

**IN THE UNITED STATES DISTRICT COURT
FOR THE 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. 25-cv-1237-DLC

DECLARATION OF PERRYIN ASHMORE

I, Perryn Ashmore, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury, as follows:

1. I am currently employed by the United States Office of Personnel Management (OPM), as the Acting Chief Information Officer (CIO) of OPM, and have served in that role since September 2, 2025, replacing the previous CIO, Greg Hogan, on that date. Prior to serving as Acting CIO, I served as the Deputy Chief Information Officer of OPM from May 18, 2025, through September 1, 2025. Prior to that, I served as a Senior Executive with OPM Human Resources Solutions from November 2023 to May 2025. I also previously served as the CIO of the U.S. Department of Health and Human Services from September 2020 to May 2021, and have decades of experience working in various roles within the federal government.

2. I make this declaration based on my personal knowledge and on information contained in OPM's files, as well as information provided to me in the course of performing my

duties, including information provided by OPM's Chief Information Security Officer (CISO), and OPM's human resources (HR) department.

3. The purpose of this declaration is to (i) provide information concerning OPM's updates to its access control policies, (ii) provide relevant information concerning certain OPM employees, and (iii) enclose additional documents supplementing the administrative record in this matter.

OPM's Updated Access Control Policy

4. On July 18, 2025, OPM instituted, on an interim basis, certain additional protocols to be followed before granting new access to PII contained in OPM data systems to (1) any U.S. DOGE Service (DOGE) employee, contractor, or detailee, or (2) any OPM employee, contractor, or detailee hired after January 20, 2025, who requires access for the primary purpose of working on an initiative or project involving DOGE. *See* ECF No. 140-1.

5. In November 2025, I reviewed these interim access protocols with OPM's Senior Agency Official for Privacy to determine whether they should remain in place. We determined that OPM should formalize access protocols and clarify that they apply to all new employee and contractors requiring access to OPM systems containing PII, and accomplished this by making them a permanent part of OPM's Cybersecurity and Privacy Policy, which was undergoing other, unrelated revisions.

6. On November 18, 2025, OPM Director Scott Kupor formally approved OPM's updated Cybersecurity and Privacy Policy, and on November 20, 2025, an email announcing its official release along with a link to the entire policy hosted on OPM's intranet was sent to all OPM employees. *See* Ex. A.

7. As pertinent to this case, the updated Cybersecurity and Privacy Policy includes the addition of Section N to the Access Control family, which includes the expanded access protocols which shall be used for new employees and contractors requiring access to OPM systems containing PII. *See* Ex. B, Excerpt of OPM Cybersecurity and Privacy Policy, dated November 18, 2025, Section 3 – Access Control. As outlined at Section N, before an individual is provided with access to an OPM system or systems containing PII, the system owner (SO) must take the following steps:

- i. Confirm with CISO [the Cybersecurity Information Officer] that the person has completed Cybersecurity and Privacy Awareness training and completed [the] Rules of Behavior acknowledgement which are included as part of the training.
- ii. Confirm with CHCO [the Chief Human Capital Officer] that the individual has been properly appointed or detailed.
- iii. Confirm with FSEM [Facilities, Services, and Emergency Management] that the individual has been appropriately vetted and they have been cleared for entrance on duty.
- iv. Confirm with SAOP [Senior Agency Official for Privacy] that the above steps have been taken, provide an explanation for need to access the system(s), and receive written approval from the SAOP that the access fits within the “need to know” criteria of the Privacy Act.

No “DOGE Agents” Currently Have Access to PII of Plaintiffs in OPM Data Systems

8. In conjunction with OPM’s CISO and OPM’s database administrators, I have verified that no individuals falling within the category of “DOGE Agent,” as defined in the Court’s preliminary injunction order, currently have access to PII of plaintiffs in this matter in any OPM data systems. *See* ECF No. 148 (OPM’s revised report provided in response to the Court’s preliminary injunction order).

9. The above verification process was delayed beyond November 25, 2025, due to OPM’s database administrators identifying certain relevant permissions which had been granted to OPM-3 in January 2025. As explained in detail below, those permissions did not allow

OPM-3 to access PII in the relevant OPM data system. However, in order to ensure the accuracy and completeness of this submission, OPM required additional time to thoroughly review those permissions, validate underlying assumptions, and confirm all factual data prior to filing.

10. During the verification process, OPM's database administrators determined that while OPM-3's front-end "Web Admin" access permission to the USAJOBS application was previously removed in February 2025, he had been separately added in January 2025 to two SQL (Structured Query Language) access groups for the USAJOBS application that in conjunction could potentially allow access to PII stored in that application through a SQL viewer. However, after a thorough investigation, OPM confirmed that although he was a member of these groups, he was never provided with additional required elements necessary to access PII stored in the USAJOBS application through a SQL viewer—all of which must be obtained directly from an OPM database administrator. These elements include: (i) OPM-approved SQL viewer software; (2) access to the USAJOBS server name and port information; and (3) access to the Azure secure database connection string for the USAJOBS application. Because OPM-3 lacked these necessary elements, he could not start the connection process and therefore could not reach or view PII stored in the USAJOBS application. OPM's CISO further confirmed by reviewing Security Information and Event Management logs and firewall logs that there were no direct access attempts or any successful access by OPM-3 to the USAJOBS database. OPM removed OPM-3 from these SQL access groups on November 26, 2025.

11. I am no longer in the direct supervision chain of OPM-2, who is currently being supervised by the Director of OPM. *See* ECF No. 148, paragraph 7.c.

12. On May 13, 2025, OPM determined that OPM-4 was no longer with the agency, and his OPM network access credentials were removed on May 14, 2025.

Supplement to the Administrative Record

13. I hereby certify, to the best of my knowledge, that the supplemental administrative record consists of the accompanying documents attached hereto as Exhibit C, as listed in the enclosed index.¹

Dated: December 5, 2025
Washington, D.C.

**PERRYN
ASHMORE** Digitally signed by
PERRYN ASHMORE
Date: 2025.12.05
08:10:37 -05'00'

Perryn Ashmore

¹ Defendants maintain that the Complaint does not challenge any final agency action and reserve their right to argue in further proceedings in this case, including in any subsequent appeal, that the Administrative Procedure Act does not provide for review.