

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN FEDERATION OF GOVERNMENT
EMPLOYEES, AFL-CIO, *et al.*,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT,
et al.,

Defendants.

Case No. 1:25-cv-01237-DLC

**SECOND DECLARATION OF DAVID NESTING IN SUPPORT OF
PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION**

I, David Nesting, declare as follows:

1. I am over 18 years old and competent to give this declaration. This declaration is based on my personal knowledge, information, and belief.

2. In addition to the materials I reviewed for my first Declaration, which includes the public portions of the Administrative Record, I have now also reviewed the publicly-filed materials filed by Defendants in Opposition to Plaintiffs' Preliminary Injunction.

3. For the reasons stated in my first declaration, and upon review of Defendants materials, I maintain my opinion that there is a risk of imminent, irreparable harm from DOGE's actions.

A. Inherent threats associated with administrative access.

4. As the government's motion confirms, on January 20, 2025, the DOGE officials directed that they be given "admin" access to three different IT systems, each of which contain

personally identifiable information of millions of government employees and others. *See* Document 51-1 at 32 (email from Charles Ezell); Document 64-1 at 25 (Teams message from Amanda Scales). They were granted that access.

5. As an example, according to publicly-available documentation on the USA Staffing system¹, the Office Administrator role has broad permissions to access applicant and other data stored in the system. While it was not specified what “admin” meant in the emails requesting or granting access to these systems to DOGE personnel, it’s implausible to me that this does not grant access to personal data held by these systems.

6. I saw nothing to suggest this access was being tailored to any of these individuals or the particular work that they planned to do with that access, which is the normal process at OPM and other agencies to comply with their obligations under the Privacy Act.

7. To the contrary, it appears that the approach was to grant these individuals as much access as possible as early as possible, in case they “might need to move quickly.” *See* OPM-000029.

8. This is consistent with Mr. Hogan discovering in March, after press coverage and the filing of this suit, that most of those people had not used the access they were granted.

9. Granting people excessive privileges that they don’t intend on using is a violation of the Principle of Least Privilege. *See also* Lewis Decl. ¶¶ 12–16.

10. Similarly, Mr. Hogan’s description, which shows the same people being granted administrator access to three different systems at OPM, violates the Principle of Separation of Duties. *See* Schneier Decl., ¶¶ 29–35.

¹ <https://resourcecenter.usastaffing.gov/hc/en-us/articles/35074300744340-USA-Staffing-Permission-Profiles>

11. Despite Mr. Hogan's assertions, what he describes is inconsistent with the Principle of Least Privilege or the Principle of Separation of Duties, both of which are codified by NIST. See NIST Special Publication 800-53 Rev. 5, controls AC-5 and AC-6.

12. The wholesale assignment of these privileges to people who did not need them—demonstrated by their lack of access—creates a security and privacy hazard. Regardless of whether the individuals given this access exercised it, the fact that the privileged credentials were issued in the first place creates risk.

13. The risks are not limited to abuse committed by the authorized holders of the privileged access; credentials can be stolen or compromised and abused. The Principle of Least Privilege is also about minimizing the “attack surface” of an agency by minimizing the number and value of targets.

14. That the Defense's declaration contends that the access was originally appropriate underscores that the Government does not understand or appreciate the risks that the Privacy Act was created to mitigate, and telegraphs that they could easily decide to repeat the same decisions at any time. For this reason I support enjoining them until the Court can ascertain whether their behaviors comply with the law.

15. The government emphasizes that being granted administrative access to OPM systems did not “necessarily” mean that the DOGE agents had full “god mode” powers.

16. The Privacy Act is concerned only with access to personally identifiable information contained within these systems. While having greater levels of access creates greater risks for data integrity, authenticity, and confidentiality, establishing that the level of administrative access they were granted is less than “god mode” does not mean that the concerns no longer exist.

B. My experience at OPM as Deputy CIO.

17. To the best of my recollection, at no time during my tenure as Deputy CIO at OPM did I have blanket administrative access—or *any* non-public access—to the personal data in OPM’s data systems. I can recall only a single data system at OPM I had privileged access to, for a single, small, and time-limited project that required extracting data from that system.

18. For me to possess administrative access over OPM’s data systems for no reason other than my role as Deputy CIO would have been an egregious violation of good security practices, as I had no need for any special access or privileges on these systems, even in a position of authority over the teams operating them.

19. That the defendants’ attorneys find it “curious” that this statement wasn’t present in my original declaration, and go on to assume that the reason for this can only be an awareness that “by virtue of that position the need is readily apparent” betrays a fundamental failure to understand these basic security principles, what Separation of Privileges truly means, as well as the responsibilities the Government has under the Privacy Act.

20. These failures are why I have grave concerns that basic security practices as mandated under the Privacy Act aren’t simply being neglected; the defendants are seemingly unaware of what those practices are, and consequently appear incredulous of their value.

21. I observe that Mr. Hogan himself was granted sweeping “Global Admin” privileged access to OPM systems. *See* Document 64-1, at 9–10. While this is consistent with the defense’s incredulity that I didn’t do something similar during my tenure, it underscores that the administration is prioritizing absolute control over risk management or compliance with the law.

C. Defendants still show no need for the level of access granted.

22. Defendants have made no showing of “need” for the level of access granted to

DOGE personnel. They simply assert that the President's Executive Order, which they admit mostly replicated longstanding requirements that OPM take steps to modernize its systems, somehow required immediate administrative access for seventeen DOGE employees for three separate large OPM database systems containing the sensitive personal data of millions of people, and currently requires administrative access for four people for one database.

23. But that summary assertion does not prove a "need," for access to personnel data, much less provide sufficient documentation of it.

24. As I note above, the government has provided a few top-down emails and references to names in a spreadsheet, and a long list of systems that they required administrative access to. It included one email that admitted that these people didn't need access, but might for some unspecified future "emergency."

25. These were *blanket* access grants, which is the opposite of the Privacy Act's requirement that access be granted selectively based on a need.

26. That does not necessarily mean that each individual person and each individual access requires documentation, but it does mean significantly more than simply stating the goal of "modernization" or "increasing efficiency," or even "emergency," without demonstrating how access to sensitive personal information is "needed" to reach that goal.

27. As I explained in my prior Declaration, designers and developers who are tasked with building, improving and modernizing a system do not require special privileges within governmental IT systems. *See* Nesting Decl. ¶¶ 12–19.

D. "System changes" are alarming and suspect.

28. Mr. Hogan separately confirms that before March 6, 2025, four DOGE individuals were granted "administrative access" to the USA Staffing system so that they could

make unspecified “system changes” to automate hiring/onboarding and job posting processes and develop a data-driven hiring plan.” Memo. in Opp. at 8, citing Hogan Decl. at 14.

29. This also does not demonstrate a “need” to access personal data.

30. Moreover it is deeply concerning. Without further specificity, it is impossible to know what these “system changes” were, whether they involved access to or manipulation of personal data stored in these systems, which include information about prospective hires.

31. The government points out that, with respect to OPM, the Government Accounting Office (“GAO”) has previously identified sixteen “priority recommendations” for improving OPM’s operations involving, among other things, “preventing improper payments,” “improving payroll data,” and “strengthening IT security and management.”

32. However the government provides no information much less a justification for why these goals require access by the specific DOGE agents, or any DOGE agents at all.

33. In fact, it seems unlikely that the few DOGE personnel would have the skills to accomplish these differing goals. For instance, you might want a data scientist working with anonymized data, an IG inspector actually investigating individuals for fraud, a cybersecurity specialist who only is exposed to system data incidentally, and a system administrator who—because of separation of privileges—is doing *none* of those things.

34. The government also notes, correctly, that before January 20, 2025, the USDS was engaged in modernization activities at agencies across the government. *Id.* at Fn. 19. As I noted in my previous declaration, these activities were commonly accomplished with no blanket, privileged access to personal data in the associated systems. And neither the government nor Mr. Hogan describe what DOGE was doing differently that required administrative access.

35. To be clear, I am in favor of modernization and have devoted much of my career

to this goal. My argument isn't that modernization is bad, or inherently insecure, or inherently a violation of the Privacy Act. It's that the people modernizing systems do not need access to the personal data contained in those systems, especially at the start of their modernization activity.

E. Security concerns persist.

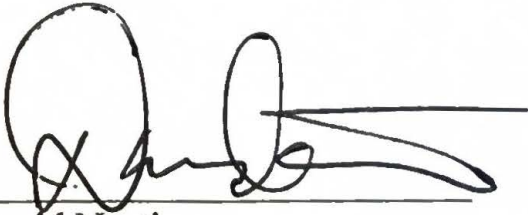
36. Mr. Hogan details how OPM uses some Microsoft tools such as Entrata ID to secure its system from unauthorized use. *See, e.g.*, Hogan Decl. at ¶¶ 5, 7–9. This misses the point I and the other experts are making. Our concerns are about the decision to grant sweeping authorization to access personal information in OPM systems, and what their intentions are for those granted that authorization, not how secure the systems are once people are authorized.

37. This scenario raises serious concerns that Defendants are using “modernization” as a pretext for other goals, such as centralizing all government data. This is in direct conflict with the Privacy Act.

38. My concerns were heightened by another Presidential EO 14243², as well as this news article: Hannah Natanson, et al., *DOGE Aims to Pool Federal Data, Putting Personal Information at Risk*, WASH. POST, May 7, 2025, <https://www.washingtonpost.com/business/2025/05/07/doge-government-data-immigration-social-security/>

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 22, 2025.



David Nesting

² <https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/>