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' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

In the middle of the briefing of Plaintiffs' motion for a Temporary Restraining Order ("TRO"), Defendant Office of Personnel Management ("OPM") filed a motion to dismiss the case under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Notwithstanding the Court's denial of Plaintiffs' TRO motion, OPM's motion must fail for various reasons, not least of which is the fact that the standard of review for a motion to dismiss is significantly more lenient than that for a TRO motion, and the Court must accept all reasonable inferences in the complaint in Plaintiffs' favor.

As an initial matter, this briefing has become disjointed due to OPM's publication of *another* purported Privacy Impact Assessment ("PIA") since the Court denied Plaintiffs' TRO motion. *See* OPM, *Privacy Impact Assessment for Government-Wide Email System (GWES)*, at 8 (Feb. 28, 2025), *available at* https://www.opm.gov/media/kfpozkad/gwes-pia.pdf (last accessed Mar. 2, 2025) [hereinafter 2d PIA]. This new PIA completely reverses OPM's position on a key issue identified previously, removing any mention of responses to emails being sent from the Government-Wide Email System ("GWES") being voluntary. *Compare id.* ("The consequences

for failure to provide the requested information will vary depending on the particular email at issue."), *with* OPM, *Privacy Impact Assessment for Government-Wide Email System (GWES)*, at 7 (Feb. 5, 2025), *at* https://web.archive.org/web/20250222125024/https://www.opm.gov/media/kfpozkad/gwes-pia.pdf (last accessed Mar. 2, 2025) ("The Employee Response Data is explicitly voluntary. The individual federal government employees can opt out simply by not responding to the email."). However, this new purported PIA still does not meet the standard of a legitimate PIA, and so the Court should not be swayed by this latest attempt by OPM to move the goalposts once again. That being said, Plaintiffs will attempt to incorporate the new purported PIA into this Opposition, but reserve the right to request leave to file a sur-reply if OPM makes any arguments in its reply based on changes to the published PIA, which is not currently in evidence.

Additionally, this Opposition will be largely duplicative of Plaintiffs' briefs regarding their TRO motion, and they are endeavoring to avoid repeating too many arguments that the Court has already seen multiple times before. To that end, Plaintiffs stand behind their earlier briefs on these topics—Dkt. #15 and 18—and incorporate any relevant arguments from them herein if they are not explicitly reiterated.

ARGUMENT

For ease of reading, Plaintiffs will address the most problematic issues with OPM's arguments, none of which effectively refute any of Plaintiffs' contentions, in roughly the order in which they are presented in OPM's brief.[1]

[1] Plaintiffs' decision to follow the course of OPM's brief should not be interpreted as a concession that OPM has properly framed the issues; it is solely to assist the Court in matching OPM's arguments with Plaintiffs' counterarguments.

At the outset, OPM concedes that a motion to dismiss is not the appropriate place to dispute the factual allegations of a complaint: "Many of Plaintiffs' factual allegations, based on a since-deleted Reddit post, are unsubstantiated and, if this case proceeds, *will be rebutted in due course.*" (Def.'s Comb. Mem. P. & A. Supp. Def.'s Mot. Dismiss & Opp'n Pls.' Renewed Mot. TRO, Dkt. #17-1, at 1 (filed Feb. 11, 2025) [hereinafter OPM's Mem.] (emphasis added).) This basic fact of civil litigation is the core reason that OPM's motion must fail, because Plaintiffs' First Amended Complaint easily satisfies the *Twombly*/*Iqbal* standard.[2]

I. PLAINTIFFS HAVE CLEARLY ESTABLISHED STANDING

OPM's first argument attacks Plaintiffs' standing, adopting a cramped interpretation of injury which does not comport with either the record or the prevailing opinion in the case law. OPM argues, "Plaintiffs do not allege that any such [third-party] data breach has occurred, and any alleged injury stemming from a hypothetical, future data breach is too speculative to establish standing." (OPM's Mem. at 6.) But in a case like this in this current procedural posture, Plaintiffs do not *have* to allege that a third-party data breach has occurred, since the harm is *the information being stored in an insecure system where it is more vulnerable to hacking*.[3]

[2] So named for the seminal cases *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

[3] Regarding OPM's implicit argument that the GWES and associated systems are not at risk of cyberattack, Plaintiffs already introduced into evidence the opinion of a cybersecurity professional that these systems are at risk. (*See* Pls.' Mem. P. & A. Supp. Renewed Mot. TRO, Dkt. #15, at 22 (filed Feb. 7, 2025) (citing 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)).) This expert is willing to testify on these matters in this case. Moreover, this analysis has been supported elsewhere. *See DOGE Exposes Once-Secret Government Networks, Making Cyber-Espionage Easier than Ever* Cyber-Intelligence Brief (Feb. 9, 2025), *at* https://cyberintel.substack.com/p/doge-exposes-once-secret-government (last accessed Feb. 13, 2025).

The Court already explored this argument in its opinion denying Plaintiffs' TRO motion, albeit in a slightly different context, concluding:

> The information that Plaintiffs have offered does not satisfy Plaintiffs' burden of showing that they face a concrete and impending risk that their .gov email addresses will be misappropriated in the absence of emergency injunctive relief—or that their proposed relief would redress that risk. This is not to say that Plaintiffs will not be able to establish standing at a later stage of the proceeding. But they have failed to carry their burden for purposes of obtaining a TRO.

(Mem. Op. & Order, Dkt. #21, at 13 (filed Feb. 17, 2025) [hereinafter TRO Op.].) Just as the Court held then that the evidence elucidated at a later stage of the proceeding would conclusively establish whether or not the threatened harm was imminent or speculative, so should it decline to answer the question now based on the smattering of evidence from the public record before it.

If anything, the Court should order jurisdictional discovery to allow Plaintiffs to issue limited written discovery requests to OPM about the security measures currently in place around the GWES—such as Security Impact Statements, Security Assessments, Impact Assessments, Risk Assessments, and Security Reviews, which are mandatory for new government systems under the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3541, *et seq.* and/or relevant National Institute of Standards and Technology ("NIST") cybersecurity standards and guidelines, including but not limited to NIST Special Publications 800-53, 800-37, and the NIST Cybersecurity Framework—and information about attempted or actual cyberintrusions.

Courts in this Circuit have upheld the importance of jurisdictional discovery during the briefing stage of a motion to dismiss "to discover evidence relevant to [a plaintiff's] jurisdictional claim." *Citizens for Resp. & Ethics in Wash. v. Office of Admin.*, No. 07-964, 2008 WL 7077787, at *2 (D.D.C. Feb 11, 2008) (approving limited jurisdictional discovery in FOIA case to reveal OA's agency status) (citing *Nat'l Resources Def. Council v. Pena,* 147 F.3d 1012, 1024 (D.C. Cir. 1998), and *Wilderness Soc'y v. Griles,* 824 F.2d 4, 16 n.10 (D.C. Cir. 1987)).

The U.S. Supreme Court has similarly recognized a federal court's discretionary power to order "the discovery of facts necessary to ascertain their competency to entertain the merits." *Oppenheimer Fund, Inc. v. Sanders,* 437 U.S. 340, 351 (1978). "Where issues arise as to jurisdiction or venue, discovery is available to ascertain facts bearing on such issues." *Id.* at 351 n.13.[4]

OPM's second major standing argument, like a later argument pertaining to OPM's legal responsibilities, is predicated on the Court forgetting the nature of the claims and the identities of the Plaintiffs. OPM argues that Plaintiffs lack informational standing because, "[o]ther than speculation on social media, Plaintiffs provide no evidence that OPM took any of the actions that would trigger the PIA requirement under section 208(b)(1)(A)(i)-(ii) of the E-Government Act." (OPM's Mem. at 7.) According to OPM's logic, if there is no PIA requirement, then Plaintiffs cannot demonstrate informational standing when OPM does not publish a PIA. Plaintiffs agree with this assessment of the law, but it does not help OPM, since there *was* a PIA requirement, and OPM continues to disingenuously twist the record to suggest that the GWES does not contain information that it demonstrably does.

For this argument, OPM relies on the assertion: "The privacy protection covers 'citizen-centered' information being gathered 'from or about members of the public.'" (*Id.* at 8.)

[4] Courts have permitted jurisdictional discovery often in other contexts. *See*, *e.g.*, *Arar v. Ashcroft*, 585 F.3d 559 (2d Cir. 2009) (detainee mistreatment); *DeCastro v. Sanifill, Inc.*, 198 F.3d 282 (1st Cir. 1999) (piercing the corporate veil); *Noonan v. Winston*, 135 F.3d 85 (1st Cir. 1998) (defamation); *Trading Technologies Inter., Inc. v. BCG Partners, Inc.*, Nos. 10-C-715 *et al.*, 2011 WL 1220013 (N.D. Ill. Mar. 28, 2011) (patent infringement); *Sledge v. United States*, 723 F. Supp. 2d 87 (D.D.C. 2010) (to discover whether discretionary function exception applies to Bureau of Prisons in an FTCA case); *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153 (D. Mass. 2008) (copyright infringement); *7240 Shawnee Mission Holding, LLC v. Memon*, No. 08-2207, 2008 WL 4001159 (D. Kan. Aug. 26, 2008) (breach of contract); and *Vance v. Rumsfeld*, No. 06-C-6964, 2007 WL 4557812 (N.D. Ill. Dec. 21, 2007) (whistleblower retaliation).

According to OPM, that requirement does not apply in this case because "the PIA does not suggest that the GWES is limited to the 'Executive Branch.' Instead, it refers to "federal government employees.' Plaintiffs provide no examples of Plaintiffs whose email domains are other than .gov or .mil." (*Id.* at 16 (citation omitted).) Practically all of OPM's brief requires the Court to accept this statement as accurate, when it is decidedly not.

First, nowhere does OPM offer any legal support for the contention that federal judges or Library of Congress employees satisfy the statutory definition of "agencies, instrumentalities, or employees of the Federal Government" in a law specifically designed to apply to the Executive Branch. 44 U.S.C. § 3501 note § 208(b)(1)(A). However, even if such individuals did fall within this definition, OPM does not offer any legal support for the contention that "an employee of a National Resources Conservation District," "a Conservation Legacy Individual Placement member funded by Americorps," and "an employee of the State of California—which has a partnership with an agency in the United States Executive Branch," none of whom are U.S. Government employees, (1st Am. Compl., Dkt. #14, ¶¶ 5-7 (filed Feb. 7, 2025) [hereinafter 1st Am. Compl.]) are "agencies, instrumentalities, or employees of the Federal Government." Critically, even if *these* individuals did fall within this definition, one plaintiff is "a contractor for the Department of State." (*Id.* ¶ 8.) OPM's argument that a *contractor* is a "federal government employee" is frivolous on its face. Once the Court accepts that the GWES contains information about contractors as well as "federal government employees"—however it chooses to define that term—it must conclude that the GWES gathers information "from or about members of the public," which OPM admits triggers a PIA requirement. (OPM's Mem. at 8 (quoting *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* § II(b)(1)(a)).)

II. PLAINTIFFS HAVE STATED A CLAIM

OPM then pivots to arguing that, even if a PIA was required to be published, its publication of a PIA—no matter how incomplete—renders the case moot and therefore strips the Court of jurisdiction. It similarly argues that, even if the Court *has* jurisdiction, Plaintiffs fail to state a claim because Plaintiffs have no "right to challenge the substance and accuracy of the PIA." (*Id.* at 8-9.) Because these arguments are two sides of the same coin, Plaintiffs will address them together.

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 do 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). The Office of Management and Budget ("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 Procedure Act ("APA"), 5 U.S.C. § 706(2)(A).

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 Veterans 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 WL 11614156, at *7 (N.D. Ala. Apr. 21, 2010) (quoting Bolten Memo § II.B.3.f). However, 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.[5] OPM's decision to initiate collection and aggregation of PII belonging to over two million Executive Branch employees and countless others 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." *Id*.

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

[5] To the Court's previous question of whether a plaintiff can sue an agency under the APA for not following OMB guidance, the violation of the law in such cases is not the violation of the *guidance per se*, but the violation of the *law* based on the context of the guidance. *See*, *e.g.*, *Pub. Citizen v. Lew*, 127 F. Supp. 2d 1, 13 (D.D.C. 2000) (finding agency did not violate Federal Records Act based on OMB guidance).

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.

In short, the GWES PIA is not a legally sufficient PIA under the terms of the E-Government Act, and Plaintiffs can sue under the APA to compel the production of a legally sufficient PIA.

OPM's final two arguments do not warrant serious discussion. First, it contends that "the publication of a PIA is not a reviewable final agency action." (OPM's Mem. at 10.) In doing so, it unreasonably diminishes the statutory requirement that it create a legally mandated document which is legally required to: (a) address certain information; (b) be formally approved by a senior agency official; and (c) be made publicly available. Instead, OPM argues that PIAs are akin to "agency reports, opinions, press releases, and similar publications." (*Id.* at 12.) However, in doing so, it ignores the basic fact that if an agency does *not* create a PIA, that is recognized as a violation of the APA. If creating a PIA is not a final agency action, then nobody could sue an

agency for not creating one. Since it is well-recognized that they can, this is a meritless argument.

Lastly, OPM argues against the use of the Declaratory Judgment Act, but in doing so it misses the forest for the trees. To clarify, Plaintiffs agree that if every other part of the complaint is dismissed, then the citation to the Declaratory Judgment Act does not save the case. It was never supposed to. The Declaratory Judgment Act is cited to allow the Court to enter a declaratory judgment if it finds that Plaintiffs have the right of it as a legal matter. The Court should not expend any serious energy on this question.

CONCLUSION

For the foregoing reasons, OPM's Motion to Dismiss should be denied.

Date: March 5, 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