UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JANE DOES 1-7, Plaintiffs, v. OFFICE OF PERSONNEL MANAGEMENT, Defendant.	*	Civil Action No. 1:25-cv-00234 (RDM)

PLAINTIFFS' RENEWED MOTION FOR A TEMPORARY RESTRAINING ORDER

NOW COME Plaintiffs Jane Does 1-7 to respectfully move this Court for a Temporary Restraining Order pursuant to Federal Rule of Civil Procedure 65(b) prohibiting Defendant Office of Personnel Management from continuing to operate the Government-Wide Email System ("GWES") and any system(s) connected to it prior to the completion and public release of a required legally sufficient Privacy Impact Assessment pursuant to the E-Government Act of 2002, 44 U.S.C. § 3501 note.

In support of this Motion, the Court is respectfully referred to Plaintiffs' Memorandum of Points and Authorities in Support of Their Renewed Motion for a Temporary Restraining Order.

A proposed Order consistent with the relief sought also accompanies this Motion.

Date: February 7, 2025

Respectfully submitted,

/s/ Kelly B. McClanahan
Kelly B. McClanahan, Esq.
D.C. Bar #984704
National Security Counselors
1451 Rockville Pike
Suite 250
Rockville, MD 20852
501-301-4672
240-681-2189 fax
Kel@NationalSecurityLaw.org

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JANE DOES 1-7, Plaintiffs, v. OFFICE OF PERSONNEL MANAGEMENT, Defendant.	*	Civil Action No. 1:25-cv-00234 (RDM)

PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF THEIR RENEWED MOTION FOR A TEMPORARY RESTRAINING ORDER

After Plaintiffs filed an emergency motion for a Temporary Restraining Order ("TRO") against Defendant Office of Personnel Management ("OPM") for failing to publish a required Privacy Impact Assessment ("PIA") for what came to be known as the Government-Wide Email System ("GWES"), OPM conducted and published a document at the last minute which, while purporting to be a PIA for that system, was both factually inaccurate and legally insufficient. OPM entitled this document *Privacy Impact Assessment for Government-Wide Email System (GWES)* ("GWES PIA")[1] and published it for pretextual reasons for the purpose of misleading this Court and arguing that its publication renders the case moot, just as the Government rescinded an Office of Management and Budget ("OMB") memo for similarly pretextual reasons in *National Council of Nonprofits v. OMB*, No. 25-239, 2025 WL 368852, at *7 (D.D.C. Feb. 3, 2025) ("[I]t appears that OMB sought to overcome a judicially imposed obstacle without actually ceasing the challenged conduct. The court can think of few things more disingenuous."). This

[1] Plaintiffs refer to this document as a PIA simply for convenience. They do not concede that this document is in any way a legitimate PIA as required by law.

Court should soundly reject the GWES PIA and enter a TRO in this matter to mitigate the ongoing and irreparable harm presented by the continued operation of these systems without a legally sufficient PIA.[2]

OPM was shown ten years ago to be wholly unprepared to safeguard the PII of federal Government personnel—including contractors and applicants—when news broke that 22 million records, including five million digitized fingerprints and sensitive background records, were stolen from the OPM security clearance database. Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, Wash. Post (July 9, 2015), *available at* https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ (last accessed Feb. 2, 2025). Federal agencies are, understandably, required to take steps to safeguard personal information before collecting new data. In response to this unprecedented breach, the U.S. Government conducted a searching review to determine how the breach had occurred and prevent future breaches, concluding, "Attackers were able to access OPM systems due to poor security protocols. OPM lacked an effective managerial structure to implement reliable IT security policies and didn't comply with the agency's IT security program." Nat'l Counterintelligence & Security Center, *Cyber Aware Case Study: Office of Personnel Management* 2, *at* https://www.dni.gov/ncsc/e-Learning_CyberAware/pdf/Cyber_Aware_CaseStudy_OPM.pdf (last accessed Feb. 2, 2025) [hereinafter *OPM Case Study*]. OPM in particular took significant steps to improve its cybersecurity posture, *see* OPM, *Cybersecurity Resource Center Frequently Asked Questions* (June 1, 2016), *at* https://www.opm.gov/cybersecurity-resource-center/fact-

[2] While Plaintiffs do request an order directing OPM to delete all Personally Identifiable Information ("PII") from the GWES and all systems which are connected to it (1st Am. Compl., Dkt. #14, ¶ 61 (filed Feb. 7, 2025)), they are not seeking that relief in this Motion.

sheet.pdf (last accessed Feb. 2, 2025), and is continuing to do so, *see*, *e.g.*, OPM, *Information Technology Strategic Plan: Fiscal Years 2023-2026* 23 (June 1, 2023), *at* https://www.opm.gov/about-us/reports-publications/2023-2026-information-technology-strategic-plan.pdf (last accessed Feb. 2, 2025) (describing cybersecurity improvement plans).

Despite all of these curative measures, the evidence suggests that, at some point after 20 January 2025, OPM allowed unknown individuals to simply bypass its existing systems and security protocols and install one or more new systems to ingest and store vast quantities of PII about Executive Branch employees (as well as an unknown number of contractors and employees of other branches) for the stated purpose of being able to communicate directly with those individuals without involving other agencies. In short, the sole purpose of these new systems was *expediency*.

In installing these systems, OPM ignored entirely the rules Congress established in the E-Government Act of 2002 which would safeguard the personal data being transferred into and stored by these systems. In utilizing these systems to send numerous email messages to individuals across the Executive Branch and beyond, and then insisting that Executive Branch employees must *reply by email to the same systems*, OPM further exacerbated the situation. OPM was required to prepare and publish a Privacy Impact Assessment ("PIA") which would have addressed the types of information to be collected and maintained and the purpose of the collection, as well as, most relevantly to this case, how the information would be secured and whether it would be disclosed to others.

Instead, OPM prepared and published a document practically overnight which does not come close to satisfying the legal requirements for a PIA. (*Privacy Impact Assessment for Government-Wide Email System (GWES)*, Dkt. #11-1 (filed Feb. 5, 2025) [hereinafter GWES

PIA]. This purported PIA, listing as the Point of Contact a person who was a senior official in a private company *three weeks ago*, was approved by a purported Chief Information Officer ("CIO") who was also a senior official in a private company even more recently. (1st Am. Compl. ¶¶ 37-41.) This purported PIA, unlike every other PIA issued by OPM, *see* OPM, *Privacy Impact Assessment Summaries*, *at* https://www.opm.gov/information-management/privacy-policy/#url=PIAs (last accessed Feb. 7, 2025), was approved by the CIO instead of the Chief Privacy Officer Kirsten Moncada, who is OPM's Senior Agency Official for Privacy pursuant to Executive Order 13,719. *See* Fed. Priv. Council, *Council Members*, at https://www.fpc.gov/council-members/ (last accessed Feb. 7, 2025).

In addition to being approved by an official in a stark divergence from standard OPM practice who appears from the available evidence to be a Special Government Employee and may not be legally authorized to serve as CIO, this purported PIA falsely claims that the system "collects, maintains, and disseminates only the information of federal government employees" (GWES PIA at 1), despite the clear evidence that it also contains PII regarding various types of individuals who use email addresses assigned by the Executive Branch ending in .gov or .mil yet are not Executive Branch employees, including contractors, partners, and employees of the Legislative and Judicial Branches.

Most troubling, though, is the fact that this purported PII satisfies virtually none of the legal requirements for a PIA set forth by the E-Government Act of 2002 or the implementing regulations, and yet the Government filed it with this Court to support a claim of mootness. These authorities may not be verbose in their PIA provisions, but neither are they toothless, and no reasonable agency would expect this document to be accepted as a legally sufficient PIA.

Plaintiffs—including putative class members—and even individuals outside the Executive Branch face immediate, ongoing, and irreparable injury as a result of these violations of law. Plaintiffs accordingly ask this Court to enter a TRO prohibiting OPM from continuing to operate the GWES and any system(s) connected to it prior to the completion and public release of a required legally sufficient PIA pursuant to the E-Government Act of 2002, 44 U.S.C. § 3501 note.

FACTUAL BACKGROUND

Despite the fact that the legal questions at issue in this Motion are generally fairly simple and straightforward, they cannot be easily analyzed without first discussing the rapidly evolving factual developments which led up to this case and this request for such extraordinary relief. While Plaintiffs apologize in advance for the lengthy recitation of the factual background (much of which is drawn from the First Amended Complaint), they trust the Court will understand its relevance in the context of this Motion.

The 2015 Breach and Subsequent Security Enhancements

1. Between July 2012 and April 2014, hackers presumed to be affiliated with the People's Republic of China began probing and exfiltrating data from OPM's network. House Comm. on Oversight and Gov't Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation (Maj. Staff Rep.)* 5-6 (Sept. 7, 2016), *available at* https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf (last accessed Feb. 3, 2025) [hereinafter *House OPM Rep.*]

2. On 7 May 2014, a hacker established a foothold into OPM's network by "pos[ing] as a background investigations contractor employee (KeyPoint), us[ing] an OPM credential,

remotely access[ing] OPM's network, and install[ing] PlugX malware to create a backdoor." *Id.* at 6

3. Between May 2014 and April 2015, hackers continued to infiltrate OPM's network and eventually exfiltrated approximately 22 million background investigation records from OPM's systems. *Id.* at 6-11.

4. In the House investigation which followed, it was revealed that a key part of the attack was due to a domain—opmsecurity.org—which "was purposely named to emulate a legitimate looking website." *Id.* at 15.

5. One of the key findings of the House investigation was, "There is a pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications." *Id.* at 19.

6. Another key focus of the House investigation was the importance of the Office of the Chief Information Officer ("OCIO") and the breakdown in communications between that office and the Office of the Inspector General ("OIG"). *Id.* at 173-93. The report concluded this examination: "The future effectiveness of the agency's information technology and security efforts will depend on a strong relationship between these two entities moving forward." *Id.* at 193.

7. In response to the 2015 attack, OPM took immediate steps to improve its cybersecurity posture:

- Completing deployment of two-factor Strong Authentication for all users, which provides a strong barrier to OPM's networks from individuals that should not have access;
- Implementing a continuous monitoring program for all IT systems;
- Creating and hiring a cybersecurity advisor position that reports to the Director;
- Establishing an agency-wide centralized IT security workforce under a newly hired Chief Information Security Officer (CISO);

- Modifying the OPM network to limit remote access to exclusively government-owned computers;
- Deploying new cybersecurity tools, including software that prevents malicious programs and viruses on [its] networks;
- Implementing a Data Loss Prevention System which automatically stops sensitive information such as social security numbers from leaving the network unless authorized; and
- Enhancing cybersecurity awareness training with emphasis on Phishing emails and other user based social engineering attacks.

Id. at 225.

8. Over the next decade, OPM continued to take steps to ensure the security of the information stored in its systems. Most recently, OPM awarded a five-year contract to Bering Straits Professional Services "to support the human resources agency's IT modernization efforts." Wesley Hansen, *OPM Awards $149M ECIOSS Contract for IT Modernization*, MeriTalk.com (Jan. 10, 2025). This Enterprise Cyber, Infrastructure, and Network Operations Support Services contract "aims to serve as the agency's central hub for 24/7 monitoring and analysis, cyber threat intelligence, incident response, network and server performance, patching, and upgrades across OPM's enterprise IT systems."

9. On 14 January 2025, OPM promoted Melvin Brown II ("Brown") to CIO, stating that he "has been an integral leader in delivering many of OPM's accomplishments in modernizing IT." Madison Alder, *Melvin Brown II takes over as OPM's chief information officer* FedScoop (Jan. 14, 2025), *at* https://fedscoop.com/melvin-brown-named-opm-chief-information-officer/ (last accessed Feb. 3, 2025). According to an OPM spokesperson, OPM's progress in this field "includes the agency achieving an 'A' score on its Federal Information Technology Acquisition Reform Act, or FITARA, scorecard, which tracks agency progress in multiple IT areas." *Id.*

OPM Installs and Uses New IT Equipment

10. On 27 January 2025, an unknown "OPM employee for nearly a decade and a Federal Employee for almost 20 years" posted a message to the r/FedNews discussion board on https://Reddit.com ("FedNews Message"). Some of the contents of this message have been independently verified, while other parts can only be sourced to the message itself. The original message was deleted, but a screenshot was reposted to the same discussion board that same day. *See* "This was posted about OPM in our Union chat" (Jan. 27, 2025), *at* https://www.reddit.com/r/fednews/comments/1ibbbh7/this_was_posted_about_opm_in_our_union_chat/ (last accessed Feb. 3, 2025) [hereinafter FedNews Message].

11. According to the FedNews Message, "Our CIO, Melvin Brown, . . . was pushed aside just one week into his tenure because he refused to setup email lists to send out direct communications to all career civil servants. Such communications are normally left up to each agency." FedNews Message.

12. It is uncontroverted that, on 22 January 2025, OPM replaced Brown as CIO. Madison Alder, *Melvin Brown II swapped out as OPM's chief information officer* FedScoop (Jan. 22, 2025), *at* https://fedscoop.com/melvin-brown-ii-swapped-out-opm-chief-information-officer/ (last accessed Feb. 3, 2025).

13. Furthermore, prior to 20 January 2025, OPM lacked the technical capacity to send direct communications to all Executive Branch employees:

> But just days before President Donald Trump's inauguration, OPM did not have the capability to send a mass email of that scale, according to a person familiar with the matter. To send mass emails, the agency had used govDelivery, a cloud communications service provided by public sector IT company Granicus, a different person familiar said.
>
> The govDelivery contract had restrictions on the volume of emails available to send without incurring added costs, and the agency would not have been able to reach

> 2.3 million people, the approximate number of all civilian federal employees, the second person added.

David DiMolfetta, *OPM's new email system sparks questions about cyber compliance* Nextgov/FCW (Jan. 28, 2025), *available at* https://www.nextgov.com/digital-government/2025/01/opms-new-email-system-sparks-questions-about-cyber-compliance/402555/ (last accessed Feb. 3, 2025).

14. Additionally, OPM has used Microsoft Office 365 since at least 2021, including Outlook 365 for email. OPM, *Privacy Impact Assessment for OPM – Microsoft Office 365* (May 13, 2021), *available at* https://www.opm.gov/information-management/privacy-policy/privacy-policy/office-365-pia.pdf (last accessed Feb. 3, 2025) [hereinafter Office 365 PIA]. Outlook 365 cannot send more than ten thousand emails per day. *See* Microsoft, *Exchange Online limits* (Dec. 11, 2024), *at* https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1 (last accessed Feb. 3, 2025).

15. According to the FedNews Message, "Instead [of using the normal channels], an on-prem (on-site) email server was setup [sic]. Someone literally walked into our building and plugged in an email server to our network to make it appear that emails were coming from OPM. It's been the one sending those various 'test' message[s] [discussed below]." FedNews Message.

16. This statement is supported by recent reporting:

> A new server being used to control these [OPM] databases has been placed in a conference room that Musk's team is using as their command center, according to an OPM staffer. The staffer described the server as a piece of commercial hardware they believed was not obtained through the proper federal procurement process.

Caleb Ecarma & Judd Legum, *Musk associates given unfettered access to private data of government employees* Musk Watch (Feb. 3, 2025), *at* https://www.muskwatch.com/p/musk-associates-given-unfettered (last accessed Feb. 3, 2025).

17. On 23 January 2025, OPM published an official statement: "OPM is testing a new capability allowing it to send important communications to ALL civilian federal employees from a single email address. Testing of this messaging system functionality is expected as soon as this week." OPM, *Federal Government-Wide Email Communication Test* (Jan. 23, 2025), *at* https://www.opm.gov/statements/federal-government-wide-email-communication-test-coming/ (last accessed Feb. 3, 2025).

18. On 24 January 2025, Executive Branch personnel across the Government—as well as many contractors and Judicial Branch personnel—received an email from HR@opm.gov stating: "This is a test of a new distribution and response list. Please reply 'YES' to this message." The email included a hyperlink to the 23 January OPM announcement. *See* Billy Mitchell, *Lawsuit claims systems behind OPM governmentwide email blast are illegal, insecure* FedScoop (Jan. 28, 2025), *at* https://fedscoop.com/opm-email-federal-workforce-lawsuit-server-privacy-security/ (last accessed Feb. 3, 2025).

19. On 26 January 2025, Executive Branch personnel across the Government—as well as many contractors and Judicial Branch personnel—received an email from HR@opm.gov stating:

> This is the second test of a new email distribution and response list. The goal of these tests is to confirm that an email can be sent and replied to by all government employees.
>
> Please reply "Yes" to this email, regardless of whether you replied to the first test email.
>
> If you responded "Yes" to the first email: thank you. As a reminder, always check the From address to confirm that an email is from a legitimate government account and be careful about clicking on links, even when the email originates from the government.

Allison Gill, *ATTN: Federal Workers Who Replied to HR@opm.gov* The Breakdown (Jan. 28, 2025), *at* https://www.muellershewrote.com/p/attn-federal-workers-who-replied (last accessed Feb. 3, 2025).

20. On 28 January 2025, Executive Branch personnel across the Government—as well as many contractors—received an email from HR@opm.gov with the subject line "Fork in the Road," which described a "deferred resignation program." This email concluded:

> Upon review of the below deferred resignation letter, if you wish to resign:
>
> 1) Select "Reply" to this email. You must replay from your government account. A reply from an account other than your .gov or .mil account will not be accepted.
>
> 2) Type the word **"Resign"** into the body of this reply email. Hit "Send".
>
> **THE LAST DAY TO ACCEPT THE DEFFERED RESIGNATION PROGRAM IS FEBRUARY 6, 2025.**

OPM, *Fork in the Road* (Jan. 28, 2025), *at* https://www.opm.gov/fork (last accessed Feb. 3, 2025).

21. On 30 January 2025, Executive Branch personnel across the Government received an email from HR@opm.gov with the subject line "Fork in the Road FAQs," which concluded, "Reminder that the deferred resignation program is available until **Thursday, February 6**." Andrea Swalec, *Trump administration email urges federal workers to take 'higher productivity' jobs* NBC4 Washington (Jan. 31, 2025), *at* https://www.nbcwashington.com/news/local/trump-administration-email-urges-federal-workers-to-take-higher-productivity-jobs/3832294/ (last accessed Feb. 3, 2025).

22. On 2 February 2025, Executive Branch personnel across the Government received an email from HR@opm.gov with the subject line "Fork in the Road: Today's FAQs," which concluded, "Reminder that the deferred resignation program is available until **Thursday,**

February 6." Will Steakin & Laura Romero, *OPM, implementing Musk's DOGE plans, sends federal workers 2nd 'Fork in the Road' email* ABC News (Feb. 3, 2025), *at* https://abcnews.go.com/US/opm-implementing-musks-doge-plans-sends-federal-workers/story?id=118401375 (last accessed Feb. 3, 2025).

23. Evidence suggests that all of the aforementioned emails were sent from the GWES and other systems which were added to OPM's networks for this purpose, and to which the PII of Executive Branch employees across the Government—as well as many contractors and Legislative and Judicial Branch employees—was imported.

OPM Publishes a Legally Insufficient PIA

24. On 5 February, in response to Plaintiffs' first motion for a TRO, OPM issued the GWES PIA.

25. The GWES PIA identified Riccardo Biasini ("Biasini"), Senior Advisor to the Director, as the Contact Point, and Greg Hogan ("Hogan"), Chief Information Officer, as the Reviewing Official. (GWES PIA at Cover.)

26. Neither Biasini nor Hogan were OPM employees prior to 20 January. Prior to 20 January, Biasini was Director of Electrical and Software Engineering at the Boring Company, a company owned by Elon Musk. Prior to 20 January, Hogan was a Cloud/Infrastructure/Platform Engineer at Comma.ai, a company that develops code for self-driving car companies, including Tesla. OPM has refused to confirm or deny that they are Special Government Employees ("SGE"), and OPM's counsel admitted during the 6 February hearing in this case that SGEs had been involved in the development and administration of the GWES.

27. The GWES PIA falsely claims that the system "collects, maintains, and disseminates only the information of federal government employees" (GWES PIA at 1), despite

the clear evidence that it also contains PII regarding various types of individuals who use email addresses assigned by the Executive Branch ending in .gov or .mil yet are not Executive Branch employees, including contractors, partners, and employees of the Legislative and Judicial Branches.

ARGUMENT

This case presents the type of extraordinary circumstance that justifies a temporary restraining order. Absent a prohibition from this Court, OPM will continue to operate computer systems containing vast quantities of PII which are more susceptible to cyberattacks than the pre-existing OPM systems.

First and foremost, this proposed collection violates a core provision of the E-Government Act of 2002, which requires that agencies establish sufficient protections *prior* to initiating any new collection or storage of personal information using information technology. Second, this collection and aggregation of sensitive personal information, as well as the exposure of this data through insecure systems with no protections in place, will cause irreparable harm to Plaintiffs and all similarly situated individuals. Once data has been leaked, there is no way to control its spread. With a data breach, there is literally no way to repair the damage, once done. Third, the balance of the equities tips in Plaintiffs' favor because OPM will suffer no hardship if the operation of these systems is enjoined pending the completion of a privacy assessment as required under federal law, because, by the time this Court adjudicates this Motion, the 10 February 2025 modified deadline for responding to the Government's "deferred resignation program" will either be stayed or in the past, and there will be no cognizable Government interest in maintaining the GWES simply to avoid having to send email messages through the existing framework. Indeed, it is in the public interest to prevent a reoccurrence of the 2015

OPM breach. The safety and security of the personal information about every individual with a Government email address is of paramount importance and should not be put at risk at the whim of OPM's new leadership.

I. STANDARD OF REVIEW

In order to obtain a TRO, a plaintiff 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) that the balance of the equities tips in their favor, and (4) that an injunction is in the public interest. *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. NRDC*, 555 U.S. 7, 20 (2008)). TROs are extraordinary remedies that "should be granted only when the party seeking relief, by a clear showing, carries the burden of persuasion." *Lofton v. District of Columbia*, 7 F. Supp. 3d 117, 120 (D.D.C. 2013). The D.C. Circuit has adopted a "sliding scale" approach when evaluating these injunction factors. *Sherley*, 644 F.3d at 392. Thus if the "movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make a strong showing on another factor." *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291–92 (D.C. Cir. 2009). *But see League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 7 (D.C. Cir. 2016) (noting that the court has "not yet decided" whether the sliding scale approach applies post-*Winter*).

II. PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS

Under the E-Government Act of 2002, any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" is required to complete a PIA before initiating such collection. 44 U.S.C. § 3501 note § 208(b)(1)(A)(ii). The agency must:

> (i) [C]onduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

Id. § 208(b)(1)(B).

However, the statute and its implementing regulations does not allow an agency to conduct just *any* PIA. A PIA must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information." *Id.* § 208(b)(2)(B)(i). OMB is charged with "oversee[ing] the implementation of the privacy impact assessment process throughout the Government" and "develop[ing] policies and guidelines for agencies on the conduct of privacy impact assessments." *Id.* § 208(b)(3).

OMB regulations, for their part, require: "Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle." OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* app. II at 10 (2016). OMB instructs that "PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA." OMB, *M-03-22: Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, att. A § II.C.1.b (Sept. 26, 2003), *available at* https://www.justice.gov/opcl/page/file/1131721/dl?inline (last accessed Feb. 7, 2025) [hereinafter Bolten Memo]. OMB also requires PIAs concerning "major information systems" to "reflect more extensive analyses of:

1. the consequences of collection and flow of information;

2. the alternatives to collection and handling as designed;
3. the appropriate measures to mitigate risks identified for each alternative; and
the rationale for the final design choice or business process.

Id. § II.C.2.a.ii.

OPM has not conducted a legally sufficient PIA for the new systems installed since 20 January for the purposes of communicating with and aggregating data about all Executive Branch personnel. OPM has not ensured review of a legally sufficient PIA by any legitimate CIO or equivalent official. OPM has not made such a legally sufficient PIA available to the public. OPM's actions therefore violate the Administrative Procedures Act ("APA"), 5 U.S.C. § 706(2)(A). Plaintiffs are likely to succeed on their statutory claim.

As the Department of Justice has explained, "Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form." DOJ Office of Privacy & Civil Liberties, *E-Government Act of 2002* (June 18, 2014), *available at* https://www.justice.gov/opcl/e-government-act-2002 (last accessed Feb. 4, 2025). A PIA is "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." Bolten Memo § II(A)(f).

The E-Government Act requires that an agency "shall take actions described under subparagraph (B)" of Section 208 "before . . . initiating a new collection of information that—(I)

will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government." 44 U.S.C. § 3501 note § 208(b)(1)(A)(ii). The actions described in subparagraph (B), which OPM must take *before* collecting or aggregating this information, include "(i) conduct[ing] a privacy assessment; (ii) ensur[ing] the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), mak[ing] the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." 44 U.S.C. § 3501 note § 208(b)(1)(B).

OPM has already "initiated a new collection" of personal information, but it has not complied with any of these requirements. The APA prohibits federal agencies from taking any action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). OPM's actions are "not in accordance with law." The APA authorizes this Court to "compel agency action unlawfully withheld." 5 U.S.C. § 706(1). Such a claim may proceed "where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required to take*." *Norton v. S. Utah Wildlife Alliance*, 542 U.S. 55, 64 (2004). An agency's failure to comply with the PIA requirements of the E-Government Act is reviewable under both provisions of APA § 706. *Fanin v. Dep't of Veteran Affairs*, 572 F.3d 868, 875 (11th Cir. 2009).

The E-Government Act defines "information technology" as "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or

reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . .” 40 U.S.C. § 11101(6); *see* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 U.S.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). Courts have found that a “minor change” to “a system or collection” that does not “create new privacy risks,” such as the purchasing of a new external hard drive, would not require a PIA. *Perkins v. Dep’t of Veterans Affairs*, No. 07-310, 2010 U.S. Dist. LEXIS 162409, at *19-20 (N.D. Ala. Apr. 21, 2010) (quoting Bolten Memo § II.B.3.f). However, as noted in the Factual Background section above, the changes that OPM made to its existing systems were far from minor and created significant new privacy risks.

There is no question that the PIA requirement applies in this case. OPM’s decision to initiate collection and aggregation of PII belonging to over two million Executive Branch employees triggers the obligations of § 208(b)(1)(A)(ii) of the E-Government Act. The “test” emails requesting that every employee respond by email to HR@opm.gov and the “Fork in the Road” emails telling everyone who wished to enter the deferred resignation program that they must send their responses by email to HR@opm.gov are just the types of correspondence the E-Government Act contemplated. This personnel data is precisely the type of “personal information” in “identifiable form” that the PIA provision was intended to protect, and the response via email clearly involves the use of information technology.

As the court explained in *Perkins*, PIAs are necessary to address “(1) what information is collected and why, (2) the agency’s intended use of the information, (3) with whom the information would be shared, (4) what opportunities the [individuals] would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created.” *Id. See* 44 U.S.C. § 3501 note §

208(b)(2)(B); Bolten Memo § II.C.1.a. These types of inquiries are "certainly appropriate and required" when an agency "initially created" a new database system and "began collecting data." *Perkins*, 2010 U.S. Dist. LEXIS at *19-20.

The APA defines "agency" as "each authority of the Government of the United States, whether or not it is within or subject to review by another agency," but excludes from the definition eight specific types of entities not relevant to this case. 5 U.S.C. § 701(b). The E-Government definition provided in 44 U.S.C. § 3502 is even broader than the APA definition and includes "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include (A) the Government Accountability Office; (B) Federal Election Commission; (C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities." Under both definitions, OPM is an "agency" and was therefore required to conduct a PIA prior to initiating the operation of these systems and the ingestion of unknown amounts of PII by them to make it "easier" to communicate with the federal workforce.

Moreover, allowing an agency to conduct and publish a patently inaccurate and legally insufficient PIA would lie in stark contrast to the requirements of the law. In addition to the inaccuracy noted above, the following is a sample of the types of nonsensical statements in the GWES PIA which fall far short of the legal standard:

- "The Office 365 mailbox has been granted an Authorization to Operate (ATO) that includes a system security plan." (GWES PIA at 3) – According to the Office 365 PIA, the relevant ATO appears to have expired in 2023. Office 365 PIA at 5.
- "Many of the names and email addresses of federal government employees are publicly available." (GWES PIA at 5) – This statement both fails to respond to the question regarding "us[ing] information from commercial sources or publicly available data" and raises significant questions regarding OPM's apparent perception that Government email addresses are not PII.
    - "GWES programmatically evaluates responses to verify the quality of the system and the substance of the Employee Response Data." (*Id.* at 6.) – A statement that a system "programmatically evaluates" data falls far short of the requirement that a PIA must describe how the data is being detected. *See*, *e.g.*, Office 365 PIA at 8 ("OPM has implemented a data loss prevention tool in order to monitor endpoint web activities and email in an effort to prevent the inappropriate release of PII.").

In short, the GWES PIA is not a legally sufficient PIA under the terms of the E-Government Act, and therefore Plaintiffs remain likely to succeed on the merits.

III. PLAINTIFFS WILL SUFFER IRREPARABLE HARM WITHOUT RELIEF

If the Court does not enjoin OPM's unlawful collection, aggregation, and maintenance of this data, Plaintiffs and all similarly situated individuals will be irreparably harmed. For obvious reasons, PII about U.S. Government employees is not generally available to the public. It is well established that even "names, phone numbers, email addresses and other contact information [of Government employees] are . . . 'bits of personal information . . . the release of which would create a palpable threat to privacy.'" *Alford v. McDonough*, No. 20-2805, 2024 U.S. Dist. LEXIS

137841, at *12 (D.D.C. Aug. 2, 2024) (quoting *Prison Legal News v. Samuels*, 787 F.3d 1142, 1146-47 (D.C. Cir. 2015)).

The unauthorized release of this sensitive personal information would cause immeasurable harm which would be impossible to repair because, once this data is publicly available, there is no way to control its spread or use. The last time OPM servers were hacked, the investigation report concluded:

> The devasting consequences of OPM cyberattacks discovered in 2014 and 2015 will be felt by the country for decades to come. The key question now before the country is how will we respond? Federal agencies, including OPM, must remain vigilant in protecting the information of hundreds of millions of Americans and in an environment where a single vulnerability is all a sophisticated actor needs to steal or alter Americans' information, the identities of average Americans, and profoundly damage the interest of U.S. national security.

House OPM Rep. at 225.

"In the age of the internet, when information is made public quickly and without borders, it is nearly impossible to contain an impermissible disclosure after the fact, as information can live on in perpetuity in the ether to be shared for any number of deviant purposes." *Wilcox v. Bastiste*, No. 17-122, 2017 WL 2525309, *slip op.* at *3 (E.D. Wash. June 9, 2017); *see also Pacific Radiation Oncology, LLC v. Queen's Medical Center*, 47 F. Supp. 3d 1069, 1076 (D. Haw. 2014) (noting that it is "beyond dispute that the public disclosure of that information" in medical files would subject patients "to potential irreparable harm").

Even the mere collection and aggregation of this data would cause an irreparable harm to Plaintiffs and all similarly situated individuals because OPM has refused to adopt measures to ensure the privacy and security of that data as required by law. OPM has also failed to assess or disclose how the data will be handled and secured once it is collected. Evidence strongly points to the hurried installation and use of insecure systems and improper security protocols to meet an

arbitrary deadline. *See*, *e.g.*, Allison Gill, *A Fork in the Road: Is Federal Employee Privacy Compromised?* Mueller She Wrote (Jan. 29, 2025), *at* https://www.muellershewrote.com/p/a-fork-in-the-road-is-federal-employee (last accessed Feb. 4, 2025) ("So while there is evidence that the entire operation surrounding HR@opm.gov was rushed, sloppy, and likely engineered by a small team of three or four people outside the agency, the much bigger problem is that while those subdomains were public, OPM email servers were compromised.").

Furthermore, despite the findings ten years ago that "[t]he future effectiveness of the agency's information technology and security efforts will depend on a strong relationship between [the OCIO and OIG] moving forward," *id*. at 193, Plaintiffs cannot rely on the OPM OIG to exert any influence over these matters because President Trump dismissed the Inspector General and an unknown number of staff members on 24 January. Charlie Savage, *Fired Inspectors General Raise Alarms as Trump Administration Moves to Finalize Purge* N.Y. Times (Jan. 27, 2025), *available at* https://www.nytimes.com/2025/01/27/us/politics/trump-inspectors-general-fired.html (last accessed Feb. 4, 2025). Given the history of the 2015 OPM breach, the lack of planning and foresight on the part of OPM poses an immediate and inexcusable risk to the privacy of all Executive Branch employees, as well as to anyone else whose information was ingested into the new systems, such as the contractors and Judicial Branch employees who also received emails from HR@opm.gov. With the absence of a fully functional Office of Inspector General, Plaintiffs have no recourse but to request extraordinary relief from this Court.

IV. THE BALANCE OF THE EQUITIES AND PUBLIC INTEREST FAVOR RELIEF

The balance of the equities and public interest factors favor entry of the TRO that Plaintiffs seek. The purpose of temporary relief is to preserve, not "upend the status quo." *Sherley*, 644 F.3d at 398; *Winter*, 555 U.S. at 43. Reestablishing the status quo is the purpose of

Plaintiffs' Motion. Had OPM shown any indication of its intentions prior to installing and using these new systems, Plaintiffs would have requested a TRO at that point to preserve the original status quo. However, because OPM has insisted on acting with breakneck speed and in complete secrecy when it comes to these matters, Plaintiffs—as well as the general public—have needed time to grasp how dire the threat really is. Now that more information has been revealed about these systems and the uses to which they are being put, Plaintiffs must now instead ask the Court to *return* to the status quo which was in place before these systems were installed without prior review of the privacy implications as required by law. The public interest and balance of the equities favor Plaintiffs' request to reestablish the status quo pending review by this Court.

There are no countervailing interests that weigh against the relief Plaintiffs seek. OPM would not be harmed by a temporary halt to its plans, as it has no valid interest in violating the PIA requirements in the E-Government Act. "There is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters*, 838 F.3d at 12 (citing *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511-12 (D.C. Cir. 2016); *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013)). In fact, "there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." *Id.* at 12.

CONCLUSION

For the foregoing reasons, Plaintiffs' Renewed Motion for a Temporary Restraining Order should be granted, and OPM should be restrained from continuing to operate the GWES and any system(s) connected to it prior to the completion and public release of a required legally sufficient PIA.

Date: February 7, 2025

Respectfully submitted,

/s/ Kelly B. McClanahan
Kelly B. McClanahan, Esq.
D.C. Bar #984704
National Security Counselors
1451 Rockville Pike
Suite 250
Rockville, MD 20852
501-301-4672
240-681-2189 fax
Kel@NationalSecurityLaw.org

Counsel for Plaintiffs