**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

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

**FIRST AMENDED COMPLAINT – CLASS ACTION**

Plaintiffs Jane Does 1-7, and where appropriate all other similarly situated individuals, bring this action against Defendant Office of Personnel Management pursuant to the Administrative Procedure Act, 5 U.S.C. § 701, *et seq.* ("APA"), the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, and the All Writs Act, 28 U.S.C. § 1651.

**JURISDICTION**

1. This Court has both subject matter jurisdiction over this action and personal jurisdiction over Defendant pursuant to 28 U.S.C. § 1331.

**VENUE**

2. Venue is appropriate under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

**PARTIES**

3. Plaintiff Jane Doe 1 ("Doe 1") is a U.S. citizen and is a resident of the state of Maryland. She is an employee of an agency in the United States Executive Branch. She has an email address assigned by an Executive Branch agency which ends with .gov (".gov email address").

4. Plaintiff Jane Doe 2 ("Doe 2") is a U.S. citizen and is a resident of the Commonwealth of Virginia. She is an employee of an agency in the United States Executive Branch. She has a .gov email address.

5. Plaintiff Jane Doe 3 ("Doe 3") is a U.S. citizen and is a resident of the state of Wyoming. She is an employee of a National Resources Conservation District and not an employee of an agency in the United States Executive Branch. She has a .gov email address.

6. Plaintiff Jane Doe 4 ("Doe 4") is a U.S. citizen and is a resident of a state in the American Southwest. She is a Conservation Legacy Individual Placement member funded by Americorps and not an employee of an agency in the United States Executive Branch. She has a .gov email address.

7. Plaintiff Jane Doe 5 ("Doe 5") is a U.S. citizen and is a resident of the state of California. She is an employee of the State of California—which has a partnership with an agency in the United States Executive Branch—and not an employee of an agency in the United States Executive Branch. She has a .gov email address.

8. Plaintiff Jane Doe 6 ("Doe 6") is a U.S. citizen and is a resident of the state of Maryland. She is a contractor for the Department of State and not an employee of an agency in the United States Executive Branch. She has a .gov email address.

9. Plaintiff Jane Doe 7 ("Doe 7") is a U.S. citizen and is a resident of the state of West Virginia. She is an employee of the Library of Congress and not an employee of an agency in the United States Executive Branch. She has a .gov email address.

10. Similarly situated individuals include all individuals who have an email address assigned by an Executive Branch agency ending in .gov or .mil whose Personally Identifiable

Information has been stored in the Office of Personnel Management's ("OPM") Government-Wide Email System ("GWES") or any system connected to it.

11. Defendant OPM is an agency of the United States Executive Branch and is in control of the system(s) which are the subject of this action.

**CLASS ACTION ALLEGATIONS**

12. This action is brought by Plaintiffs on their own behalf and on behalf of the class of all others similarly situated under the provisions of Fed. R. Civ. P. 23(a) and (b)(1)-(2).

13. The class so represented by Plaintiffs in this action, and of which they are members, consists of anyone who received an email to an email address ending in .gov or .mil ("Government email address") purporting to be from HR@opm.gov, as well as any individuals with Government email addresses whose PII is stored in the system in question but who did not receive an email from HR@opm.gov.

14. The exact number of members of the class, as hereinabove identified and described, is not known, but it is reasonable to believe the class is so numerous that joinder of individual members is impractical.

15. The relief sought is common to the entire class, and there are common questions of law and fact that relate to and affect the rights of each member of the class. These common questions include and involve whether OPM can legally operate the system(s) in question without first publishing a legally sufficient Privacy Impact Assessment ("PIA") and whether OPM must disgorge all information collected before the publication of a legally sufficient PIA. Certain defenses raised by OPM would apply equally to all members of the class.

16. The claim of Plaintiffs against OPM are typical of the claims of the class in that the claims of all members of the class depend on a showing of the acts of OPM as giving rise to

rights to the relief sought herein. There is no conflict as between Plaintiffs and other members of the class with respect to this action, or with respect to the claims for relief contained herein.

17. Plaintiffs are representative parties for the class and are able to and will fairly and adequately protect the interests of the class. Plaintiffs' undersigned counsel is experienced and capable in litigating the claims at issue and has represented claimants in other matters of this nature.

18. This action is properly maintained as a class action in that the prosecution of separate actions by individual members of the class would create a risk of adjudications with respect to individual members of the class which would as a practical matter be dispositive of the interests of others not party to the adjudications, or would substantially impair or impede their ability to protect their interests.

19. This action is properly maintained as a class action inasmuch as the questions of law and fact common to the members of the class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

## BACKGROUND

### *Part I: The OPM Emails*

20. 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."

21. Beginning 23 January, some U.S. Executive Branch agencies began sending employees messages from senior officials advising that any emails received from HR@opm.gov

should be considered legitimate. For example, on 23 January, the Acting Secretary of Homeland Security sent the following message to all Department of Homeland Security employees: "The Office of Personnel Management (OPM) is testing a new capability allowing it to send important communications to ALL Federal employees from a single email address, HR@opm.gov. If you ever receive communications from this address, it can be considered trusted."

22. On 24 January, OPM sent the following message to most if not all individuals with Government email addresses purporting to be from HR@opm.gov: "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. Also on 24 January, Doe 1 was advised by senior agency attorneys to follow the instructions in the email and reply.

23. On 24 January, the Library of Congress sent all Library of Congress staff the following email regarding the above message: "The message from OPM titled 'HR' that was sent this morning is legitimate but is intended for federal employees in the Executive Branch. The messages is not a phishing attempt and is safe. However, as Library of Congress employees are in the Legislative Branch, no response is required."

24. On 24 January, the Administrative Office of U.S. Courts sent a similar message to all Judiciary Branch employees.

25. OPM sent the following message to most if not all individuals with Government email addresses purporting to be from HR@opm.gov:

> 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.

26. Upon information and belief, OPM has sent at least eight emails to most if not all individuals with Government email addresses purporting to be from HR@opm.gov, as recently as 6 February. Not all plaintiffs have received all such emails, but it is unclear whether that discrepancy is due to actions by OPM to remove their information from the relevant system(s), actions by OPM to remove their addresses from mailing lists but not from the relevant system(s), or some intermediate filtering process (such as an agency-wide spam filter).

*Part II: The Government-Wide Email System*

27. On 27 January, 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]

28. 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.

29. 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).

30. 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).

31. 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). 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).

32. 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.

33. 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).

34. Upon information and belief, this server and/or other systems linked to it are retaining information about every individual with a Government email address.

35. Upon information and belief, this server is not sending these or other emails securely due to the rapid deployment. Secure communications take time and coordination to plan and implement. Standard email is not encrypted, and it is common practice among hackers—including hackers affiliated with hostile foreign services—to begin attempting to access a new U.S. Government device as soon as they learn of its deployment.

36. On 5 February, in a response to a motion for a Temporary Restraining Order filed by the original two plaintiffs, OPM issued a document purporting to be a Privacy Impact Assessment ("PIA") for this system, which it identified as the Government-Wide Email System (GWES).

*Part III: The Purported Privacy Impact Assessment*

37. The 5 February document entitled "Privacy Impact Assessment for Government-Wide Email System (GWES)" (hereinafter "GWES PIA") identified Riccardo Biasini, Senior

Advisor to the Director, as the Contact Point, and Greg Hogan, Chief Information Officer, as the Reviewing Official.

38. Upon information and belief, Biasini and/or Hogan are Special Government Employees and not full-time OPM employees.

39. Neither Biasini nor Hogan were OPM employees prior to 20 January.

40. Biasini worked at the Boring Company prior to 20 January. It is not currently known if he still works there.

41. Hogan worked at Comma.ai prior to 20 January. It is not currently known if he still works there.

42. The GWES PIA was both factually inaccurate and legally inadequate.

**CAUSE OF ACTION**

**(FAILURE TO CREATE LEGALLY SUFFICIENT PIA)**

43. Plaintiffs repeat and reallege the allegations contained in all paragraphs set forth above.

44. 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 Privacy Impact Assessment ("PIA") before initiating such collection. *See* 44 U.S.C. § 3501 note.

45. The agency must "(i) conduct 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."

46. OPM is an agency subject to the E-Government Act because it is an "establishment in the executive branch of the Government."

47. A PIA for a "new collection of information" 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." The PIA must specifically address "(I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured."

48. The Office of Management and Budget ("OMB") is charged with "oversee[ing] the implementation of the privacy impact assessment processing throughout the Government" and "develop[ing] policies and guidelines or agencies on the conduct of privacy impact assessments."

49. Accordingly, OMB has clarified the minimum requirements for a PIA and the role of PIAs in an agency's decision to collect (or to refrain from collecting) personal data.

50. According to OMB, "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."

51. According to OMB, "PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA."

52. OMB 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
4. the rationale for the final design choice or business process.

53. OPM has not conducted a legally sufficient PIA for the GWES or any system which collects or maintains PII obtained from its use.

54. Upon information and belief, OPM has not ensured review of a PIA for any of these systems by any legally sufficient Chief Information Officer or equivalent official.

55. OPM has not published a legally sufficient PIA or made such an assessment available for public inspection for any of these systems.

56. OPM's failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

57. Plaintiffs are being materially harmed by this inaction because they are being denied information about how these systems—which will be rich in PII about every member of the class—are being designed and used.

58. Plaintiffs stand to continue to be harmed by this ongoing inaction in the future beyond the informational injury, since they will face a reasonably foreseeable risk that their PII will be unlawfully obtained from these unknown systems, much as the data of millions of federal employees were unlawfully obtained from another OPM server in 2014.

59. Plaintiffs have a direct interest in ensuring that OPM conducts and publishes a legally sufficient PIA for these systems.

60. Plaintiffs Jane Does 3-7 are particularly harmed by OPM's intentional and/or willful publication of the factually inaccurate GWES PIA because it falsely states that the GWES "collects, maintains, and disseminates only the information of federal government employees," which, if it is accepted as legitimate by the Court, arguably robs them of any ability to challenge its collection, maintenance, and dissemination of their information, since they are not federal government employees as that term is understood by the Government.

61. Plaintiffs are therefore entitled to relief in the form of: (1) an injunction prohibiting OPM from collecting or storing any information about any individual with a Government email address in the GWES or any linked systems until it has conducted the necessary legally sufficient PIA; and (2) a court order directing OPM to delete any PII collected by those systems before OPM conducted the necessary legally sufficient PIA.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Jane Does 1-7, and all other similarly situated individuals, pray that this Court:

(1) Declare and find that the purported Privacy Impact Assessment published by the Office of Personnel Management on 5 February 2025 is not legally sufficient under the E-Government Act of 2002 by way of the APA, that this violation was intentional and/or willful, and that the publication of this purported PIA was done for pretextual reasons for the purpose of misleading this Court and arguing that the case is moot;

(2) Declare and find that OPM's failure to conduct and publish a legally sufficient PIA for the GWES and any linked systems is a violation of the E-Government Act of 2002 by way of the APA, and that this violation was intentional and/or willful;

(3) Order OPM to promptly conduct legally sufficient PIAs about all such OPM systems prior to the collection of any PII using those systems;

(4) Order OPM to promptly delete any PII collected by those systems prior to conducting and publishing a legally sufficient PIA;

(5) Order preliminary and permanent injunctive and/or declaratory relief as may be appropriate;

(6) Award reasonable costs and attorneys' fees as provided in 28 U.S.C. § 2412(d), or any other applicable law;

(7) Expedite this action in every way pursuant to 28 U.S.C. § 1657(a); and

(8) Grant such other relief as the Court may deem just and proper.

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*