

**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

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

I, David Nesting, declare as follows:

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

2. I am an expert on both government and industry practices for building or modernizing IT systems, including those that operate on private information, with direct experience at the Office of Personnel Management as Deputy Chief Information Officer and Deputy Chief Data Officer, as well as experience in several other government agencies and in private industry.

3. I have reviewed the declaration of Greg Hogan, and the Defendants' Memorandum of Points and Authorities in Support of Dismissal.

4. Based upon my experience, and as explained further below, I believe that there is a risk of imminent, irreparable harm from DOGE's actions.

My Credentials and Experience

5. My CV is attached as Exhibit A.

OPM Direct Experience

6. I served as the Office of Personnel Management's Deputy Chief Information Officer from February 2019 to August 2021 (2 years, 7 months). In this role I managed OPM's IT organization and provided oversight of its IT systems and cybersecurity program. I was additionally a member of OPM's agency-wide risk management team.

7. I also served as one of OPM's Deputy Chief Data Officers, working alongside OPM's Chief Privacy Officer. In this role I became an expert on OPM's data systems, technologies, and practices.

Other Relevant Experience

8. After my service at OPM, I served as an Artificial Intelligence and Cybersecurity Specialist within the Office of the Federal Chief Information Officer at the Office of Management and Budget between February 2024 and February 2025. In this role I advised on IT modernization with an emphasis on AI, and built internal AI governance and infrastructure to allow for research and development and to create paths forward for future AI systems.

9. Before my work at OPM, I served as a Site Reliability Engineer within the United States Digital Service from 2014-2019, and Director of Engineering from July 2017 to December 2018. In this capacity I personally participated in IT modernization activities at the Departments of Health and Human Services, State, Education, Defense, Justice, as well as the General Services Administration, along with other agencies.

10. Prior to Government Service, I was a Site Reliability Engineer at Google from 2007-2014. I was directly responsible for the privacy-protecting data anonymization, deletion, and litigation hold systems.

Principles for Sensitive Data in Large Database Systems

11. Industry and government best practices for systems including sensitive data are quite similar, and both include strict access controls, sometimes called the Principle of Least Privilege. The basic guiding principle here is to keep the number of people who have access to sensitive data to an absolute bare minimum. This means clearly separating the roles that require access to the data from the roles that do not.

12. These roles typically include (a) the system **administrators, or operators**, who are tasked with deploying new versions of the system, ensuring the system is working normally, and is secure; and (b) the system **designers and developers**, who are tasked with building, improving, and modernizing the system.

13. By defining roles in this way, only the administrators actually require special privileges within an IT system, and then only some of them for some purposes, as I explain further below. This smaller group can then be held to a higher standard of vetting, and the task of keeping the systems secure becomes easier with a limited set of people with privileged access and behaviors to monitor.

14. Meanwhile, the set of designers and developers, tasked with improving the system, can operate with significantly more flexibility, with a more relaxed security posture, and with very little concern that any experimentation or testing they conduct during development can put real data at risk.

15. Put another way, a team trying to modernize bank vaults doesn't need to have access to the contents of everyone's vaults.

16. The DOGE personnel have been given a mandate of increasing efficiency and modernization, which makes them developers, not administrators of the systems.

17. When developers need to understand a system's data model, so that they can

improve it or build other systems intended to interoperate with it, that data model can be described without revealing the private information contained within the system.

18. When developers need to understand how data is used, for instance to understand data quality, they can rely on privacy-preserving techniques like replacing the original private information with randomized tokens. They can then freely share or incorporate that data into analysis or improvements without ever risking the private data the analysis is based upon.

19. For more specialized data analytics, purpose-built tools, queries, “views”, and filters can be developed to answer complex questions about the data without requiring that the developer or analyst asking the questions ever have complete access to the data itself. These tools can be reviewed by privacy experts to verify they do not create additional risk, and installed or run by qualified, authorized administrators.

It is Not Necessary to Have Full Administrative Access or Access to Personnel Information in Order to Modernize Government Systems.

20. I have applied these principles to governmental systems multiple times.

21. I know from long experience that it is not only possible, but vastly preferable to modernize IT systems without access to the data. Below are some examples from my personal experience.

22. With the Department of Health and Human Services, I participated in a resiliency and modernization activity involving the Affordable Care Act (ACA) systems, which contained personal information of everyone who has applied for or received benefits online through the ACA. In this capacity I acted as incident response lead and made recommendations for system improvements and provided troubleshooting and other tooling.

23. At no time did I have access to personal information contained within ACA systems I modernized. All requests for changes or information were made through a limited set

of authorized administrators.

24. With the Department of State, I participated in a modernization activity involving the Consular Consolidated Database, a system used for processing visas and containing the associated personally identifiable information. This began as an incident response effort but did include a series of modernization recommendations.

25. At no time did I request or receive access to personal information within these State systems to produce our recommendations. All requests for information were handled through a limited set of authorized administrators.

26. At State, I also participated in a modernization activity to improve the way that people obtain status updates online regarding their visa applications. This system contained the personal information of every person with a pending visa application. This activity resulted in code changes that were made to the system.

27. At no time did I have direct access to any actual personal data during this activity. We tested our changes using test or synthetic data.

28. Also at State, I participated in a modernization activity involving the U.S. Refugee Admissions Program's (USRAP) case management system, which contained the personal information, including results of security vetting and interviewer notes, of all potential refugees and their families. During this activity we made thousands of code changes and other improvements to these systems.

29. We did not require access to any personal information in order to complete this USRAP activity. Testing and integration was performed by a limited set of authorized administrators.

30. While not a modernization activity, at the Department of Defense, I participated

in an incident response activity involving the Army's HR systems, which included the personal information of Army personnel. The output of this activity was an incident post-mortem with recommendations.

31. As with modernization activities, no access to personal information was needed for this Army activity and at no time did I need or use access to the personal information contained within these systems.

Congress's Choice in Requiring a High Security Approach in The Privacy Act is Vital to Protecting Past, Current, and Prospective Federal Employees and their Families

32. Private sector and public sector interests are vastly different and require different risk tolerances and risk management. I note this because, having experience in both sectors, I am concerned that the DOGE officials seem to only have limited, private sector experience and are not acting consistent with an understanding of the differences.

33. In the private sector, a company's obligations and customer risk are described through terms of service and privacy policies. This, at least theoretically, gives customers a chance to assess the risks of sharing their sensitive data.

34. OPM's data systems contain some of the most sensitive information in the US government, including personnel data on past, current, and aspiring federal workers, data on their and their families' health care, as well as data on annuitants receiving retirement benefits, which can include family members as well.

35. People cannot opt out of having their personal data in OPM systems or even meaningfully assess the risk in sharing it. The public is entirely reliant on good faith implementation of the Congressional protections in the Privacy Act, which is vital to ensuring the information contained in these systems is adequately protected, and to ensuring the federal government remains a good steward of the personal data the public is required to entrust with the

government.

Inadequate Vetting Nullifies Privacy Act Protections and Agency Privacy and Cybersecurity Policy

36. The Privacy Act, the Federal Information Security Management Act (FISMA), and the associated agency privacy and cybersecurity programs, policies and processes, rely on agencies adequately vetting employees to ensure they meet minimum suitability requirements to maintain the public trust, including a good faith determination that no disqualifying factors exist, such as past criminal or dishonest conduct, financial irresponsibility, financial conflicts of interest, a divided loyalty with or coercive influence by a foreign nation, or subversive interests.

37. Based upon my experience and the public information I have reviewed, I do not believe the DOGE personnel that have obtained, or are seeking, full administrative access to OPM's IT systems have been sufficiently vetted.

Inexperience in Complex Governmental Systems Can Lead to Dangerous Approaches

38. I understand how people without experience with complex public sector databases containing sensitive personnel information might not appreciate the risks they create by failing to follow security best practices in their efforts to modernize and fight fraud in systems.

39. As a former Silicon Valley technologist who found himself applying my expertise to improve government IT, I am deeply sympathetic to the feeling that it is more difficult to fulfill a modernization vision within the constraints and guardrails imposed by law and policy.

40. But the risks are very significant and underlie the reason that the Privacy Act as well as the standard practices applied by governmental agencies in approaching modernization of systems require approaches like those I explain above.

41. With legacy systems such as many of those at OPM, the truth is that if a system is

broken or data corrupted due to inexperience and carelessness in accessing it, it simply might not be possible to fix it. Many systems at OPM are based on very old technologies, and people only exposed to more modern IT systems are unlikely to fully understand the design complexity or other factors needed to both avoid harm and repair the systems after they've been harmed. Sensitive information stored in them can be lost, altered, or compromised in ways that cannot be remedied.

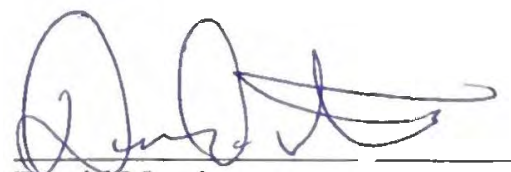
Failure of OPM's IT Systems is a National Security Risk

42. The harm caused by the failure of OPM IT systems to perform their function is also immeasurable. As an example, nearly three million households are reliant on regular payments of federal retirement annuities. The disruption of just these payments alone is, in my view, a serious national security risk in addition to creating a tremendous personal risk for those who depend on those payments.

43. Until the public—through the actions of this Court—can be assured that the concerns I've discussed above are being effectively managed, the risks to the American people are imminent, clear and present and I am supportive of the need for emergency intervention to avoid them.

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

Executed on April 22, 2025.


David Nesting