UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JANE DOE, *et al.*,

Plaintiffs,

v.

OFFICE OF PERSONNEL MANAGEMENT,

Defendant.

Civil Action No. 25-234 (RDM)

MEMORANDUM OPINION AND ORDER

In late January 2025, the Office of Personnel Management ("OPM") began to test "'a new capability allowing it to send important communications to ALL civilian federal employees from a single email address,'" and OPM subsequently began using this new system to send messages "to most if not all individuals with Government email addresses." Dkt. 14 at 4–5 (Am. Compl. ¶¶ 20, 22) (quoting OPM statement). That new system uses the email address HR@opm.gov and is known as the "Government-Wide Email System" or "GWES." *Id.* at 2–3 (Am. Compl. ¶ 10). This putative class action challenges the process by which OPM implemented this new system.

Plaintiffs are two federal executive branch employees and five other individuals who have ".gov" email addresses but are not executive branch employees. *See id.* at 1–2 (Am. Compl. ¶¶ 3–10). They contend that in the rush to adopt this new system, OPM at first entirely failed to comply with Section 208 of the E-Government Act of 2002, which requires the preparation of a Privacy Impact Assessment ("PIA") before "initiating a new collection of [certain] information . . . using information technology," 44 U.S.C. § 3501 note, Pub. L. No.

107-347, § 208, 116 Stat. 2899, 2921-22 (Dec. 17, 2002) (hereinafter "E-Government Act"), and, then, when confronted with that omission, immediately threw together an inaccurate, insufficient, and unconsidered PIA in the hope of mooting the case. According to Plaintiffs, OPM's failure to prepare a meaningful Privacy Impact Assessment has left vast amounts of private information, including the government email addresses of millions of individuals (which reveal their names and, at least in some cases, their employers) at risk of disclosure in the event that the GWES is hacked.

OPM, for its part, contends that it was not required to prepare a PIA because, on OPM's reading, Section 208 does not apply to the collection of information about government employees, as opposed to about members of the public. And, even if that contention is wrong—either because it has misread the statute or because OPM inadvertently collected email addresses from individuals who do not work for the federal government but nonetheless use .gov or .mil email addresses—OPM, in any event, has now prepared a PIA. That is all that is required, on OPM's telling, and the Court lacks the authority to examine the "substance and accuracy" of the PIA that the agency prepared. Dkt. 17-1 at 15.

Pending before the Court is Plaintiffs' motion for a temporary restraining order ("TRO"), Dkt. 15, which asks the Court to enjoin OPM "from continuing to operate the Government-Wide Email System or any computer system connected to it prior to the completion and public release of a required legally sufficient Privacy Impact Assessment." Dkt. 15-2 at 1. But Plaintiffs have failed to carry their burden of demonstrating (1) that they likely have standing to bring this action, and (2) that they are likely to suffer irreparable injury in the absence of emergency relief. The Court will, accordingly, **DENY** Plaintiffs' motion.

I. BACKGROUND

A. Regulatory Background

"In 2002, the Congress passed the E-Government Act to streamline government use of information technology 'in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.'" *EPIC v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 375 (D.C. Cir. 2017). Among other provisions of the Act, Section 208 requires federal agencies to prepare PIAs "before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or "(ii) initiating a new collection of information that . . . will be collected, maintained, or disseminated using information technology; and . . . includes any information in an identifiable form permitting the . . . 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." E-Government Act, § 208(b)(1)(A). In 2003, the Office of Management and Budget ("OMB") issued guidance, construing Section 208 to require preparation of "a PIA before . . . developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about any member of the public." *See* M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Att. A, Sec. II(B)(a)(1) (Sept. 26, 2003) (hereinafter "OMB Guidance"). According to that guidance, "[n]o PIA is required where information relates to internal government operations," including when information is collected "for government-run . . . IT systems . . . to the extent that they do not collect or maintain information in identifiable form about members of the general public." *Id.* at Sec. II(B)(c).

When an agency is required to prepare a PIA, the agency's "Chief Information Officer, or equivalent official, as determined by the head of the agency," must review the PIA, and, "[i]f practicable," the PIA must then be made "publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act, § 208(b)(1)(B). The statute also instructs OMB to "issue guidance to agencies specifying the required contents" of a PIA, and stipulates that such guidance must require at least that PIAs identify the information to be collected, why it is being collecting, the intended use of the information, "with whom the information will be shared," "what notice of opportunity for consent would be provided to individuals regarding what information is collected and how that information is shared," "how the information will be secured," and whether the information will be maintained in a system of records for purposes of the Privacy Act, 5 U.S.C. § 552a. E-Government Act, § 208(b)(2)(B).

The OMB Guidance, in turn, specifies that PIAs must (in addition to addressing the considerations required by the E-Government Act) "identify what choices the agency made . . . as a result of performing the PIA." OMB Guidance, Att. A, Sec. II(C)(a)(2). It also instructs that "[t]he depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system." *Id.* at Sec. II(C)(b)(1). "Major information systems," for example, should "reflect more extensive analysis" of the consequences and alternatives to collection, whereas "routine database systems" can be assessed using a "standardized approach (e.g., checklist or template)." *Id.* at Sec. II(C)(b)(1)(2), (3).

B. Factual Background

Summarizing the relevant factual background presents a unique challenge in this case because OPM has yet to submit an administrative record, and Plaintiffs cite to a series of news reports but have failed to offer any declarations or other evidence in support of their motion. As

far as the Court can discern, however, the following facts are either uncontested or are reflected in the one administrative document before the Court, the February 5, 2025 PIA prepared by OPM and reviewed by the agency's newly installed Chief Information Officer, Greg Hogan. Dkt. 10-1.

Three days after the presidential transition, OPM issued a statement indicating that it was "testing a new capability allowing it to send important communications to ALL civilian federal employees from a single email address," HR@opm.gov. Dkt. 14 at 4–5 (Am. Compl. ¶¶ 20–21). Since then, OPM has sent several email messages to large swaths of the executive branch workforce, and, perhaps inadvertently, to a host of others, including (apparently) members and staff of the federal judiciary, government contractors, state employees with .gov email addresses, and employees of agencies in the legislative branch. OPM launched this effort without conducting a PIA in advance.

Two federal employees initiated this action on January 27, 2025, alleging that OPM was acting in violation of Section 208 of the E-Government Act, Dkt. 1, and they filed a motion for a TRO on February 4, 2025, Dkt. 4. The emergency relief that Plaintiffs sought was an order barring OPM from operating "any computer systems connected to the HR@opm.gov address . . . prior to the completion and public release of a required Privacy Impact Assessment." Dkt. 4-2 at 1. OPM responded to that motion the following day, and the agency attached to its opposition a "Privacy Impact Assessment for Government-Wide Email System (GWES)," dated February 5, 2025. *See* Dkt. 10, Dkt. 10-1.

The Court held a hearing on the motion on February 6, 2025, and denied the motion as moot. *See* Min. Entry (Feb. 6, 2025). As the Court explained, because OPM had conducted a PIA, the relief that Plaintiffs sought was no longer meaningful; there was no reason for the Court

to issue an order barring OPM from using computer systems connected to the HR@opm.gov email address because the condition precedent that Plaintiffs themselves specified had already been satisfied. Nor was the Court persuaded by the arguments that Plaintiffs' counsel presented for the first time at the hearing. In particular, Plaintiffs' counsel argued that the February 5 PIA was inadequate. As the Court explained, however, neither Plaintiffs' complaint nor their then-pending motion for a TRO challenged the adequacy of the PIA—which post-dated both filings. Finally, the Court expressed skepticism that the two Plaintiffs, both current federal employees, could challenge the PIA, given Section 208's focus on the general public.

On February 7, 2025, Plaintiffs filed an amended complaint that made two significant changes to their case. Dkt. 14 (Am. Compl.). First, they added five new plaintiffs, each of whom has a .gov email address, but none of whom work in the executive branch of the United States government. *Id.* at 2–3 (Am. Compl.). Second, Plaintiffs challenged the adequacy of the February 5 PIA. *Id.* at 9–12 (Am. Compl.). That same day, the expanded group of Plaintiffs filed a renewed motion for a TRO. Dkt. 15. On February 11, 2025, OPM responded both by opposing Plaintiffs' motion for a TRO and by moving to dismiss Plaintiffs' amended complaint for lack of jurisdiction and for failure to state a claim. Dkt. 16. Plaintiffs filed a reply on February 13, 2025, Dkt. 18, and the Court held a hearing on the renewed motion the following day. Plaintiffs have failed to offer any evidence, other than news stories and a podcast, in support of their motion, and, instead, suggested (incorrectly) that the Court should simply treat their as-of-yet uncontroverted allegations as true.

Plaintiffs' renewed motion for a TRO is now ripe for decision.

II. ANALYSIS

A TRO is "an extraordinary form of relief," *Banks v. Booth*, 459 F. Supp. 3d 143, 149 (D.D.C. 2020), which a court should grant only under extraordinary circumstances. Although considered on an abbreviated schedule and without the benefit of a complete record, the same factors the apply to a motion for a preliminary injunction apply to a motion for a TRO. Most critically, a TRO "may only be awarded upon a clear showing that the plaintiff is entitled to [the requested] relief." *Id.* (quoting *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011)). A TRO is not merely a means of maintaining the status quo while a plaintiff prepares a motion for a preliminary injunction and the defendant prepares its opposition brief. Rather, as with a motion for a preliminary injunction, federal courts are empowered to grant relief if and only if the moving party has established "[1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest." *Aamer v. Obama*, 742 F.3d 1023, 1038 (D.C. Cir. 2014) (alterations in original) (quotation marks omitted). When seeking such relief, "the movant has the burden to show that all four factors, taken together, weigh in favor of the injunction." *Abdullah v. Obama*, 753 F.3d 193, 197 (D.C. Cir. 2014) (quoting *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1292 (D.C. Cir. 2009)) (internal quotation marks omitted).

The Court's inquiry begins and ends with Plaintiffs' asserted injuries, which must satisfy two important requirements before the Court can grant emergency relief:

First, to obtain a TRO, a plaintiff must demonstrate that it is likely that she has standing to pursue the claim at issue, and absent that showing, the Court may not grant relief. *See Nat'l Wildlife Fed'n v. Burford*, 835 F.2d 305, 328 (D.C. Cir. 1987) (Williams, J., concurring and

dissenting) (noting that a party seeking preliminary injunctive relief must demonstrate a likelihood of success, which "necessarily includes a likelihood of the court's reaching the merits, which in turn depends on a likelihood that [the] plaintiff has standing"); s*ee also Nguyen v. U.S. Dep't of Homeland Sec.*, 460 F. Supp. 3d 27, 33 (D.D.C. 2020) ("In the context of a temporary restraining order or preliminary injunction, courts 'require the plaintiff to show a substantial likelihood of standing under the heightened standard for evaluating a motion for summary judgment.'" (quoting *EPIC*, 878 F.3d at 377)). In short, "[a] plaintiff unlikely to have standing is *ipso facto* unlikely to succeed, and when the plaintiff is unlikely to succeed, 'there is no need to consider the remaining factors.'" *EPIC*, 878 F.3d at 375 n.2 (quoting *Greater New Orleans Fair Hous. Action Ctr. v. HUD*, 639 F.3d 1078, 1088 (D.C. Cir. 2011)).

Second, "a showing that irreparable injury is 'likely' is the *sine qua non* for obtaining a preliminary injunction—it is what justifies the extraordinary remedy of granting relief before the parties have had the opportunity fully to develop the evidence and fully to present their respective cases." *Achagzai v. Broad. Bd. of Governors*, 2016 WL 471274, at *3–4 (D.D.C. Feb. 8, 2016); *see also California Ass'n of Private Postsecondary Schools v. DeVos*, 344 F. Supp. 3d 158, 167 (D.D.C. 2018); *Texas Children's Hosp. v. Burwell*, 76 F. Supp. 3d 224, 241–42 (D.D.C. 2014); *Trudeau v. FTC*, 384 F. Supp. 2d 281, 296 (D.D.C. 2005), *aff'd*, 456 F.3d 178 (D.C. Cir. 2006). "A movant's failure to show any irreparable harm is therefore grounds for refusing to issue a preliminary injunction, even if the other three factors entering the calculus merit such relief." *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006).

Here, Plaintiffs premise their motion for preliminary relief on two alleged injuries: first, that they are suffering an ongoing injury simply because their "information [is] being stored in an insecure system," Dkt. 18 at 3 (emphasis removed), and second, that their information is

"more vulnerable to hacking because it is in a system that is vulnerable to hacking," Feb. 14, 2025 Hrg. Tr. (Rough at 15); *see also* Dkt. 15 at 23.[1] Plaintiffs, however, have failed to carry their burden with respect to establishing that they have a "substantial likelihood of standing" based on either injury, *Nguyen*, 460 F. Supp. 3d at 33, let alone that those injuries are "certain" enough and "great" enough to warrant preliminary injunctive relief, *Wisconsin Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985).

A.

"To establish standing, a party must demonstrate: '(1) an injury in fact that is concrete and particularized as well as actual or imminent; (2) a causal connection between the injury and the challenged conduct; and (3) a likelihood, as opposed to mere speculation, that the injury will be redressed by a favorable decision.'" *Nat. Res. Def. Council v. Wheeler*, 955 F.3d 68, 76 (D.C. Cir. 2020) (quoting *Nat. Res. Def. Council v. EPA*, 755 F.3d 1010, 1016 (D.C. Cir. 2014)). Here, OPM focuses on Plaintiffs' failure at the first step in this inquiry—they have failed to identify an "injury in fact" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan v. Defs. of Wildlife*, 504 U.S. 55, 560–61 (1992). It bears emphasis, moreover, that a plaintiff cannot establish standing by merely asserting that the government has failed to follow a required procedure (say, for example, failing to conduct a PIA), since "bare procedural violation[s], divorced from any concrete harm" do not "satisfy the injury-in-fact requirement of Article III." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016).

[1] In its opposition brief, OPM identified an alternative potential source of injury to Plaintiffs—informational injury—and argued that the relevant standard is not satisfied here. *See* Dkt. 17-1 at 13. Plaintiffs, however, have never pressed this theory of standing and, indeed, when asked repeatedly at oral argument to identify every possible injury that they rely upon, Plaintiffs said nothing about informational standing.

As the Supreme Court has explained, not every statutory violation results in the type of concrete injury-in-fact sufficient to support Article III standing. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021). Rather, "Article III standing requires a concrete injury even in the context of a statutory violation." *Spokeo*, 578 U.S. at 341. The question, then, is "[w]hat makes a harm concrete for purposes of Article III?" *TransUnion LLC*, 594 U.S. at 424. To answer that question in a case like this one, which does not involve an alleged constitutional violation, Plaintiffs must "identif[y] a close historical or common-law analogue for their asserted injur[ies]." *Id.* at 425. In *TransUnion*, for example, a credit reporting agency had erroneously placed Office of Foreign Assets Control or "OFAC" alerts in the plaintiffs' credit reports, "labeling them as potential terrorists." *Id.* at 431. The Supreme Court assumed that the credit reporting agency "violated its obligations under the Fair Credit Reporting Act" to maintain accurate information about consumers. *Id.* But the Court held that plaintiffs whose information had not been communicated to third parties lacked standing to bring that claim. The Court explained that an uncommunicated erroneous OFAC alert was not a "concrete injury" because "there is no historical or common-law analog" to this type of harm. *Id.* at 434 (quotation marks omitted). Instead, "the plaintiffs' harm [wa]s roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer." *Id.* Thus, "the mere existence" of an incorrect OFAC alert in a consumer's credit file—even if a violation of federal law—was "insufficient to confer Article III standing." *Id.*

Here, neither of the injuries that Plaintiffs have identified at this stage of proceeding are sufficient to confer Article III standing. Plaintiffs' first alleged injury—the mere fact that their .gov email addresses are being stored on an allegedly unsecured system—cannot survive *TransUnion*. Even assuming that Plaintiffs' .gov email addresses are being held on an unsecured

system, that alleged injury is no more concrete or actual than the alleged injury of those members of the *TransUnion* class who complained about uncommunicated erroneous OFAC alerts. Moreover, rather than identify any common-law analogues, as *TransUnion* requires, Plaintiffs instead resort to a policy argument unmoored to Article III. They contend that, if standing is unavailable here,

> the only way that any court could ever enjoin any agency from operating an insecure system to prevent it from being hacked would be if it had already been hacked, at which point an injunction would be pointless.

Dkt. 18 at 3.[2] But it is not the job of the federal courts to police the security of the information systems in the executive branch, just as it is not the job of the federal courts to police the internal notations on consumers' credit reports. *See TransUnion LLC*, 594 U.S. at 434.

Plaintiffs' second theory of standing, which posits that the OPM computers that are connected to the GWES are vulnerable to hacking, fares no better. Although an actual hacking incident or an imminent hack might suffice, Article III requires more than a possibility of future harm—a "theory of future injury" must be "certainly impending" and non-speculative. *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 401 (2013) (internal quotation marks omitted). Here, at least on the present record, Plaintiffs have failed to carry their burden of demonstrating that their .gov email addresses (which reveal their names and, possibly, their places of employment) are at

---

[2] Plaintiffs also conjure a hypothetical, asking the Court to

> imagine a scenario in which an agency posted a list of its employees' social security numbers on its website and then argued that no court could make it take the list down until someone's identity was stolen.

Dkt. 18 at 3. But that hypothetical hurts Plaintiffs' argument more than it helps. This case is very different from a case in which the loss of sensitive personal information is a near certainty. Just as *TransUnion* drew a distinction between those individuals whose erroneous credit reports were shared with third parties and those whose erroneous reports were not, so too is a case where personally identifying information has been published different from one where the harm is a yet-unrealized risk of disclosure.

imminent risk of exposure outside the United States government—much less that this risk is a result of OPM's failure to conduct an adequate PIA. Rather, their arguments "rel[y] on a highly attenuated chain of possibilities." *Id.* at 410.

Plaintiffs premise much of their argument on an earlier hack of OPM databases containing sensitive information about millions of government employees, which occurred almost a decade ago. Dkt. 15 at 4. But past is not always prologue, particularly when it comes to Article III. Where, as here, a plaintiff seeks prospective, injunctive relief, the plaintiff must demonstrate that she is "likely to suffer future injury from the" alleged unlawful conduct, and a past violation will not suffice absent reason to believe it will occur again in the future. *City of Los Angeles v. Lyons*, 461 U.S. 95, 106 (1983). Here, that means that Plaintiffs must do more than point to a decade-old failure to protect sensitive data; they must show that OPM computer systems that are connected to the GWES are at imminent risk of cyberattack and that this risk would be mitigated were the agency required to conduct a new and improved PIA.

As evidence that a hack is supposedly imminent, Plaintiffs point to a podcast on which an anonymous "systems security expert" discusses potential vulnerabilities related to the GWES. *See* 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. 14, 2025).[3] Although that podcast raises questions about the process by which the GWES servers were set up, it does not provide any specific information

[3] According to a blurb accompanying the podcast, Plaintiffs' counsel was the person who introduced the podcast host to the "system security expert" who the host interviewed. Plaintiffs' counsel has indicated that this expert is prepared to testify in this matter. Subject to the governing rules, Plaintiffs are welcome to proffer whatever evidence they deem appropriate at a later stage of the proceeding. For present purposes, however, the Court can consider only the evidence that is before it.

that would permit the Court to conclude that the servers housing .gov email addresses collected for purposes of the GWES are at imminent risk due to likely cyberattack. To the contrary, the anonymous expert mostly addresses a past vulnerability that has since been rectified. He explains that, when the GWES was first set up, hundreds of "host names" that "appeared" to be linked to "internal" OPM systems (which included systems with names that indicated they were "admin portals" or "security portals") were made "accessible from the internet." *Id.* But those "host names" were later "redacted" and are no longer visible on the public domain. *Id.* The fact that those systems were more visible than they should have been for some period of time after the GWES was set up does not support Plaintiffs' assertion that a hack is likely or imminent.

Although the anonymous expert also stated that the GWES servers were *possibly* set up in ways that were not "within the standard that you would consider an internal system to be held to," he also indicated that the system was protected in other ways, such as by a using "a web application firewall from Akamai" that "provide[s] some degree of protection." *Id.* The evidence provided by the podcast is, therefore, mixed at best. More is required to satisfy Article III, and more is required to demonstrate, as Plaintiffs must do to obtain emergency injunctive relief, that they are likely to succeed in establishing standing to sue. 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.

The Court, accordingly, concludes that Plaintiffs' motion for a TRO fails because they have not shown that they likely have standing to sue.

B.

Although the Court need not reach the issue, the Court further concludes that Plaintiffs' motion fails for a second, related reason. They have failed to carry their burden of demonstrating that, absent emergency relief, they are like to suffer an irreparable injury.

The D.C. Circuit "has set a high standard for irreparable injury." *Chaplaincy of Full Gospel Churches*, 454 F.3d at 297. To qualify, the injury must not only be unrecoverable, it must also be "both certain and great; [and] it must be actual and not theoretical." *Wis. Gas Co.*, 758 F.2d at 674. Here, it goes without saying that the mere fact that Plaintiffs' .gov email addresses are stored on an allegedly unsecure IT system does not—standing alone—amount to irreparable injury. Nor can the Court conclude that the risk of some future harm due to a potential hack of OPM, and disclosure of Plaintiffs' .gov email addresses, is either "certain" or "great."

For the reasons explained above, Plaintiffs have failed to demonstrate that there is a significant risk that their .gov email addresses will be stolen or publicly disclosed in the next 14 days or that any such risk is a product of the inadequacies of OPM's February 5 PIA. In assessing irreparable injury, moreover, the Court must also consider the nature of the potential injury. That matters because this is not a case in which Plaintiffs seek to protect *highly sensitive* personal information, like tax records or sensitive medical files. Instead, they seek to protect their work email addresses. The Court does not doubt that government employees, at times, have a privacy interest in their work email addresses, which identify their names and oftentimes where they work. In some cases, revealing that information could result in harassment or unwanted attention. But, here, the seven named Plaintiffs have failed to offer any evidence that, even if a massive hack were to occur due to OPM's failure to prepare an adequacy PIA, the disclosure of

their .gov email addresses—along with millions of other .gov email addresses—would likely subject them to personal harassment, much less that it would cause them a harm that is "certain" and "great."[4] Were this a case brought under the Freedom of Information Act ("FOIA"), the Court might conclude that the agency is entitled to withhold the email addresses on the ground that disclosure "would constitute a clearly unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(6). But this is not a FOIA case, and the requirement for issuance of a TRO is far more demanding.

The Court, accordingly, concludes that Plaintiffs have failed to carry their burden of demonstrating that they are likely to incur some irreparable injury if the Court does not enjoin OPM from operating the GWES without first preparing a more robust and accurate PIA.

CONCLUSION

For all these reasons, Plaintiffs' motion for a temporary restraining order, Dkt. 15, is hereby **DENIED**.

SO ORDERED.

/s/ Randolph D. Moss
RANDOLPH D. MOSS
United States District Judge

Date: February 17, 2025

[4] At oral argument, Plaintiffs' counsel indicated that one of the Plaintiffs works for the Federal Emergency Management Agency ("FEMA"), and he argued that associating her with FEMA could invite harassment. *See* Feb. 14, 2025 Hrg. Tr. (Rough at 27). But that argument, raised by counsel and without any evidentiary support, is insufficient to justify the issuance of a TRO. And, in any event, the argument fails to address the more fundamental problem with Plaintiffs' theory of irreparable injury; they have failed to offer evidence sufficient to permit the Court to find that the risk of a breach is "certain"—or even likely to occur in the next 14 days.