
-----X	:	

JEANNETTE A. VARGAS, United States District Judge:

This is one of many lawsuits brought in recent weeks challenging aspects of the work of the newly established Department of Government Efficiency (“DOGE”). In this particular case, nineteen states (collectively, the “States” or “Plaintiffs”) represented by their respective Attorneys General, challenge the access to information provided to members of the DOGE team established at the U.S. Department of Treasury. Currently pending before this Court is Plaintiffs’ motion for a preliminary injunction pursuant to Rule 65 of the Federal Rules of Civil Procedure. Specifically, Plaintiffs seek to enjoin Defendants “from taking any action to develop, facilitate, or implement any process, whether automated or manual, for Treasury Department payment systems to flag and pause payment instructions for reasons other than the statutorily-authorized business of the Treasury Department”; and to restrain any Treasury Department employee (other than those in Senate-confirmed positions) from accessing any Treasury Department system that contained personally identifiable information (“PII”) or financial

information of payees, other than those “with a need for access to perform their lawful duties within the [BFS] who have passed all background checks and security clearances, taken all information security training called for in federal statutes and Treasury Department regulations, and have complied with all applicable government ethics rules.” ECF No. 51-1 at 2.

For the reasons stated herein, Plaintiffs’ motion for a preliminary injunction is GRANTED. The preliminary injunction substantially tracks the terms of the temporary restraining order (“TRO”) that is presently in place, in that it bars the Treasury Department from granting access to any member of the DOGE team within the Treasury Department to any payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees. But Plaintiffs have not demonstrated that they are entitled to the broad and sweeping relief they seek, which would far exceed the scope of the present TRO to prohibit members of the DOGE team from developing automated (or even manual) processes to halt payments coming through Treasury Department payment systems. The remedy in this case must be narrowly tailored to redress the specific harm asserted by the Plaintiffs: the threatened disclosure of the States’ sensitive bank information contained in the Treasury Department’s payment systems. Plaintiffs’ proposed preliminary injunction order is anything but narrow.

Additionally, the duration of the preliminary injunction also has the potential to be limited in scope. The Court is providing Defendants with an opportunity to promptly cure the procedural defects relating to the protection of sensitive and

confidential information that the Court has identified in this Opinion. Should Defendants do so, the Court will determine whether termination or modification of the preliminary injunction is warranted.

BACKGROUND

A. Factual History

“In deciding a motion for preliminary injunction, a court may consider the entire record including affidavits and other hearsay evidence.” *Park Irmat Drug Corp. v. Optumrx, Inc.*, 152 F. Supp. 3d 127, 132 (S.D.N.Y. 2016) (quotation marks omitted); *see also Mullins v. City of New York*, 626 F.3d 47, 52 (2d Cir. 2010).

Accordingly, the following facts are drawn from the entire record in this case, including the complaint, documents cited in the complaint, and the affidavits submitted by the parties. *See Banco San Juan Int’l, Inc. v. Federal Reserve Bank of New York*, 700 F. Supp. 3d 86, 92 (S.D.N.Y. 2023) (relying upon operative complaint as well as party affidavits in making findings of fact); *Pawelsky v. County of Nassau, New York*, 684 F. Supp. 3d 73, 78 n.1 (E.D.N.Y. 2023) (same).

1. The Bureau of the Fiscal Services

The Bureau of Fiscal Services (“BFS”) is an operational bureau within the U.S. Department of the Treasury. Compl., ¶ 67. BFS manages the federal government’s accounting, central payment systems, and public debt, and serves as the central payment clearinghouse for all payments to and from federal agencies. ECF No. 33 (“Second Krause Decl.”), ¶ 5. BFS handles 87.8% of the U.S. Government’s payments, valued at \$5.46 trillion annually, in over 1.2 billion transactions per year. ECF No. 32 (“Robinson Decl.”), ¶ 2; *see also* Second Krause

Decl., ¶ 5; Treasury Department Letter to Members of Congress Regarding Payment Systems, U.S. Dep't of the Treasury (Feb. 4, 2025), available at <https://perma.cc/Y6DF-UVZ4> (cited in Compl., ¶ 69 n.35). Included in those disbursements are funding to state governments for, *inter alia*, Medicaid, FEMA, Edward Byrne JAG grants, education, and foster care programs. Compl., ¶ 69.

BFS employs three primary payment systems, each of which performs critical functions in the federal government's financial infrastructure. ECF No. 34 ("Gioeli Decl."), ¶¶ 3, 5; Second Krause Decl., ¶ 14. The Payment Automation Manager ("PAM") is the primary application used by Treasury to process payments for disbursement. Gioeli Decl., ¶ 6. PAM includes several component sub-systems. *Id.* PAM's "file system" receives payment files from payor agencies into its "landing zone," the system that ingests payment files before agencies certify the payments for processing. Robinson Decl., ¶ 5. These payment files contain confidential personally identifiable information, including Social Security and bank account numbers, federal tax return information regulated by Internal Revenue Code section 6103, and Automated Clearing House data subject to 31 C.F.R. Part 210. Compl., ¶¶ 2, 48, 71. When payment files come into the "landing zone," they are transferred to the PAM application, where the payment file is validated. Robinson Decl., ¶ 5. BFS conducts a review of the file and generates a pre-edit report that, among other things, contains information about potentially improper or fraudulent payments. *Id.* For example, BFS will compare the payments in the file against the Do Not Pay working system, which is used to identify payments that may be improper or fraudulent. Second Krause Decl., ¶ 19. BFS notifies the submitting

agency of any potential issues with the payment, and the agency then reexamines the payment file to determine whether to ultimately certify it for processing. *Id.* The agency uses the Secure Payment System (“SPS”) to certify the payment file. Gioeli Decl., ¶ 8. Certified payments are then processed consistent with the agency’s instructions in the file. Robinson Decl., ¶ 5.

The other two BFS payment systems relevant here are the Automated Standard Application for Payments (“ASAP”) and International Treasury Services.gov (“ITS”). Second Krause Decl., ¶14; Gioeli Decl., ¶ 5. ASAP allows recipients to draw down funds from established accounts. Gioeli Decl., ¶ 7. ITS is used by federal agencies to make international payments, such as to recipients of Social Security benefits living abroad. *Id.* ¶ 9. All three payment systems feed information into the Central Accounting and Reporting System (“CARS”), which records data regarding agency spending for budgetary purposes. *Id.* ¶ 10; Second Krause Decl., ¶ 14.

2. The Department of Government Efficiency

On January 20, 2025, President Donald Trump issued Executive Order 14,158, entitled Establishing and Implementing the President’s “Department of Government Efficiency” (the “E.O.”). Exec. Order 14,158, 90 Fed. Reg. 8441 (Jan. 29, 2025). The E.O. established the Department of Government Efficiency, with the stated purpose of “implement[ing] the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.” E.O. § 1. The E.O. renamed the former United States Digital Service as the United States DOGE Service (“USDS”) and placed the USDS within the

Executive Office of the President. *Id.* § 3(a). The E.O. further created the U.S. DOGE Service Temporary Organization within the USDS, which is “dedicated to advancing the President’s 18-month DOGE agenda.” *Id.* § 3(b). The U.S. DOGE Service Temporary Organization is led by the USDS Administrator, who reports to the White House Chief of Staff. *Id.*

The E.O. calls for the creation of DOGE Teams within each executive agency. *Id.* § 3(c). The DOGE Teams are to consist of at least four employees, including one DOGE Team Lead, one engineer, one human resource specialist, and one attorney. *Id.* Agency Heads are required to consult with the USDS Administrator in selecting the members of the DOGE Team. *Id.* Additionally, Agency Heads are required to coordinate their work with USDS, and DOGE Team Leads are to “advise their respective Agency Heads on implementing the President’s DOGE Agenda.” *Id.*

The E.O. directs 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.” *Id.* § 4(a). One goal of this project is to “promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization.” *Id.* § 4(a). The E.O. commands agency heads to “take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems.” *Id.* § 4(b). USDS is required to “adhere to rigorous data protection standards.” *Id.*

3. The United States Treasury DOGE Team

Within a few days of the promulgation of the E.O., a DOGE Team was formed at the Treasury Department. Second Krause Decl., ¶ 1. Although the E.O. calls for a minimum of four members to each DOGE Team, to date the DOGE Team embedded within the Department of Treasury has never had more than two members (and currently only has one member): Thomas H. Krause, Jr., the DOGE Team Lead, and Marko Elez, who was the Treasury DOGE Team's technical specialist prior to his resignation. *Id.* ¶ 3. No attorney or human resource specialist has been named to serve on the Treasury DOGE Team. *Id.*

a. Thomas Krause

Krause is the DOGE Team Lead at the Treasury Department. Second Krause Decl., ¶¶ 1-2. Although Krause claims to have been hired by the Treasury Department for this position, he also suggests that USDS/DOGE "placed" him in the Treasury Department. *Id.* ¶ 11. However his appointment came to be, the Treasury Department created the role of Senior Advisor for Technology and Modernization for Krause, *id.* ¶¶ 1-2, and on January 23, 2025, he was appointed as a consultant for Treasury in accordance with 5 U.S.C. § 3109, ECF No. 31 ("Wenzler Decl."), ¶ 3. Consultants appointed under the authority of section 3109 are deemed to be federal employees. 5 C.F.R. § 304.101. Krause waived compensation and is serving unpaid. Wenzler Decl., ¶ 3.

Krause's duties as Senior Advisor, as set forth in his appointment paperwork, were to assist in executing BFS's "mission of promoting the financial integrity and operational efficiency of the federal government through exceptional accounting,

financing, collections, payments, and shared services.” Wenzler Decl., ¶ 6. He was charged with focusing on issues related to operational resiliency; advancing government-wide payment integrity; critical modernization programs; improving the payment experience; and TreasuryDirect user credential costs. *Id.*

Yet Krause’s appointment as a consultant meant that, as a legal matter, he was circumscribed in the authority he could wield. As Defendants acknowledge, under the governing regulation, agencies are prohibited from employing consultants to perform managerial or supervisory work, to make final decisions on substantive policies, or to function in the agency chain of command. 5 C.F.R. § 304.103(b); *see also* Wenzler Decl., ¶ 7. Accordingly, the Treasury Department soon began to explore options to retain Krause under different hiring authority. *Id.* ¶ 8. On February 13, 2025, Krause was converted to a Temporary Transitional Schedule C appointment pursuant to 5 C.F.R. § 213.3302. ECF No. 58 (“Third Krause Decl.”), ¶¶ 3-4. Section 213.3302 permits federal agencies to create positions “necessary to assist a department or agency head during the 1-year period immediately following a change in presidential administration.” *Id.* § 213.3302(a). Such positions “may be established only to meet legitimate needs of the agency in carrying out its mission during the period of transition associated with such changeovers,” and “[t]hey must be of a confidential or policy-determining character.” *Id.* Upon his conversion, Krause assumed the duties of the Fiscal Assistant Secretary. Third Krause Decl., ¶ 4. In that role he oversees the activities of BFS. Second Krause Decl., ¶ 5.

Notwithstanding the high-level roles he has assumed within the U.S. Government, Krause has maintained his position as the CEO of Cloud Software Group, “one of the largest privately held enterprise software companies globally.” *id.* ¶ 6. To address the ethics issues resulting from this arrangement, the Treasury Department designated Krause a Special Government Employee (“SGE”) under 18 U.S.C. § 202. *Id.* ¶ 1. An SGE is an officer or employee of the executive branch who is retained, designated, appointed, or employed to perform, with or without compensation, temporary duties for a period of time not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days. 18 U.S.C. § 202. SGEs are exempted from certain conflict-of-interest prohibitions set forth in Chapter 11 of the Criminal Code. *See, e.g., id.* §§ 203(c), 205(c); *see also* Wenzler Decl., ¶ 11.

Krause claims that he is “not an employee of USDS/DOGE,” but an employee of the Treasury Department. Second Krause Decl., ¶ 4. The Court notes, however, that in his role as DOGE Team Lead, Krause coordinates closely with officials at USDS/DOGE. He provides USDS/DOGE officials with regular updates on his work. *Id.* He also “receive[s] high-level policy direction” from USDS/DOGE. *Id.*

Krause explained that one of his goals was to understand how “BFS’s end-to-end payment systems and financial report tools work, recommend ways to update and modernize those systems to better identify potentially improper and fraudulent payments, and find ways to assist federal agencies in responding to statutes, regulations, and Executive Orders that affect the Government’s payment authorities and spending priorities.” *Id.* ¶ 11. Krause cites various GAO reports

that have highlighted issues in properly accounting for transactions between federal agencies and its weaknesses in identifying fraudulent payments. *Id.* ¶¶ 7-9. The GAO has called upon agencies to improve their collection and use of data to prevent and detect fraud. *Id.*

b. Marco Elez

Marco Elez was hired as the second member of the Treasury DOGE Team, where he was given the title of Special Advisor for Information Technology and Modernization. Wenzler Decl., ¶ 9. Elez is a software engineer who previously worked at several of Elon Musk’s companies, including SpaceX and X. Second Krause Decl., ¶ 3. Elez was “recommended” to Krause and Treasury leadership by unspecified people within USDS/DOGE. *Id.*

Elez’s tenure at the Treasury Department was brief: he was appointed on January 21, 2025, and resigned 16 days later, on February 6. Wenzler Decl., ¶ 9. Elez was appointed to a Temporary Transitional Schedule C position. *Id.* Unlike Krause, Elez was not designated as an SGE. *Id.* ¶ 11. Elez’s official duties, as set forth in his appointment paperwork, were to conduct “special and confidential studies on a variety of strategies and issues related to Treasury’s information technology,” as well as making recommendations as to how to “strengthen Treasury’s hardware and software.” *Id.* ¶ 10.

c. The Engagement Plan

Upon the DOGE Team’s arrival at the Treasury Department, BFS decided to “develop and implement a 4–6 week payment process engagement plan” that would outline how BFS would support the Treasury DOGE Team (the “Engagement

Plan”). Robinson Decl., ¶ 6. The purpose of this Engagement Plan was to provide the DOGE Team with insight into the full, end-to-end BFS payment processes, to identify data gaps that could make the systems work more efficiently, and “identify opportunities to advance payment integrity and fraud reduction goals.” *Id.*; *see also* Second Krause Decl., ¶ 13. “The scope of work as envisioned in the engagement plan required access to [BFS] source code, applications, and databases across all the [BFS] payment and accounting systems and their hosting environments.” Gioeli Decl., ¶ 11. The Treasury Secretary approved the Engagement Plan. Second Krause Decl., ¶ 15.

BFS immediately apprehended that the broad level of access being provided to the DOGE Team posed risks to the security of its sensitive payments systems. *Id.* Those risks included “access to sensitive data elements, insider threat risks, and other risks that are inherent to any user access to sensitive IT systems.” Gioeli Decl., ¶ 11. BFS employees therefore developed a mitigation strategy to reduce those risks as part of the Engagement Plan. *Id.*

For example, Elez was provided with a BFS laptop, which would be his only method of connecting to the various BFS payment systems. *Id.* ¶ 12. BFS “used several cybersecurity tools to monitor [Elez’s] usage of his BFS laptop . . . and continuously log his activity.” *Id.* BFS also enabled enhanced monitoring on the laptop, which included “the ability to monitor and block website access, block the use of external peripherals (such as USB drives or mass storage devices), monitor any scripts or commands executed on the device, and block access to cloud-based

storage services.” *Id.* Additionally, the laptop contained data exfiltration detection. *Id.*

Elez was also supposed to be limited to read-only access to PAM and SPS, which would allow him to view and query information and data but would not allow him to make any changes to that data. *Id.* ¶ 17. Krause was given “over the shoulder” access by which he could view BFS payment systems or source code while they were being accessed by another person with the required access and permissions. *Id.* ¶ 4.

At the hearing held on Plaintiffs’ motion, the Court inquired of counsel for Defendants as to whether Krause or Elez were provided with any training on “the array of federal regulations that govern handling of information of a sensitive nature such as, for example, Internal Revenue Code regulations governing the handling of return information [or] regulations governing the handling of Social Security numbers.” ECF No. 68 (“PI Hearing Tr.”) at 20:13-19. In response, counsel for Defendants referred the Court to paragraph 14 of the Gioeli Declaration, which states that BFS “would provide safeguarding and handling instructions for Treasury data for the duration of the project,” and that Elez and Krause were instructed “that no Treasury information and data could leave the Bureau laptop for the duration of the engagement.” Gioeli Decl., ¶ 14. From this description, it does not appear that Elez and Krause were provided any specific training on the numerous federal regulations and policies governing the handling and care of sensitive information.

Pursuant to the Engagement Plan, on January 28, 2025, BFS provided Elez with an encrypted laptop and copies of the source codes for PAM, SPS, and ASAP in a “separate, secure coding environment known as a ‘secure code repository’ or ‘sandbox.’” *Id.* ¶ 16. Elez could review and make changes to the source code in the sandbox, but he could not publish any changes to the actual payment systems themselves. *Id.*

On February 3, Elez was provided read-only access, through his BFS laptop, to the PAM Database and PAM File System. *Id.* ¶ 17. He received a walk-through demonstration that same day of those payment systems. Although his access to PAM was “closely monitored” that day by “multiple BFS administrators,” *id.* ¶ 18, it does not appear as if his access was subsequently monitored other than through the logging program; BFS is still in the process of reviewing those logs to determine what actions Elez took with respect to PAM while he had access to those systems. *Id.*

On February 5, Elez was given access to the SPS database. *Id.* ¶ 19. He accessed the database once under the supervision of BFS administrators in a virtual walkthrough session. *Id.* Elez resigned the next day, and thus did not have the opportunity to access the database further. *Id.* Yet BFS later discovered that they had erroneously provided Elez with read/write permissions for the SPS database. *Id.* ¶ 20.

Despite the security measures that were available, the record is less clear as to the extent they were actually employed or were adequate to protect against unauthorized disclosures of the information contained in the BFS systems. The

Government's declarations indicate that it had the "ability" to block Elez's access to peripherals on his BFS laptop but is silent as to whether it actually did so. *Id.* ¶ 12. Elez was apparently allowed, for example, to take screenshots of BFS data. *Id.* ¶ 4. Elez also sent emails outside of the Treasury Department to USDS/DOGE. PI Hearing Tr. at 15:18-23. The Treasury Department cannot say whether or not those emails contained sensitive BFS data. *Id.* at 15:17-22. More than a week after Elez resigned from the Treasury Department, BFS was still in the process of reviewing the logs of Elez's activity on his laptop and within the BFS systems to determine if there was any unauthorized use. Gioeli Decl., ¶ 21. Although a preliminary review of those logs did not reveal any use outside the scope of the Engagement Plan, it is notable that Treasury has to conduct a forensic review of Elez's activity and review the logging reports in order to determine what precisely Elez was doing during the periods he had access to BFS source codes and payment systems.

d. DOGE Team Work on Automating Pauses of Payments

One of the Treasury DOGE Team's tasks was to "help agencies effectuate the President's Executive Orders requiring pauses to certain types of financial transactions." Second Krause Decl., ¶ 17. Their efforts in this area have to date been focused on intercepting payments potentially implicated by the President's Executive Orders regarding foreign development assistance, including the January 20, 2025 Executive Order entitled "Reevaluating and Realigning United States Foreign Aid." *Id.* The DOGE Team assisted in developing a process to identify payment files within the PAM file system's "landing zone" potentially implicated by

the Executive Order and to flag those payments for the State Department prior to their entry into the PAM payment processing systems. Robinson Decl., ¶ 8; Second Krause Decl., ¶¶ 18-19.

The DOGE Team originally focused on developing a process to intercept potential USAID payment files. Robinson Decl., ¶ 8. On January 27, however, the State Department decided that it would review USAID files prior to the initial submission to BFS, rendering the BFS intercept process unnecessary. *Id.* Ultimately, no USAID payments were interrupted as a result of the DOGE Team's work. *Id.*

On January 31, 2025, BFS and the DOGE Team developed a process to identify incoming payment files to the "landing zone" associated with one of four specified Treasury Account Symbol ("TAS") codes. *Id.* ¶ 10; Second Krause Decl., ¶ 20. TAS codes are identifiers for particular agency accounts. Robinson Decl., ¶ 10. The four TAS codes at issue were non-USAID payments that nonetheless may have been covered under the foreign aid Executive Order. *Id.* BFS created copies of the payment files containing those TAS codes and moved them into a separate folder (the "MoveIT" folder) where they could then be sent to the State Department for further review. *Id.*

BFS career staff initially queried the PAM file system manually to identify the implicated payment files and shared those payment files with Elez for review through the MoveIT folder. *Id.* ¶ 11. At some point after January 31, Elez assisted in automating the manual review of the payment files. *Id.* On the morning of February 7, 2025, four payment files were flagged, but the State Department

ultimately determined that the payments were not implicated by the foreign aid Executive Order, and the four payment files were processed that same day. *Id.* ¶ 13. On February 10, another payment file was flagged for further review by the State Department; the State Department requested that BFS not process the payment. *Id.* ¶ 14.

B. Procedural History

On February 7, 2025, the Attorneys General of nineteen states (collectively, the “States”) filed a Complaint, ECF No. 1 (“Compl.”), which also served as a Request for Emergency Temporary Restraining Order Under Federal Rule of Civil Procedure 65(B), seeking declaratory and injunctive relief. The States are each recipients of significant amounts of federal funds, which are processed through BFS. *Id.* ¶¶ 74-120. In order to receive funds through BFS payment systems, the States provide the Treasury Department with their wiring and bank account information. *Id.* ¶¶ 76-80. Additionally, the sensitive, confidential information of State residents, including social security numbers, bank account information, and federal tax return information, is also contained in the BFS payment systems. *Id.* ¶¶ 74-75.

In their TRO application, the States alleged that the Treasury Department had provided access to their data to DOGE officials who “were not employees of Treasury,” in violation of federal law. *Id.* ¶ 138. They further alleged that the “conduct of DOGE members presents a unique security risk to States and State residents whose data is held by BFS.” *Id.* ¶ 139; *see also id.* ¶ 10. The States cited media reporting that DOGE had been feeding data from federal agencies into an open-source Artificial Intelligence system owned and controlled by a private third

party, without measures taken to ensure its security. *Id.* ¶ 10. The States argued that “[u]nsecure data is susceptible to cyber attacks and identity theft.” *Id.* ¶ 140. The Complaint also raised concerns that this new policy had been implemented as a mechanism to block payments to States that they were entitled to under federal law. *Id.* ¶¶ 15, 141, 174, 189.

The Complaint contends that the policy of granting expanded access to the BFS payment systems to DOGE officials violates the Administrative Procedure Act (“APA”), 5 U.S.C. §§ 551 *et seq.*; exceeds the statutory authority of the Department of the Treasury; violates the separation of powers doctrine; and violates the Take Care Clause of the United States Constitution. *Id.* ¶¶ 154-99.

In support of their motion, Plaintiffs submitted the Affirmation of Colleen K. Faherty, which explained that Plaintiffs were concerned that the expanded access to BFS payment systems granted to officials associated with DOGE would result in the “numerous injuries as described in the” Complaint. ECF No. 5 (“Faherty Aff.”), ¶¶ 4-5.

On February 8, 2025, the Part I Judge granted the States’ emergency request for an *ex parte* Temporary Restraining Order (ECF No. 7) to restore the status quo prior to the agency action. ECF No. 6 (“February 8 TRO”). Based upon his review of Plaintiffs’ submissions, the Part I Judge determined that the States had adequately shown that they faced “irreparable harm in the absence of injunctive relief,” specifically “because of the risk that the new policy presents of the disclosure of sensitive and confidential information and the heightened risk that the systems in question will be more vulnerable than before to hacking.” *Id.* at 2. The Part I

Judge further found that the States “have shown a likelihood of success on the merits of their claims, with the States’ statutory claims presenting as particularly strong.” *Id.*

The February 8 TRO restricted Defendants from

granting access to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees, other than to civil servants with a need for access to perform their job duties within the Bureau of Fiscal Services who have passed all background checks and security clearances and taken all information security training called for in federal statutes and Treasury Department regulations [and] from granting access to all political appointees, special government employees, and government employees detailed from an agency outside the Treasury Department, to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees.

Id. at 3. The TRO also scheduled a show cause hearing on Plaintiff’s motion for a preliminary injunction for February 14, 2025. *Id.* at 2.

On the evening of February 9, 2025, Defendants filed an Emergency Motion to Dissolve, Clarify, or Modify the *Ex Parte* TRO. ECF No. 11. Defendants argued that the February 8 TRO’s restriction on access by political appointees, to the extent it included the Secretary of the Treasury and other senior Treasury leadership, raised constitutional concerns and should be dissolved. ECF No. 12 at 5-6.

Defendants alternatively sought modification of the February 8 TRO to allow for access by contractors who provided operational support for the payment systems

and employees of the Federal Reserve Bank who were responsible for helping to maintain several of the payment systems on Federal Reserve servers. *Id.* at 8-9.

Although the parties reached agreement on proposed language to modify the February 8 TRO as it regards the issue of access by Federal Reserve employees and outside contractors, Plaintiffs opposed any modification to the February 8 TRO's prohibition of access for political appointees. ECF No. 20 at 3-5. The Court granted in part and denied in part the motion to modify the TRO. ECF No. 28 ("Modified TRO"). The Modified TRO clarified that the Secretary of the Treasury and other Senate-confirmed senior Treasury Officers were not prohibited from accessing the Treasury's payment systems. *Id.* at 6-7. Federal Reserve employees and outside contractors were also allowed access to the BFS payment systems. *Id.* at 7.

In advance of the preliminary injunction hearing, the Court issued an Order requiring the parties to submit a joint letter setting forth their positions regarding the process that should be followed in adjudicating Plaintiffs' motion for a preliminary injunction. ECF No. 29. As set forth in that joint submission, neither party sought any discovery in advance of the preliminary injunction hearing. ECF No. 49 at 4. Additionally, the parties agreed that an evidentiary hearing in connection with the preliminary injunction motion was not needed, and that the parties were instead relying solely on the parties' submissions and oral argument at the hearing. *Id.* Finally, neither party sought consolidation of the hearing on the preliminary injunction motion with a trial on the merits. *Id.* at 4-5.

In opposition to the TRO and the preliminary injunction motion, Defendants submitted (1) three declarations from Thomas Krause, the DOGE Team Lead at the

Treasury Department, ECF Nos. 13, 33, 58; (2) two declarations from Vona Robinson, the Deputy Assistant Commissioner for Federal Disbursement Services at BFS, ECF Nos. 32, 47; (3) the Declaration of Joseph Gioeli III, the Deputy Commissioner for Transformation and Modernization at BFS, ECF No. 34; and (4) the Declaration of Michael J. Wenzler, the Associate Chief Human Capital Officer for Executive and Human Capital Services at the Department of the Treasury, ECF No. 31.

After having the benefit of those submissions, which clarified the chain of events at the Treasury Department, Plaintiffs submitted a reply brief that modified their position regarding the nature of the agency action that was the subject of their motion. ECF No. 51 (“Pls. Rep. Br.”). Plaintiffs indicated that they no longer sought an injunction focused on “the category of employee” engaged in the challenged conduct, but rather on the challenged conduct itself. *Id.* at 1.¹

Plaintiffs submitted a Proposed Preliminary Injunction Order that would restrain Defendants “from taking any action to develop, facilitate, or implement any

¹ It bears noting that, in seeking an emergency TRO, Plaintiffs (based largely on media reporting) alleged that Defendants were allowing the BFS payment systems to be accessed on non-government third-party servers, and potentially feeding information from those systems into a cloud based open-source Artificial Intelligence (“AI”). Compl. ¶¶ 9-11. Plaintiffs further claimed that the “third party cloud computing service that DOGE is reportedly using for this effort has experienced at least one major security breach.” *Id.* ¶10. Plaintiffs also alleged that Elon Musk, whom they referred to as the co-head of DOGE, made comments about wanting to put the BFS payment system on the blockchain. *Id.* ¶¶ 6, 9. Ultimately, in connection with the preliminary injunction proceedings, Defendants submitted evidence rebutting these allegations. Accordingly, in deciding Plaintiffs’ preliminary injunction motion, the Court is proceeding with a markedly different record than was before the Court on the emergency TRO application.

process, whether automated or manual, for Treasury Department payment systems to flag and pause payment instructions for reasons other than the statutorily-authorized business of the Treasury Department”; prevent any Treasury Department employee (other than those in Senate-confirmed positions) from accessing any Treasury Department system that contained PII or financial information of payees, other than those “with a need for access to perform their lawful duties within the [BFS] who have passed all background checks and security clearances, taken all information security training called for in federal statutes and Treasury Department regulations, and have complied with all applicable government ethics rules”; and require Defendants to maintain the quarantine of all devices and logs used by the Treasury DOGE Team members while working at the Treasury Department. ECF No. 51-1.

The Court held a hearing on Plaintiffs’ motion for a preliminary injunction on February 14, 2025. At the conclusion of the hearing, the Court reserved decision on the preliminary injunction motion, but held that there was good cause to extend the Modified TRO while it considered the arguments presented by the parties.

DISCUSSION

The Court first addresses the threshold question of standing, as that goes to the Court’s subject matter jurisdiction. The Court then applies the traditional four-factor test that governs the Court’s consideration of Plaintiffs’ preliminary injunction motion: likelihood of success on the merits, irreparable harm, the balance of equities, and the public interest.

I. STANDING

Under Article III of the Constitution, the federal judiciary is limited to hearing “Cases” and “Controversies.” This constitutional limitation requires a plaintiff to prove that they have a personal stake in the litigation, i.e., standing. “To demonstrate their personal stake, plaintiffs must be able to sufficiently answer the question: ‘What's it to you?’” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (citation omitted). Standing is measured by the three-part test set forth in *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiffs must show an injury in fact that is (i) actual and imminent; (ii) fairly traceable to the challenged conduct of the defendant; and (iii) likely to be redressed by a favorable judicial decision. *Id.*; see also *TransUnion*, 594 U.S. at 423. These requirements ensure that the federal courts are not “exercise[ing] general legal oversight of the Legislative and Executive Branches,” but are instead confining themselves to resolving disputes with real consequences for the parties. *TransUnion*, 594 U.S. at 423-24.

“[T]o establish standing for a preliminary injunction, ‘a plaintiff cannot rest on such mere allegations as would be appropriate at the pleading stage but must set forth by affidavit or other evidence specific facts, which for purposes of the summary judgment motion will be taken to be true.’” *Do No Harm v. Pfizer Inc.*, 126 F.4th 109, 119 (2d Cir. 2025) (quoting *Cacchillo v. Insmmed, Inc.*, 638 F.3d 401, 404 (2d Cir. 2011)).

A. Injury in Fact

To show an injury in fact, the alleged injury must be “concrete,” meaning “particularized, and actual or imminent.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (1983). When assessing whether the unauthorized disclosure of confidential information qualifies as a concrete injury sufficient to bring a claim for injunctive relief—particularly in cases involving the disclosure of PII—this Court is guided by the Supreme Court’s decision in *TransUnion* and the Second Circuit’s decision in *Bohnak v. Marsh & McLennan Companies, Inc.* 79 F.4th 276, 279-80 (2d Cir. 2023).

In *Bohnak*, the plaintiff’s PII was accessed by an unauthorized third party that accessed her name and Social Security number (“SSN”) through a targeted data breach of her employer. 79 F.4th at 280. The *Bohnak* court thus had to consider “the proper framework for evaluating whether an individual whose [PII] is exposed to unauthorized actors, but has not (yet) been used for injurious purposes such as identity theft, has suffered an injury in fact for purposes of . . . Article III standing to sue for damages” *Id.* at 279.

The Second Circuit instructed that whether plaintiff has suffered a cognizable injury-in-fact from an unauthorized data disclosure should be analyzed under a two-part framework, which considers first whether an injury is sufficiently concrete under the Supreme Court’s decision in *TransUnion* and second whether the injury is actual or imminent. *Id.* at 287-89. Although *Bohnak* concerned a suit for damages, as opposed to injunctive relief, this Court will apply the two-part *Bohnak* framework and analyze Plaintiffs’ standing accordingly.

1. *TransUnion: Concreteness*

In *TransUnion*, Sergio Ramirez, the named plaintiff, filed a class action lawsuit seeking statutory damages for TransUnion’s violations of the Fair Credit Reporting Act (“FCRA”). 594 U.S. at 417. TransUnion, a major credit reporting agency, conducted credit checks using a third-party software to compare the consumer’s name against the United States Treasury Department’s Office of Foreign Assets Control list of “specially designated nationals who threaten America’s national security” (“OFAC List”). *Id.* at 419-20. When Ramirez attempted to purchase a car, his name was flagged as being a “potential match” on the OFAC List, and the car dealership refused to sell him a car. *Id.* at 420. Ramirez brought suit under the FCRA, alleging that TransUnion “failed to follow reasonable procedures to ensure the accuracy of information in his credit file.” *Id.* at 421. Ramirez sought certification of a class consisting of all persons whom TransUnion had internally matched in its system as being on the OFAC List, even though only a portion of the class members had had credit reports disseminated to potential creditors. *Id.*

To determine whether the class members had standing to recover monetary damages, the Supreme Court assessed “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.” *Id.* at 424 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). *TransUnion* instructs that, while “history and tradition offer a meaningful guide . . . an exact duplicate in American history and tradition” to the plaintiff’s alleged harm is not required. *Id.*

Applying these principles, the *TransUnion* Court concluded that the class plaintiffs whose credit reports had been disclosed to creditors had suffered a concrete injury closely related to the “reputational harm associated with the tort of defamation” by having their names falsely identified as potentially being an individual on the OFAC List. *Id.* at 432. In contrast, the Supreme Court held that there was no historical analogue for a suit for damages based upon unpublished reports, no matter their inaccuracies. *Id.* at 433-34.

Notably, in reaching this decision, the Supreme Court emphasized that the result may well have been different if the plaintiff class members had been seeking injunctive relief rather than retrospective damages. *Id.* at 435. Specifically, “a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.” *Id.*; *see also Bohnak*, 79 F.4th at 285 (noting that the Supreme Court in *TransUnion* “explained that, although mere risk of future harm does not provide standing to seek retrospective damages where actual harm never materialized, ‘a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.’”); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155 (3d Cir. 2022) (“Where the plaintiff seeks injunctive relief, the allegation of a risk of future harm alone can qualify as concrete as long as it ‘is sufficiently imminent and substantial.’” (citation omitted)); *Rand v. Travelers Indem. Co.*, 637 F. Supp. 3d 55, 65 (S.D.N.Y. 2022) (relying upon

TransUnion in holding that a different standard applied to standing for claims for injunctive relief and for compensatory damages).

When applying the *TransUnion* framework to *Bohnak*, the Second Circuit concluded that the “exposure of Bohnak’s private PII to unauthorized third parties” bore a “close relationship to a well-established common-law analog: public disclosure of private facts.” *Bohnak*, 79 F.4th at 285 (citing *Restatement (Second) Torts* § 652D). Indeed, the Second Circuit underscored that the “disclosure of private information” was explicitly listed as an intangible harm “traditionally recognized as providing a basis for lawsuits in American courts.” *Id.* at 285-86. Therefore, the “core of the injury” Bohnak experienced was “the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor,” falling right within the “scope of an intangible harm the Supreme Court has recognized as ‘concrete.’” *Id.* (citing *TransUnion*, 594 U.S. at 424-25).

As the Second Circuit did in *Bohnak*, this Court uses *TransUnion* as the “touchstone” to determine whether the States have adequately alleged a concrete harm. The Court holds that they have. Specifically, Plaintiffs have adequately alleged both past harm in the unauthorized disclosure of the States’ confidential financial information to the DOGE Team, and the risk of future harm, in the risk of exposure of their confidential information to officials of USDS/DOGE and to the public through potential hacking. The unauthorized disclosure of the States’ confidential information is an intangible harm that is “traditionally recognized as providing a basis for lawsuits in American courts.” *Bohnak*, 79 F.4th at 285.

2. Imminence

To have standing to pursue forward-looking injunctive relief, the risk of harm alleged by Plaintiffs must be “sufficiently imminent and substantial.” *Bohnak*, 79 F.4th at 285. “A substantial risk means there is a ‘realistic danger of sustaining a direct injury.’” *Raw Story Media, Inc. v. OpenAI, Inc.*, No. 24-cv-01514 (CM), 2024 WL 4711729, at *4 (S.D.N.Y. Nov. 7, 2024) (quoting *Pennell v. City of San Jose*, 485 U.S. 1, 8 (1988)).

The Court finds, based on the record before it, that Plaintiffs have established that there is a realistic danger that confidential financial information will be disclosed absent the grant of injunctive relief. First, the record establishes that a member of the Treasury DOGE Team sent emails to government employees outside of the Treasury Department. The Treasury Department currently does not know whether those emails disseminated confidential PII outside the Treasury Department, potentially in contravention of the Privacy Act and section 6103 of the Internal Revenue Code. PI Hearing Tr. at 15:18-23.

More fundamentally, there is a realistic danger that the rushed and ad hoc process that has been employed to date by the Treasury DOGE Team has increased the risk of exposure of the States’ information. Defendants themselves concede that granting such broad and unprecedented access to the members of the Treasury DOGE team created heightened security risks, Gioeli Decl., ¶¶ 4, 11, 15, 17, but contend that their mitigation efforts were sufficient to reduce that risk, *id.* ¶¶ 4, 11, 13, 15, 17. By Defendants’ own account, however, their mitigation efforts did not completely address those risks. *Compare Id.*, ¶ 13 (“Additional mitigation measures

that were adopted included that Mr. Elez would receive ‘read-only’ access to the systems.”) *with id.* ¶ 20 (“[I]t was discovered that Mr. Elez’s database access to SPS on February 5 had mistakenly been configured with read/write permissions instead of read-only.”) And the record demonstrates that the granting of access to the Treasury DOGE Team was rushed and undertaken under political pressure. PI Hearing Tr. at 18:19-23; *id.* at 19:9-11; *id.* at 53:11-13 (“[T]ime was of the essence because the executive order made time of the essence and compliance with them made time of the essence.” (cleaned up)); Second Krause Decl., ¶¶ 11, 13, 17; Gioeli Decl., ¶ 4; Robinson Decl., ¶ 6. In that environment, it is unclear whether training was provided to the individuals who were to be granted that access. PI Hearing Tr. at 20:14-21:23. The critical sensitivity of the information contained in the BFS payment systems, which includes the PII and confidential information of both the States and millions of their residents, requires more than a band-aid approach to cybersecurity.

Courts have routinely found that plaintiffs have standing to seek injunctive relief where inadequate cybersecurity measures put their confidential information at risk of disclosure. *See, e.g., Baton v. Ledger SAS*, 740 F. Supp. 3d 847, 882 (N.D. Cal. 2024) (“Plaintiffs have plausibly alleged that they have Article III standing for a claim for injunctive relief against TaskUs, because they remain at risk due to Defendants’ continuing inadequate security system.”); *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 473 (S.D.N.Y. 2022) (plaintiffs “plausibly allege that they face a substantial risk of future harm if USAA’s security shortcomings are not redressed, making this dispute sufficiently real and immediate with respect to the parties’

legal relations, which are adverse” (cleaned up)); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 414-15 (E.D. Va. 2020) (“Plaintiffs have plausibly alleged the continued inadequacy of Defendants’ security measures. And in that respect, Plaintiffs plausibly allege that they face a substantial risk of future harm if Amazon's security shortcomings are not redressed.”)

Defendants insist that the Court must evaluate the imminence of the risk of future harm under the test set forth by the Second Circuit in *McMorris v. Carlos Lopez & Associates*, 995 F.3d 295, 303 (2d Cir. 2021). PI Hearing Tr. at 17:3-22. But *McMorris*, while instructive, was concerned with a different question than the instant case. At issue in *McMorris* was whether the plaintiff could pursue a claim for monetary relief based upon a future risk of identity theft or fraud resulting from a data breach, where no such identity theft had yet occurred. *McMorris* sets forth a list of non-exhaustive factors to be used in assessing whether the risk of identity theft or fraud following the disclosure of an individual’s PII is sufficiently imminent to permit a damages suit to move forward. *McMorris*, 995 F.3d at 301-303. Yet the States are seeking injunctive relief to prevent the unauthorized disclosure of their information from occurring in the first instance. The question, then, is whether there is a realistic danger of future unauthorized disclosures of the States’ financial information. *Id.* The *McMorris* factors do not bear on this question. But what *McMorris* does tell us is that, in assessing substantial risk, there are no rigid prerequisites. As the Second Circuit reminds us, “determining standing is an inherently fact-specific inquiry that ‘requires careful judicial examination of a complaint’s allegations to ascertain whether the particular plaintiff is entitled to an

adjudication of the particular claims asserted.” *Id.* at 302 (citation omitted).

Applying that fact-specific test here, the Court holds that Plaintiffs have established the imminence of their future harm.

B. Causation and Redressability

“The second and third standing requirements—causation and redressability—are often ‘flip sides of the same coin.’” *FDA v. Alliance for Hippocratic Med.*, 602 U.S. 367, 380-81 (2024) (citing *Sprint Communications Co. v. APCC Services, Inc.*, 554 U.S. 269, 288 (2008)). “If a defendant’s action causes an injury, enjoining the action or awarding damages for the action will typically redress that injury.” *Id.*

Plaintiffs’ threatened injury is “fairly . . . traceable to the challenged action of the defendant, and not . . . the result of the independent action of some third party not before the court.” *Lujan*, 504 U.S. at 560 (cleaned up). The States have adequately shown that “but for” the Engagement Plan allowing undertrained DOGE Team members unusually broad access to sensitive Treasury data, including source code for all of the BFS payment systems, the States’ financial data would not be at a higher risk of being exposed, both within the federal government to potentially unauthorized individuals and outside the government. Indeed, that the Engagement Plan increased the security risk to the confidential data maintained on the BFS systems is undisputed.

Defendants argue, however, that any injury resulting from this heightened security risk are too speculative and attenuated to meet Article III’s standing requirements. ECF No. 35 (“Def. Opp. Br.”) at 15-16 (citing *Clapper*, 568 U.S. at

410-411). Yet the causal connection element of Article III standing “does not create an onerous standard. For example, it is a standard lower than that of proximate causation. *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 55 (2d Cir. 2016); *see also Gonzalez v. Costco Wholesale Corp.*, No. 16-CV-2590, 2018 WL 4783962, at *4 (E.D.N.Y. Sept. 29, 2018) (“The [traceability] requirement is meant to ensure that the injury was caused by the conduct complained of rather than by an independent action of some third party not before the court.”). Moreover, *Clapper* is inapposite. In *Clapper*, the Supreme Court held where the parties’ communications could be subject to lawful surveillance under a number of different legal authorities, the parties could not show that any surveillance of their communications was fairly traceable to the challenged statute. 568 U.S. at 412-13. In other words, there was a potentially intervening action that broke the chain of causation. No such break in the chain of causation exists here.

“[A] plaintiff satisfies the redressability requirement when he shows that a favorable decision will relieve a discrete injury to himself. He need not show that a favorable decision will relieve his *every* injury.” *Massachusetts v. EPA*, 549 U.S. 497, 525 (2007) (cleaned up). The States plausibly contend that granting the undertrained DOGE Team members access to the BFS payment systems poses a higher risk of exposing their confidential financial data. Compl., ¶¶ 10, 131, 139; ECF No. 4 (“Pls. Br.”) at 11-13. And the States warn that “expanded access . . . puts state’s [sic] finances at an increased risk of interference, fraud, and unauthorized access.” Pls. Br. at 12. Plainly, a preliminary injunction is capable of redressing this harm.

II. THE PRELIMINARY INJUNCTION MOTION

Injunctive relief “is an extraordinary and drastic remedy, one that should not be granted unless the movant, by a clear showing, carries the burden of persuasion.” *Sussman v. Crawford*, 488 F.3d 136, 139 (2d Cir. 2007) (per curiam) (cleaned up). Plaintiffs seeking a preliminary injunction must show that “(1) they are likely to succeed on the merits; (2) they are likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in their favor; and (4) an injunction is in the public interest.” *New York v. U.S. Dep’t of Educ.*, 477 F. Supp. 3d 279, 293 (S.D.N.Y. 2020). If the federal government is the opposing party, then the latter two factors merge. *Id.* at 294 (citing *Nken v. Holder*, 556 U.S. 418, 435 (2009)). Moreover, the establishment of irreparable harm is the “single most important prerequisite for the issuance of a preliminary injunction.” *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quotation marks and citations omitted).

A. Likelihood of Success on the Merits

In their Complaint, Plaintiffs assert claims under the APA, a common law claim that the Defendants have acted *ultra vires*, and constitutional claims that Defendants’ actions violate the separation of powers doctrine and the Take Care Clause of the United States Constitution. To obtain the extraordinary relief of a preliminary injunction, the States bear the burden of demonstrating that they will more likely than not prevail on at least one of these claims. “To establish a likelihood of success on the merits, a plaintiff need not show that success is an absolute certainty. It need only make a showing that the probability of . . .

prevailing is better than fifty percent.” *fuboTV Inc. v. Walt Disney Co.*, No. 24-CV-01363, 2024 WL 3842116, at *16 (S.D.N.Y. Aug. 16, 2024) (cleaned up).

1. Plaintiffs’ APA Claims

The APA establishes a “basic presumption of judicial review for one suffering legal wrong because of agency action.” *Dep’t of Homeland Sec. v. Regents of the Univ. of California*, 591 U.S. 1, 16-17 (2020) (cleaned up). The APA authorizes courts to set aside agency actions that are contrary to law, in excess of statutory authority, or arbitrary and capricious. 5 U.S.C. § 706(2). In Counts I and II of their Complaint, Plaintiffs assert that the United States Treasury acted contrary to law and in excess of its statutory authority “under the statutes that govern the collection, storage, handling, and disclosure of PII and confidential financial information.” Compl., ¶¶ 154-70. In Count III of the Complaint, Plaintiffs contend that the Treasury Department acted arbitrarily and capriciously by failing to adequately consider the numerous privacy and security problems associated with the Engagement Plan. The Court finds that Plaintiffs have not established a likelihood of success with respect to their statutory APA claims. Plaintiffs have, however, established that they more likely than not will prevail on their claim that the challenged agency action was arbitrary and capricious.

a. Zone of Interests Test

As a preliminary matter, in order to bring a statutory or constitutional claim, Plaintiffs must satisfy the zone of interests test. That is, they must demonstrate that the “interest sought to be protected by the complainant is arguably within the zone of interests to be protected or regulated by the statute or constitutional

guarantee in question.” *Bennett v. Spear*, 520 U.S. 154, 163 (1997) (quoting *Association of Data Processing Service Org., Inc. v. Camp*, 397 U.S. 150, 153 (1970)). The zone of interests test “denies a right of review if [the plaintiff’s] interests are so marginally related to or inconsistent with the purposes implicit in [the underlying statute] that it cannot reasonably be assumed that Congress intended to permit the suit.” *Clarke v. Securities Industry Assn.*, 479 U.S. 388, 399 (1987); *cf. Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 127 (2014) (“Whether a plaintiff comes within ‘the ‘zone of interests’ is an issue that requires us to determine, using traditional tools of statutory interpretation, whether a legislatively conferred cause of action encompasses a particular plaintiff’s claim.”).

In the APA context, “the interest the party asserts must be arguably within the zone of interests to be protected or regulated by the statute that he says was violated.” *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 567 U.S. 209, 224 (2012) (cleaned up). Plaintiffs argue that the Treasury Department violated the Privacy Act, 5 U.S.C. § 552a; the Tax Reform Act of 1976, 26 U.S.C. § 6103; Section 208 of the E-Government Act of 2002, 44 U.S.C. § 101 et seq.; provisions of the criminal code governing conflicts of interest in government employment, 8 U.S.C. § 208; and Treasury regulations governing the protection of SSNs, 31 C.F.R. § 1.32(d). On this record, it is unclear whether there have been violations of these provisions, in particular the Privacy Act, which circumscribes agency access to and permissible uses for sensitive confidential information pertaining to individuals, and section 6103 of the Internal Revenue Code and its implementing regulations, which similarly creates tight controls over the

dissemination of tax return information within the federal government. But ultimately the Court does not need to reach those merits questions, as the Court finds that these Plaintiffs are not the proper parties to litigate these issues.

“The relevant zone of interests for an APA claim is defined by ‘the statute that the plaintiff says was violated,’ rather than by the APA itself.” *Moya v. United States Dep’t of Homeland Sec.*, 975 F.3d 120, 131 (2d Cir. 2020) (citation omitted); see also *Haitian Refugee Ctr. v. Gracey*, 809 F.2d 794, 813 (D.C. Cir. 1987) (“[A] court must discern whether the interest asserted by a party *in the particular instance* is one intended by Congress to be protected or regulated by *the statute under which suit is brought*” (emphasis in original)). “In applying the zone of interests test, we do not ask whether, in enacting the statutory provision at issue, Congress specifically intended to benefit the plaintiff. Instead, we first discern the interests arguably to be protected by the statutory provision at issue; we then inquire whether the plaintiff’s interests affected by the agency action in question are among them.” *Nat’l Credit Union Admin. v. First Nat. Bank & Tr. Co.*, 522 U.S. 479, 492 (1998) (cleaned up). Although the zone of interests test “is not meant to be especially demanding,” *Clarke*, 479 U.S. at 399, “it is not toothless,” *Moya*, 975 F.3d at 132. Applying this standard, it is clear that all but one of Plaintiffs’ statutory APA claims are unlikely to succeed on the merits.

i. Privacy Act

The Court starts its analysis with the Privacy Act. “Congress enacted the Privacy Act to provide certain safeguards for an individual against an invasion of personal privacy, by requiring governmental agencies to maintain accurate records

and providing individuals with more control over the gathering, dissemination, and accuracy of agency information about themselves.” *Bechhoefer v. U.S. Dep’t of Just. D.E.A.*, 209 F.3d 57, 59 (2d Cir. 2000) (cleaned up). Subject to certain exceptions, the Privacy Act prohibits agencies from disclosing “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).

Plaintiffs do not contest that the Privacy Act only protects information regarding *individuals*, which the statute defines as “a citizen of the United States or an alien lawfully admitted for permanent residence.” 5 U.S.C.A. § 552a(a)(2). *See, e.g.*, PI Hearing Tr. at 31:9-18; Pls. Rep. Br. at 8. In other words, the States’ financial information is not protected by the Privacy Act, and any disclosure of State financial information by a federal agency would not violate the Privacy Act. The security of financial data belonging to states does not even arguably fall within the zone of interests that Congress intended to protect through the Privacy Act.

In arguing that they nonetheless fall within the zone of interests the Privacy Act seeks to protect, Plaintiffs point to the alleged disclosure of the PII and other confidential information of their resident citizens. The States argue that, because they were the “conduits” by which this PII was obtained by the Treasury Department—as the States upload the PII of its citizens to obtain Medicaid, Medicare, and other types of funding—they have an interest in protecting this information. PI Hearing Tr. at 28:17-29:14.

State residents are no doubt individuals whose information is protected by the Privacy Act from unlawful disclosure. But Plaintiffs did not claim to be advancing the interests of their residents when making their standing arguments. Nor could they, as the law is clear that a state cannot bring suit against the federal government to vindicate the rights of its citizens. *Haaland v. Brackeen*, 599 U.S. 255, 295 (2023) (“A State does not have standing as *parens patriae* to bring an action against the Federal Government.”).

Plaintiffs have premised their standing to pursue this action on their interest in the security of their *own* financial information. PI Hearing Tr. at 7:3-15; *id.* at 12:14-19. There is a clear disjunct between the harm alleged by the Plaintiffs—the disclosure of their own financial data—and the statutory violation that they assert under the Privacy Act. Although the zone of interests test is distinct from that of Article III standing, *Moya*, 975 F.3d at 133, the nature of the asserted injury in fact at the standing phase cannot be entirely divorced from “the plaintiff’s interests affected by the agency action.” *Nat’l Credit Union Admin.*, 522 U.S. at 492. The Court must compare Plaintiffs’ affected interests—which in this case is the protection of their own financial information from unauthorized disclosure—with the zone of interests that the Privacy Act seeks to protect. *Id.* To hold otherwise would allow Plaintiffs to perform a bait-and-switch, relying upon the harm to themselves to establish Article III standing, yet an entirely separate harm for purposes of the zone of interests inquiry. The zone of interests test does not permit this. *See Lujan v. Nat’l Wildlife Fed’n*, 497 U.S. 871, 883 (1990) (“[T]he plaintiff must establish that the injury he complains of (*his* aggrivement, or the adverse

effect *upon him*) falls within the ‘zone of interests’ sought to be protected by the statutory provision whose violation forms the legal basis for his complaint” (emphasis in original)); *Haitian Refugee Ctr.*, 809 F.2d at 812 (“[T]o satisfy the zone of interests requirement, appellants must establish that their particular interests alleged to have been injured by the interdiction program fall within the respective zones of interests intended to be protected or regulated [by the challenged statute].”).

It is plain that the States’ interest in the protection of its own financial data is not the type of interest the Privacy Act was enacted to protect. Accordingly, the claims based upon the Privacy Act are unlikely to succeed on the merits.

ii. Tax Reform Act and Treasury Regulations

Plaintiffs’ claims premised on section 6103 of the Internal Revenue Code and Treasury Regulation section 1.32(d) are unlikely to succeed for the same reason as their Privacy Act claim. The States’ interest in protecting their financial data from exposure does not fall within the zone of interest of either provision.

Section 6103 of the Internal Revenue Code protects tax returns and return information. 26 U.S.C. § 6103(a) (“Returns and return information shall be confidential, and except as authorized by this title[,] . . . no officer or employee of the United States . . . shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section.”). The disclosure requirements of section 6103 are stringent, elaborate, and comprehensive.

The legislative history of section 6103 indicates Congress's overriding purpose was to curtail loose disclosure practices by the IRS. Congress was concerned that IRS had become a 'lending library' to other government agencies of tax information filed with the IRS, and feared the public's confidence in the privacy of returns filed with IRS would suffer. . . . Congress also sought to end 'the highly publicized attempts to use the Internal Revenue Service for political purposes' involving delivery of tax returns to the White House by the IRS[.]

Stokwitz v. United States, 831 F.2d 893, 894 (9th Cir. 1987); *see also Church of Scientology of California v. I.R.S.*, 484 U.S. 9, 16 (1987) ("One of the major purposes in revising § 6103 was to tighten the restrictions on the use of return information by entities other than [the IRS]."). The statute therefore dictates the strict procedures that must be followed before tax return information can be disclosed to the President, 26 U.S.C. § 6103(g)(1), to officials within the Executive Office of the President, 26 U.S.C. § 6103(g)(2), or the head of a federal agency, *id.*

Return information is broadly defined to include

a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense.

Id. § 6103(b)(2). The States' confidential financial data in no way constitutes return information. There is no allegation that the States' financial data was provided to the IRS as part of a tax return, or in connection with the determination of any tax

liability. Accordingly, the harm asserted by the States bears no relation to section 6103's overriding concern with ensuring the privacy of tax returns.

Plaintiffs' reliance upon 31 C.F.R. § 1.32(d) is similarly misplaced. As pertinent here, this regulation requires the Treasury Department to take "feasible" steps to "mask, or truncate/partially redact Social Security numbers visible to authorized Treasury/component information technology users so they only see the portion (if any) of the Social Security number required to perform their official Treasury duties." The States do not have SSNs, so this regulation has no bearing on their claim for relief.

iii. The E-Government Act

The claim that Defendants failed to comply with the procedural requirements of Section 208 of the E-Government Act, which mandates agencies to conduct a privacy impact assessment ("PIA") before "developing or procuring technology that collects, maintains, or disseminates information that is in an identifiable form." Section 208(b)(1)(A)(i), Compl., ¶¶ 51, 164, fares no better. Plaintiffs maintain that the "work performed by the DOGE [T]eam using source code to create an automated process for flagging and pausing payment instructions in the 'landing zone' for further review by the submitting agency" triggered the Treasury's requirement to conduct a PIA prior to the execution of such work. Pls. Rep. Br. at 51. During oral argument, Plaintiffs further clarified that "[t]he creation in the sandbox of the automated process falls squarely within the [statute's] description of developing information technology." PI Hearing Tr. at 32:21-23.

As with the other statutes concerning the protection of PII, Plaintiffs do not fall within the zone of interests the E-Government Act was intended to protect. Section 208, entitled “Privacy Provision,” “by its very name, declares an express ‘purpose’ of ‘ensur[ing] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.” *Elec. Priv. Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity*, 878 F.3d 371, 378 (D.C. Cir. 2017) (quoting section 208(a)). Citing this language, the D.C. Circuit has explained that the E-Government Act is intended “to protect *individuals*—in the present context, voters—by requiring an agency to fully consider their privacy before collecting their personal information.” *Id.* at 378 (emphasis in original). The D.C. Circuit therefore rejected on standing grounds a claim by an organizational plaintiff. *Id.* As with the organization in *EPIC*, the States do not have the type of personal privacy interest that lies at the heart of the E-Government Act.

iv. Conflict of Interest Criminal Statutes

Plaintiffs also attempt to bring an APA claim on the grounds that Elez and Krause were acting in contravention of criminal statutes governing conflicts of interest in federal employment. Pls. Br. at 19. Plaintiffs cite 18 U.S.C. § 208(a), which prohibits officers or employees of the executive branch from participating in decision making on a matter in which they have a financial interest. Compl., ¶ 169. The parties disagree as to whether Plaintiffs have a sufficient personal interest to bring claims to enforce these criminal statutes through the APA. *See* Def. Opp. Br. at 32; Pls. Rep. Br. at 14.

The Court ultimately does not need to decide this question, however, because Plaintiffs have failed to meet their burden to show, as a factual matter, that this provision was more likely than not violated, or even implicated by the agency action in this case. Plaintiffs initially claimed that all members of the DOGE Team were hired as SGEs, and thus subject to section 208(a)'s requirements. Pls. Br. at 19-20. The record did not bear this out, as only Krause is an SGE. But in any event, this is a non-sequitor, as Treasury employees are subject to the provisions of section 208(a) whether they are SGEs or not. While section 208 does allow SGEs who serve on advisory committees to be exempted from the prohibitions contained in the statute if they, *inter alia*, obtain a certification "that the need for the individual's services outweighs the potential for a conflict of interest created by the financial interest involved," 18 U.S.C. § 208(b)(3), that provision is inapplicable here. Krause did not serve on an advisory committee; he was originally appointed as a consultant pursuant to 5 U.S.C. § 3109. Krause Decl., ¶ 1. And again, whether he was or was not exempted from the provisions of section 208(a) is irrelevant, as Plaintiffs have not shown that this statute was violated.

Plaintiffs argue that section 208(a) "does not authorize disclosure to an SGE without [a] certification, yet such disclosures have been made to DOGE team members." Pl. Br. at 20. But section 208(a) says nothing about who is or is not authorized to disclose or receive agency information. Accordingly, Plaintiffs cannot premise their request for injunctive relief on a purported violation of section 208(a).

b. Final Agency Action

To succeed on the merits of their remaining APA claim—that the challenged agency action was arbitrary and capricious—Plaintiffs bear the burden of establishing that there has been a “final agency action.” 5 U.S.C. § 704. For an agency action to be “final” under the APA, two requirements must be met. “First, the action must mark the consummation of the agency’s decisionmaking process 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) (cleaned up).

An agency’s decisionmaking process is considered consummated when its position is “definitive,” *Her Majesty the Queen in Right of Ontario v. U.S. E.P.A.*, 912 F.2d 1525, 1531 (D.C. Cir. 1990), not “merely tentative” or of an “interlocutory nature.” *Bennett*, 520 U.S. at 178. Defendants argue that Plaintiffs are unable to satisfy this aspect of the finality prong because they do not offer “written rules, orders, or even guidance documents that set forth the supposed prior access policy, or the challenged ‘change’ to that policy.” Def. Opp. Br. at 18. Precedent, however, is clear that the APA allows challenges to unwritten agency policies and practices where the requirements of finality are otherwise satisfied. Consummation simply means that the agency has reached a decision on the issue before it and effectuated it in some manner; it does not necessarily mean that the challenged agency action must have been reduced to a written statement. *See, e.g., Her Majesty the Queen*, 912 F.2d at 1531 (“[T]he absence of a formal statement of the agency’s position, as here, is not dispositive[.]”); *Amadei v. Nielsen*, 348 F. Supp. 3d 145, 165 (E.D.N.Y.

2018) (citing cases); *R.I.L.-R v. Johnson*, 80 F. Supp. 3d 164, 184 (D.D.C. 2015) (“Agency action . . . need not be in writing to be final and judicially reviewable.”). “The practical effect of the [agency’s] action, not the informal packaging in which it was presented, is the determining factor in evaluating whether the [agency’s] action was ‘final.’” *De La Mota v. U.S. Dep’t of Educ.*, No. 2-cv-4276 (LAP), 2003 WL 21919774, at *8 (S.D.N.Y. Aug. 12, 2003).

The agency action challenged by Plaintiffs is the decision by the Treasury Department to constitute a DOGE Team with individuals from outside the agency, who were employed pursuant to temporary hiring authorities, and provide those individuals with unprecedented access to the BFS payments systems pursuant to a four-to-six week Engagement Plan. Pls. Rep. Br. at 5-7; PI Hearing Tr. at 26:23-27:1 (“It was clearly the culmination of a decision-making process, which is the first requirement for determining whether something is a final agency action.”). That this agency action was “consummated” can hardly be gainsaid. Treasury not only decided to take these steps, it then in fact, by its own admission, implemented them. As set forth in the declarations submitted by the Treasury witnesses, “BFS initiated a 4-6 week payment process engagement plan,” where “[t]he objective of the engagement is to gain insight into the full, end-to-end payment process across multiple BFS payment systems, and to identify data gaps that, if resolved, would make the system to work more efficiently and securely.” Second Krause Decl., ¶ 13. The Treasury Secretary approved the engagement plan, and BFS and the DOGE Team even “implemented a number of mitigation measures . . . to protect sensitive

data and minimize the potential of disruptions to systems from the DOGE Team's work." *Id.* ¶ 15; *see also* Gioeli Decl., ¶¶ 12-13.

Defendants' primary argument is that "legal consequences" did not flow from this agency action. Def. Opp. Br. at 18-20. It is well settled that courts must apply a "pragmatic" approach to this prong of the *Bennett* test. *See, e.g., U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 599 (2016); *Salazar v. King*, 822 F.3d 61, 82 (2d Cir. 2016). "In characterizing the inquiry as pragmatic," courts are to focus 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).

Plaintiffs contend that the disclosure of their sensitive banking information, as well as the risk of additional disclosures, is an action from which rights are determined or legal consequences flow. Plaintiffs assert that the grant of access to the DOGE Team was itself unauthorized and ultra vires, and that any sharing of that information outside of the Treasury Department with USDS/DOGE further compounded their injury. Pls. Br. at 4-6; Pls. Rep. Br. at 11-16. The States further maintain that the expansion of access to the DOGE team members increases data security risk. Pls. Rep. Br. at 3-5 ("There can be no serious dispute that the DOGE team's prior and future access contemplated by the plan carries with it substantial risk that could cause future harm by compromising the States' financial information."). Defendants' own declarant admits the same. According to Gioeli, the "scope of work as envisioned in the engagement plan" necessitated a level of access that "presented risks, which included potential operational disruptions to Fiscal Service's payment systems, access to sensitive data elements, insider threat

risk, and other risks that are inherent to any user access to sensitive IT systems.” Gioeli Decl., ¶ 11. Acknowledging the risks of data disclosure, “BFS and Treasury Departmental Office employees developed mitigation strategies that sought to reduce these risks.” *Id.*

Indeed, a real possibility exists that sensitive information has already been shared outside of the Treasury Department, in potential violation of federal law. Although the Gioeli Declaration states that Elez had not used his BFS laptop to transmit BFS data outside of the U.S. Government, Gioeli Decl., ¶ 21, the declaration is “silent as to whether any such information was shared outside of Treasury.” Pls. Rep. Br. at 11. The careful wording of the Gioeli Declaration was no accident. At the preliminary injunction hearing, counsel for Defendants admitted that Elez did send emails outside of the Treasury Department, and that the agency does not know whether any of those emails contained protected PII or confidential bank information. PI Hearing Tr. at 15:18-23.

The disclosures of confidential information to the Treasury DOGE Team that have already taken place as part of the Engagement Plan, as well as the risk of future disclosures both to those in USDS/DOGE and outside the federal government, are sufficient to meet the second prong of the *Bennett* test. *See Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) (“Adopting a policy of permitting employees to disclose confidential information without notice is surely a ‘consummation of the agency’s decisionmaking process, and one by which [the submitter’s] rights [and the agency’s] obligations have been determined.’” (citation omitted)). Applying the pragmatic approach, the Court

therefore holds that Plaintiffs have sufficiently shown the concrete consequences that flow from the challenged agency action.

Defendants counter that, “to establish finality, Plaintiffs would need to show that their data has, in fact, been *improperly* disclosed (including to the Treasury DOGE Team)—not just that the Team had access to it.” Def. Opp. Br. at 20 (emphasis added). This argument conflates the final agency action prong with the ultimate merits inquiry, however. The D.C. Circuit’s decision in *Venetian Casino Resort* is particularly instructive on this point. In that case, the D.C. Circuit held that the agency’s adoption of a policy permitting employees to disclose confidential information in its possession without notice to the owner of the information was final agency action, because it was an action from which the rights of the owner of the information were determined. 530 F.3d at 931. This was so even though the Court ultimately concluded that the agency had not violated the law in making such disclosures. *Id.* at 934. Whether the disclosures were authorized by law was a separate inquiry that went to the merits of Plaintiffs’ APA claim, not to the question of final agency action. *Id.* at 931.

Defendants also rely on *Lujan v. Nat’l Wildlife Federation*, in which the Court rejected an APA challenge to the Bureau of Land Management’s land withdrawal review program. 497 U.S. 871, 890 (1990); PI Hearing Tr. at 43:14-16 (“[The Engagement Plan] is more akin to the broad programmatic attack in *Lujan*, but it just doesn’t fit within the definition of a final agency action.”). *Lujan*, however, is inapposite as the Court there specifically rejected the respondent’s sought-after “wholesale improvement of the program” instead of narrowing its challenge to an

“identifiable ‘agency action.’” 497 U.S. at 875. By failing to narrow the “land withdrawal review program” to “a single BLM order or regulation, or even to a completed universe of particular BLM orders and regulations,” the respondent could not identify a “concrete action that harms or threatens to harm the complainant.” *Id.* But the States have in fact narrowed their challenge to the Engagement Plan, as Defendants concede. PI Hearing Tr. at 46:8-9 (“[Plaintiffs] clearly stated [in their reply brief] that the final agency action is the engagement plan, and they have embraced that.”).

Accordingly, the Court finds that, under the pragmatic approach, legal consequences flow from the Engagement Plan’s effect of providing the “agreed-upon levels of access to BFS databases and source code.” Second Krause Decl., ¶ 16. The Engagement Plan is not an amorphous component of a large set of “continuing (and thus constantly changing) [agency] operations,” as was the case in *Lujan*. 497 U.S. at 875. The Engagement Plan was a concrete action that, according to Defendants’ own affidavits, had a clear objective and provided access to Treasury DOGE Team members. Second Krause Decl., ¶¶ 3, 12-14.

c. Plaintiffs’ Arbitrary and Capricious Claim

Having determined that there is final agency action, the Court now turns to the merits of Plaintiffs’ remaining APA claim. The APA authorizes courts to set aside agency action that is arbitrary or capricious. 5 U.S.C. § 706(2). In determining whether an action is arbitrary and capricious, courts “consider whether the decision was based on a consideration of the relevant factors and whether there has been a clear error of judgment.” *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State*

Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43 (1983). An agency practice is arbitrary and capricious “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.” *Id.* Agency actions can also be considered arbitrary and capricious if there is an “[u]nexplained inconsistency” in its policy, *Encino Motorcars, LLC v. Navarro*, 579 U.S. 211, 222 (2016); if the agency is found to have acted in bad faith, *Saget v. Trump*, 375 F. Supp. 3d 280, 354 (E.D.N.Y. 2019); or if an agency fails to provide a “reasoned explanation” for a change in policy, *New York v. United States Dep’t of Health & Hum. Servs.*, 414 F. Supp. 3d 475, 547 (S.D.N.Y. 2019). The arbitrary and capricious standard “is not limited to formal rules or official policies and applies equally to practices implied from agency conduct.” *Saget*, 375 F. Supp. 3d at 355. Although the reviewing court cannot “substitute its judgment for that of the agency,” its “inquiry . . . is to be searching and careful.” *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 416 (1971).

Additionally, a court may not set aside an agency action solely because it might have been influenced by political considerations or prompted by the priorities of a new Presidential administration. Agency policymaking is not a “rarified technocratic process, unaffected by political considerations or the presence of Presidential power.” *Dep’t of Com. v. New York*, 588 U.S. 752, 781 (2019). *But see Town of Orangetown v. Ruckelshaus*, 740 F.2d 185, 188 (2d Cir. 1984) (a claim of improper political influence on a federal administrative agency will lie if the

“political pressure was intended to and did cause the agency’s action to be influenced by factors not relevant under the controlling statute”).

Based upon the factual record developed to date, the Court finds that Plaintiffs will more likely than not succeed in establishing that the agency’s processes for permitting the Treasury DOGE Team access to critical BFS payment systems, with full knowledge of the serious risks that access entailed, was arbitrary and capricious. While it appears that the career staff at BFS did their best to develop what mitigation strategies they could, the inexplicable urgency and time constraints under which they operated all but ensured that the launch of the Treasury DOGE Team was chaotic and haphazard.

As an initial matter, everything about this process was rushed. The E.O. was signed on January 20, 2025. Elez was hired by the Treasury Department on January 21, and Krause was appointed on January 23. The record is silent as to what vetting or security clearance process they went through prior to their appointment.

Krause was first appointed under the authority of 5 U.S.C. § 3109, even though that hiring authority did not allow him to exercise the supervisory or policymaking authority that he clearly had. 5 C.F.R. § 304.103(b). Within a few weeks time, the Treasury Department then had to switch his appointment to a Temporary Transitional Schedule C employee. Elez was brought on board, then resigned a mere 16 days later. Gioeli Decl., ¶ 22.

The Treasury DOGE Team started its work almost immediately, even though it did not yet have either the HR specialist or the attorney that the E.O. mandated

should be members of the team. This left career staff with almost no time to develop their mitigation measures. Within days of his appointment, and apparently after receiving minimal, if any, training regarding the handling of sensitive government information (beyond being instructed to maintain the information on his BFS laptop), Elez was given full access to system source codes. *Id.* ¶ 4. Perhaps most troubling is that Elez was mistakenly given read/write access to SPS. *Id.* ¶ 20. Although this error was discovered the day Elez resigned, it speaks to the hurried nature of this process that it occurred at all.

Although the record indicates that Elez's access to BFS payment systems was at times closely monitored, at other points it appears that no one from BFS was contemporaneously aware of what he was doing. *Id.* ¶ 18. Even now, weeks after his departure, the Treasury Department is still reviewing his logs to determine what precisely he accessed and what he did with his access. *Id.* The Treasury Department also could not confirm whether or not Elez emailed PII or other confidential information to officials outside the Treasury Department. PI Hearing Tr. at 15:18-23.

It is also unclear from this record whether the agency established clear reporting lines for the Treasury DOGE Team. Although they are nominally agency employees who sit within the Treasury chain of command, it is notable that they also take instructions from officials at USDS/DOGE. How this works in practice, and the uncertainty this creates as to their status as Treasury employees, calls into question their authority to access Treasury record systems. Given the uniqueness

of the DOGE Team's almost hybrid status, a more considered process for bringing the DOGE Team on board might have helped clarify these issues.

When asked at the preliminary injunction hearing the reason for this accelerated process, counsel for the Government pointed to the urgency sparked by the President's Executive Orders. PI Hearing Tr. at 18:20-19:14. This explanation is riddled with inconsistencies. *Encino Motorcars*, 579 U.S. at 222 (inconsistencies and failure to offer a reasoned explanation for policy render agency action arbitrary and capricious). The E.O. did not demand that the Treasury DOGE Team begin its work immediately; indeed, the E.O. provided agencies with 30 days to constitute agency DOGE Teams. E.O. § 3(c). And to the extent it was suggested that the Treasury Department required the expertise of these two individuals, who had been employed at the Treasury Department for a matter of days and who had not yet been trained on the BFS payment systems, to implement the President's Executive Orders requiring pauses of certain categories of foreign assistance, the Court finds this explanation lacks credibility. In any event, any artificial sense of urgency engendered by the Government's imposition of time limits on itself would not justify the flawed process that occurred here.

The process by which the Treasury DOGE Team was appointed, brought on board, and provided with access to BFS payment systems could have been implemented in a measured, reasonable, and thoughtful way. To date, based on the record currently before the Court, it does not appear that this has been the case.

2. Plaintiffs' Constitutional and Common Law Claims

a. Separation of Powers Doctrine

As with their statutory APA claims, there is a disconnect between Plaintiffs' separation of power claim and the harm that Plaintiffs nominally seek to remedy through this suit. Plaintiffs' separation of powers claim is primarily premised on a concern that the Treasury Department DOGE Team has or will seek to block Congressionally-appropriated funding. Compl., ¶ 189; Pls. Br. at 23-24. Plaintiffs argue that "the application under the Engagement Plan of an ideological litmus test to flag and block legislatively appropriated and authorized federal funding is an unlawful usurpation of Congress's power of the purse in violation of the Separation of Powers doctrine." Pls. Rep. Br. at 16.

The zone of interests protected by the separation of power doctrine sweeps broadly and is not limited to the interests of the three branches of the federal government. *See, e.g., Bond v. United States*, 564 U.S. 211, 222 (2011) ("Separation-of-powers principles are intended, in part, to protect each branch of government from incursion by the others. Yet the dynamic between and among the branches is not the only object of the Constitution's concern. The structural principles secured by the separation of powers protect the individual as well."). "The declared purpose of separating and dividing the powers of government, of course, was to 'diffus[e] power the better to secure liberty.'" *Bowsher v. Synar*, 478 U.S. 714, 721 (1986) (quoting *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring)).

But Plaintiffs have repeatedly affirmed that they are not directly challenging any blocking of federal funding. For example, at the preliminary injunction hearing held in this matter, counsel for Plaintiffs stated:

[Interruption of state funding] is not part of our case, so it's really not relevant. Our case is not brought based on the states' funding having been blocked. That's not the basis for our injury in fact under Article III, and it's not the basis for why we are here. We are here because the states' bank information has been accessed. . . . There are other cases in other courts that are centered on funding being blocked. That's not this case.

PI Hearing Tr. at 12:14-24.

The structural and liberty interests at the heart of the separation of powers doctrine would appear, at best, tangential to Plaintiffs' asserted interest in the protection of its financial data. Plaintiffs argue that the reason their sensitive financial data has been compromised by the Treasury DOGE Team is to further Defendants' agenda to interrupt federal funding streams in violation of separation of powers. Compl., ¶ 189. This may bear on the causation prong of an Article III standing analysis, but it does not establish that the security of financial data falls within the interests that animate the separation of powers doctrine.

Accordingly, the Court finds that Plaintiffs' asserted interest in data security is too attenuated from the concerns of the separation of power doctrine, and thus they are unlikely to prevail on this claim.

b. Take Care Clause

The States also contend that the President, in "directing that the Agency Action be adopted and implemented," contravened the Take Care Clause of the

Constitution. Compl., ¶¶ 194-99. Although Plaintiffs do not specify, presumably this refers to the President's issuance of the E.O. Plaintiffs' Take Care Clause claim is without merit and thus does not provide a basis for granting injunctive relief.

Article II of the U.S. Constitution mandates the President to "take Care that the Laws be faithfully executed." U.S. Const., art. II § 3. Just as the Constitution prevents Congress from intruding on the President's power to execute the laws, the President — and his subordinates — do not wield "authority to set aside congressional legislation by executive order." *In re United Mine Workers of Am. Int'l Union*, 190 F.3d 545, 551 (D.C. Cir. 1999).

Neither set of parties devote more than a few sentences to the Take Care Clause claim. Our discussion will be similarly brief. Courts have expressed serious doubts as to the justiciability of Take Care Clause challenges. *See Citizens for Resp. & Ethics in Washington v. Trump*, 302 F. Supp. 3d 127, 139-40 (D.D.C. 2018); *see also Mississippi v. Johnson*, 71 U.S. 475, 499 (1866) (acknowledging "the general principles which forbid judicial interference with the exercise of Executive discretion"). Nevertheless, even when assuming that a Take Care Clause challenge of an Executive Order is justiciable, courts have required that plaintiffs either challenge the President's Executive Order directly or argue that the President has exceeded his authority in issuing the Order. *Citizens for Resp. & Ethics*, 302 F. Supp. at 140; *see also Am. Fed'n of Gov't Emps., AFL-CIO v. Trump*, 318 F. Supp. 3d 370, 439 (D.D.C. 2018) (declining to find a Take Care Clause violation due to lack of "some indication that the [Executive] Orders issued here exceed the statutory authority of the President in a manner that clearly implicates the constitutional

duties and prerogatives that [Plaintiff] says apply”), *rev’d and vacated on other grounds*, 929 F.3d 748 (D.C. Cir. 2019).

The States are unlikely to prevail on their Take Care Clause claim because they do not point to anything in the E.O. itself that exceeded the President’s statutory authority. Although the States’ reply brief maintains that the President cannot apply the Engagement Plan to “flag and block legislatively appropriated and authorized federal funding” in violation of his duties under the Take Care Clause, Pls. Rep. Br. at 16, the E.O. does not speak to the blocking of funding. As to information access, the E.O. states that “Agency Heads shall take all necessary steps, in coordination with the USDS Administrator *and to the maximum extent consistent with law*, to ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. USDS shall adhere to rigorous data protection standards.” E.O. § 4(b) (emphasis added). Plaintiffs do not point to any language in the E.O. that is in contravention of federal law. Nor do Plaintiffs explain how the President has acted “without authority to set aside congressional legislation” through issuing the E.O. itself. *In re United Mine Workers of Am. Int’l Union*, 190 F.3d at 551.

c. Ultra Vires

Plaintiffs’ ultra vires claim likewise can be disposed of easily. An ultra vires claim “is only available in the extremely limited circumstance when 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) (cleaned up). An ultra vires claim has been referred to as “essentially a Hail Mary pass,” *DCH Reg’l Med. Ctr. v. Azar*, 925 F.3d 503, 509 (D.C. Cir. 2019) (citation omitted), because of its “extraordinarily narrow” scope, *Hartz Mountain Corp. v. Dotson*, 727 F.2d 1308, 1312 (D.C. Cir. 1984).

Plaintiffs’ limited argument in support of its ultra vires claim is that, for the same reasons that the Engagement Plan violate the APA, they are also ultra vires. Pls. Br. at 22; Pls. Rep. Br. at 15-16. Yet just as Plaintiffs cannot rely upon the APA to press statutory claims because they do not fall within the zone of interests of the cited statutes, Plaintiffs cannot use the backdoor of an ultra vires claim to achieve the same end. *Haitian Refugee Ctr.*, 809 F.2d at 811 n.14 (for ultra vires claim, where litigant claims that a statute limited an agency’s authority, the litigant must be in the zone of interests that limitation was designed to protect).

In any event, Plaintiffs have not established that the Department of the Treasury acted contrary to a “specific prohibition” that is “clear and mandatory.” For example, while Plaintiffs allege that allowing Krause and Elez access to PII in the BFS payment systems violated the Privacy Act, the Privacy Act 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.” 5 U.S.C. § 552a(b)(1). Plaintiffs have offered no evidence that Krause and Elez were not employees of the Treasury Department at the time of the disclosures. And the language permitting employees to have access “in the performance of their duties”

does not so clearly prohibit the DOGE Team's access to these systems that it rises to the extraordinary level of an ultra vires violation.

B. Irreparable Harm

Although the States' irreparable harm arguments are closely tied to their injury points to establish standing, the Court shall separately address the question of irreparable harm required to obtain a preliminary injunction. "To satisfy the irreparable harm requirement, 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." *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 118 (2d Cir. 2009) (quoting *Grand River Enter. Six Nations, Ltd. v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007)). Although the "mere possibility of irreparable harm is insufficient," *Borey v. Nat'l Union Fire Ins. Co.*, 934 F.2d 30, 34 (2d Cir. 1991), Plaintiffs need only show that there is a "threat of irreparable harm, not that irreparable harm already [has] occurred," *Mullins v. City of New York*, 626 F.3d 47, 55 (2d Cir. 2010). Indeed, courts have recognized that increased "risk" of negative consequences is sufficient to meet the irreparable harm requirement for a preliminary injunction. *See, e.g., Mullins*, 626 F.3d at 55 (increased risk of deterrence from protecting employees' rights due to retaliation); *Holt v. Continental Group, Inc.*, 703 F.2d 87, 91 (2d Cir. 1983) (same); *Arias v. Decker*, 459 F. Supp. 3d 561, 571 (S.D.N.Y. 2020) (increased risk of severe infection in immigration detention).

Courts in the Second Circuit have repeatedly found that the future risks of disclosure of PII can amount to irreparable harm satisfying the injunctive relief standard, as long as the expectation of privacy is reasonable. For example, the Court in *Weisshaus v. Cuomo* denied a preliminary injunction to the plaintiff who could not demonstrate that his “expectation of privacy in [his] information . . . [was] [] one society is prepared to recognize as reasonable.” 512 F. Supp. 3d 379, 394 (E.D.N.Y. 2021). And, in *Trump v. Deutsche Bank AG*, the Second Circuit affirmed that there was irreparable harm where the plaintiffs had a reasonable interest in keeping their records private, and the defendants’ promises to keep the records confidential did not sufficiently protect such interest. 943 F.3d 627, 637 (2d Cir. 2019) (“plaintiffs have an interest in keeping their records private from everyone, including congresspersons”), *vacated on other grounds, Trump v. Mazars USA, LLP*, 591 U.S. 848 (2020).

Here, Plaintiffs sufficiently allege irreparable harm from the risk of “expanded access” to the BFS payment systems that will possibly compromise the systems to become “far more vulnerable to hacking or activities that render the information corrupted or compromised.” Pls. Br. at 13. The Court finds that there is a “substantial risk of future harm” where the data access protocols in place do not satisfactorily vet the employees with access and rigorously train them in data security measures. *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 414-15 (E.D. Va. 2020) (plaintiffs “plausibly alleged the continued inadequacy of [USAA’s] security measures” to show “they face a substantial risk of future harm if [the] security shortcomings are not redressed”); *see also Rand v.*

Travelers Indemnity Co., 637 F. Supp. 3d 55, 73 (S.D.N.Y. 2022) (plaintiff entitled to “injunctive relief in the form of requiring [defendant] to implement certain specific security protocols, including engaging third-party auditors to test its systems for weaknesses and regularly testing its systems for security vulnerabilities”).

Moreover, as the Court has already found that Plaintiffs have sufficiently alleged Article III standing, it is proper to find that Plaintiffs have sufficiently demonstrated irreparable harm absent a preliminary injunction. *See, e.g., New York v. U.S. Dep’t of Homeland Sec.*, 408 F. Supp. 3d 334, 350-51 (S.D.N.Y. 2019) (finding that plaintiff who demonstrated concrete and particularized injuries for standing had also shown irreparable harm); *Make the Road New York v. Cuccinelli*, 419 F. Supp. 3d 647, 665 (S.D.N.Y. 2019) (same).

C. Balance of the Equities and Public Interest

“In determining whether the balance of the equities tips in the plaintiff’s favor and whether granting the preliminary injunction would be in the public interest, the Court must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief, as well as the public consequences in employing the extraordinary remedy of injunction.” *Bionpharma Inc. v. CoreRx, Inc.*, 582 F. Supp. 3d 167, 178 (S.D.N.Y. 2022) (cleaned up).

Defendants’ interest in the modernization and increased efficiency in Treasury payment systems is not undercut by the relief the Court is Ordering. Indeed, taking the time to adequately mitigate potential security concerns and properly onboard members to engage in this work outweighs the Defendants’

immediate need to access and redevelop Treasury systems. Without addressing these issues, the potential consequences of a cybersecurity breach could be catastrophic.

It is undisputed that the BFS payment systems are critical to the financial infrastructure of the nation. Moreover, those systems contain sensitive PII and financial data regarding millions of American citizens. The public interest is plainly served by requiring the Treasury Department to ensure, to the maximum extent possible, the security of these systems and the information contained therein.

III. REMEDY

Having found that Plaintiffs have met the requirements for a preliminary injunction under Rule 65, the Court must now fashion appropriate relief. In doing so, the Court takes heed of the Second Circuit's admonishment that a preliminary injunction should be "narrowly tailored to fit specific legal violations." *Faiveley Transp. Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 119 (2d Cir. 2009) (citation omitted).

Plaintiffs' request for an injunction preventing the Treasury Department from developing automated and manual processes to halt payments coming through the BFS systems bears only an attenuated relation to Plaintiffs' injury. Plaintiffs argued at the preliminary injunction hearing that "if we restrain them from developing this automated process, that gives us some assurance that they won't be bringing in more DOGE team engineers or other engineers, or anybody who doesn't have the requisite training to access this information." PI Hearing Tr. at 62:10-14.

This argument does not withstand scrutiny. Plaintiffs' proposed injunction simultaneously sweeps too broadly and not broadly enough. It would not prevent, for example, the DOGE Team from accessing the BFS payments systems for any of their other stated goals, including modernizing the Treasury Department's technology systems to improve their capability for detecting fraud. Such an injunction does not remedy Plaintiffs' harm.

Additionally, as counsel for the Government pointed out at the preliminary injunction hearing, the language of the proposed injunction does not make clear to Defendants what actions they are prohibited from taking. *Id.* at 64:24-65:7. Plaintiffs request that Treasury employees "other than those employees with a need for access to perform their lawful job duties" be prohibited from accessing Treasury payment systems, but that begs the question of whether DOGE Team members are performing "lawful job duties." Clearly the Treasury Department contends that they are. This formulation, then, does not have the clarity required of an injunction.

In determining the appropriate scope of the injunction, the Court is mindful that the usual remedy in an APA case is to remand to the agency in order to provide it with an opportunity to cure the identified deficiency. Such a course is particularly appropriate where, as here, the issues identified by the Court largely have to do with the processes followed by the agency, and not with the substance of its decisions.

With these principles in mind, the Court hereby ORDERS as follows:

ORDERED that, pursuant to Rule 65 of the Federal Rules of Civil Procedure, the United States Department of the Treasury and the Secretary of the Treasury are restrained from granting access to any Treasury Department payment record, payment systems, or any other data systems maintained by the Treasury Department containing personally identifiable information and/or confidential financial information of payees to any employee, officer or contractor employed or affiliated with the United States DOGE Service, DOGE, or the DOGE Team established at the Treasury Department, pending further Order of this Court;

ORDERED that, by **Monday, March 24, 2025**, the United States Department of the Treasury shall submit a report to this Court: (i) certifying that the Treasury DOGE Team members have been provided with all training that is typically required of individuals granted access to BFS payment systems, including training regarding the federal laws, regulations, and policies governing the handling of personally identifiable information, tax return information, and sensitive financial data, and maintaining the integrity and security of Treasury data and technology, and attesting that any future Treasury DOGE Team member will be provided with this same training prior to being granted access to BFS systems; (ii) certifying the vetting and security clearances processes that members of the Treasury DOGE Team have undergone, and how that vetting process compares with the processes undergone by career employees who have previously been granted access to the BFS payment systems; (iii) describing the mitigation procedures that have been developed to minimize any threats resulting from increased access by members of the Treasury DOGE Team to BFS payment

systems; (iv) setting forth the legal authority pursuant to which each DOGE Team member was employed by or detailed to the Treasury Department; and (v) explaining the reporting chains that govern the relationship between the DOGE Team members, USDS/DOGE, and Treasury leadership (with reference, if applicable, to any Memorandum of Understanding setting forth that relationship).

Upon receipt of the above submissions from the Department of the Treasury, the Court will schedule prompt briefing to address whether the Treasury Department has adequately redressed the violations of the APA found herein, so as to justify the termination or modification of the preliminary injunction.

The Court hereby defers setting deadlines for the filing of a proposed case management plan or motions to amend the Complaint, and stays any deadlines for filing dispositive motions. The Court will take up such matters after determining whether, and if so to what extent, a preliminary injunction remains warranted after the Treasury Department's forthcoming submission.

CONCLUSION

For the foregoing reasons, Plaintiffs' motion for a preliminary injunction is GRANTED.

SO ORDERED.

Dated: February 21, 2025
New York, New York



JEANNETTE A. VARGAS
United States District Judge