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 ANN LEWIS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

1. I, Ann Lewis, under 28 U.S.C. § 1746, declare that the following statements are true and correct to the best of my knowledge and belief: 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 have worked in the technology industry for more than 20 years, with the past 12 years spent in various leadership roles. I have a degree in computer science from Carnegie Mellon University and have authored numerous articles on tech, software engineering, and modernization of government systems. My experience includes serving as Chief Technology Officer for both a national nonprofit organization and a business advisory firm, and as Senior Advisor for Technology and Delivery for the U.S. Small Business Association.

3. Most recently, I served as the Director of Technology Transformation Services ("TTS") within the U.S. General Services Administration. TTS applies modern methodologies and technologies to government systems. TTS's primary goal is to help agencies use technology

to make their services more accessible, efficient, and effective. As Director, my role was to lead a team of about 700 technologists in implementing industry best practices and modernizing government systems with modern applications, platforms, processes, personnel, and software solutions.

4. More information about me and links to my many writings and talks about implementing tech industry best practices in government are available at annlewis.tech. My Curriculum Vitae is attached as Exhibit A.

5. From long experience in the field, I am familiar with the best practices, risks, and costs associated with data sharing. My roles in government service specifically provide me insight on challenges in federal data sharing, including the heightened national-security implications associated with handling federal data.

6. I have read public reporting and reviewed the public record in this matter, including the declarations submitted that discuss the level of access Department of Government Efficiency (DOGE) personnel have within the OPM systems.

7. I understand that several DOGE personnel have "root access" (sometimes called "administrator access" or more colloquially "God Mode") to all Office of Personnel Management (OPM) technology systems. It is my professional opinion, to a reasonable degree of professional certainty, that DOGE's access to sensitive OPM information is unnecessary for the purposes expressed by DOGE—and ignores vital security protocols.

8. Administrator access is defined by the Cybersecurity and Infrastructure Security Agency (CISA) as "elevated system privileges that allow a user to install software, change security settings, manage accounts, and configure system settings." Administrator access is generally understood by the tech industry and by IT professionals as the highest and most

powerful level of access to any system. Administrator access to a system gives the user the ability to create, read, update, and delete/destroy any data and code within the system. This can include modifying or deleting website content, reading another user's emails, sending email on behalf of every user, adding or removing code to change the behavior of the system, granting other users any level of access (including additional administrator access), revoking access from any user, updating data, deleting data, and extracting all data including sensitive data and the Personal Identifying Information of users. Administrator access not only allows the user to delete critical data owned by and affecting other users, but it also allows the user to disable, modify, or destroy data backups and audit trails used to conduct forensic analysis, and it allows the user to take system components fully offline.

9. Administrator access is a significant responsibility for any individual, especially within the context of government systems. Each additional individual in possession of administrator access heightens the risk of harm that could occur. When numerous individuals with low-level familiarity with specialized government systems are given administrator access, the risk of harm becomes significantly more severe.

10. Through my experience leading TTS and in data management, I became aware of the Federal Information Security Management Act (FISMA), and the National Institute of Standards and Technology's SP 800-53 Security and Privacy Controls for Information Systems and Organizations.

11. FISMA is a law designed to protect government information and operations, and NIST 800-53 is a cybersecurity framework that provides a comprehensive set of security and privacy controls for federal information systems and organizations. These are standard, well-settled frameworks within which government technologists operate.

12. One framework that all of these tools agree upon is called the "Principle of Least Privilege." This is a fundamental cybersecurity concept and best practice that states that users should have only those minimum rights, roles, and permissions required to perform their roles and responsibilities. This protects access to high-value data and critical assets, and helps prevent unauthorized access, accidental damage from user errors, and malicious actions. The Principle of Least Privilege applies to all aspects of system and software management, including access control, user roles in systems, software, databases, applications, service accounts, APIs, and automated processes.

13. FISMA § 3544 (Management of Information Security Risk) codifies this principle, stating that the head of each agency shall be responsible for complying with this subchapter and related policies, procedures, standards, and guidelines, including information-security standards promulgated under § 11331 of Title 40. And § 11331 of Title 40 states that the National Institute of Standards and Technology (NIST) prescribes standards and guidelines pertaining to federal information systems.

14. NIST 800-53 AC-6 lists The Principle of Least Privilege as a key security control: https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

15. NIST 800-53 defines "administrator access" as a privileged role that allows users to perform security-relevant functions not typically available to ordinary users.

16. Granting DOGE engineers administrator access to all OPM systems violates the Principle of Least Privilege, and at odds with cybersecurity best practices federal agencies are required to follow, as specified by NIST SP 800-53.

17. Granting administrator access to any system creates new fraud vectors and new cybersecurity risks. As a technology professional and former government employee, I believe that **every cybersecurity risk is also a national-security risk**. Specifically, every hacker in the world now knows there are a small number of people new to federal service who hold the keys to access all U.S. government payments, contracts, civil-servant personal information, and more. When sensitive data exists within government-security boundaries, we can audit and track it. But after that data leaves those boundaries, we have no way to know where it goes or what it is used for. Anyone with administrator access to a system can not only export all data but can also disable tracking and audit logging critical to forensic analysis.

18. The costs of cybersecurity incidents are high, not just to the agency or breached system, but especially to the users and former users whose Personal Identifying Information is leaked, shared without their permission, or stolen. Stolen PII is not easily changed and usually cannot be clawed back. So the damage to the individual can last a lifetime. A user's stolen PII can be sold and used for fraud, scams, harassment, blackmail, and identity theft.

19. It's my understanding that DOGE's stated objective is "modernizing federal technology and software to maximize efficiency and productivity" and specifically, "improv[ing] the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems." https://www.whitehouse.gov/presidential-actions/2025/01/establishing-and-implementing-the-presidents-department-of-government-efficiency/.

20. It is my professional opinion, to a reasonable degree of certainty, that not only does DOGE not have a "need" for broad administrative access to multiple government systems to achieve the stated objectives of the Executive Order, but that the Executive Order objectives

will not be met by DOGE's actions, even apart from the security risks they create. "Federal technology and software" include thousands of instances across hundreds of agencies of "government-wide software, network infrastructure, and information technology (IT) systems," each with separate databases, separate infrastructure, and separately managed teams and access control policies. The small team of DOGE-affiliated employees who are implementing it (and sidelining other, more experienced staff) simply cannot modernize thousands of systems simultaneously. Government implementation and modernization work for each system generally involves public-private partnerships where vendor teams perform most of the implementation work, and agency teams largely manage this work, rather than performing it directly.

21. To accomplish this kind of work at all, much less to observe the necessary security to protect this large number of complex systems and the people whose sensitive data is housed in them, requires careful management. It involves coordination across many teams, reviewed and approved by the agency office of the CIO to allow large groups of workers to collaborate securely.

22. Moreover, this careful, secure coordination already happens regularly. DOGE's stated objectives are not new. Thousands of people across agency and vendor teams are already engaged in modernization and implementation work across all these systems.

23. The way DOGE is operating is inconsistent with both the need to successfully modernize these systems and to do so securely. Preemptively granting DOGE operators administrator access to all systems is not just useless, it's a security risk.

24. It is also inconsistent with how the private sector implements modernization and access management. For example, large global consumer technology companies face continuous fraud risks they must combat. These companies have thousands of teams managing separate

systems and databases. They do not fight fraud by creating small strike teams or granting small teams access to all data. They also do not attempt to consolidate all data together first. These companies invest in robust, long-term anti-fraud capabilities, share data across teams via secure APIs, perform continuous monitoring of fraud signals, and adopt adaptive risk modeling. Software engineers and software engineering leaders with experience in nationally or globally scaled enterprise software companies know this, and know how to effectively balance security, speed of delivery, and fraud concerns. That is not what DOGE is doing.

25. From my long experience in the tech industry, I know that proper adherence to standard security protocols is not a rational impediment to modernization, efficiency, and productivity. To the contrary, ignoring the risks that foundational security protocols address only jeopardizes DOGE's stated goals.

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

Executed on the 22nd day of April, 2025.

Ann Lewis