

EXHIBIT 43

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

AFL-CIO, et al.,

Plaintiffs,

vs.

Case No. 1:25-cv-339-JDB

U.S. DEPARTMENT OF LABOR, et al.,

Defendants.

DECLARATION OF JOHN DOE

I, John Doe, of over eighteen years of age and sound mind, declare under penalty of perjury under 28 U.S.C. § 1746 that the following is true and correct to the best of my knowledge:

1. Until 2025, I served as a Digital Services Expert at the United States Digital Service, now the United States DOGE Service. I am filing this declaration pseudonymously due to concerns I have about potential retaliation against me for my participation in this matter. Counsel for Plaintiff is aware of my identity.
2. For several years in my capacity at USDS, I partnered with the Department of Health and Human Services and the Centers for Medicare and Medicaid on several critical technology and data systems projects.
3. My experience in this role included assisting and advising departmental leadership with tasks involving the analysis of sensitive data and the implementation of data systems at HHS and CMS.

4. I have reviewed selected filings and factual materials in the above-captioned case, including the Plaintiffs' Brief in Support of Their Motion for a Preliminary Injunction, ECF No. 80-1, Defendants' Objections and Responses to Plaintiffs' Requests for Expedited Discovery, Including Supplemental Responses, ECF No. 80-5, Excerpts of the Deposition of Jennifer Wendel, ECF No. 80-15, Defendants' Memorandum in Opposition to Plaintiffs' Motion for a Preliminary Injunction, ECF No. 82, and the April 29 Declaration of Jennifer Wendel, ECF No. 82-1.

5. In reviewing those materials, I have familiarized myself with the breadth of access that has been granted to DOGE to access sensitive systems housed at HHS and CMS.

6. During my tenure, I was aware of no other individual detailed to or employed by HHS that had active concurrent access to as many sensitive databases as DOGE Team member Luke Farritor. This degree of active concurrent access across many disparate and unrelated databases for detailees from outside of HHS, is to the best of my knowledge without precedent.

7. I am also aware from these filings that a member of the DOGE Team has been granted access to the Unaccompanied Children (UC) Portal in order to identify waste, fraud or abuse. *See* ECF No. 80-15, 46:19-47:49:9. For instance, HHS indicated that UC Portal access may help identify waste, fraud or abuse because it contains "employment information and sponsor information" including "financial account information" that could help determine if "payments to sponsors were legal and legitimate." *Id.* 48:4-48:25.

8. The UC Portal is a highly sensitive system of record that contains Personally Identifiable Information (PII) and medical records about children. As the Privacy Impact Assessment (PIA) for this system details, the information collected in this system includes “[p]hotograph[s]” of children “at various ages and/or locations,” the children’s “Medical Notes (examples: vaccinations, medications, doctor visit details),” “Biometric Identifiers,” and an additional “2,000+ data elements”.¹

9. Some children whose information is stored in the UC Portal have been victims of abuse or sexual violence, either before entering the United States or while in federal custody. Case notes containing information about those experiences are stored in the UC Portal.

10. The database also contains sensitive information about children’s sponsors, including their social security numbers, financial account information, employment status and income, tax returns, and other highly-sensitive records.²

11. I am not aware of any payment information in the UC Portal that would be relevant to identifying financial waste, fraud, or abuse of the kind described by the Executive Order issued on February 26, 2025. While HHS discussed “payments to sponsors” as a potential vehicle for financial fraud, I am not aware of the federal government making any payments to sponsors related to the children in their custody nor

¹ U.S. Dep’t of Health and Human Servs. *Privacy Impact Assessment* (2024), <https://www.hhs.gov/sites/default/files/acf-unaccompanied-children-portal-r.pdf>, archived at <https://perma.cc/43WL-SEKQ>.

² *Id.*

am I aware of any such data being contained in the UC Portal or included in the UC Portal PIA.³

12. As such, it is unlikely that an employee detailed to HHS would need access to all of the information contained in the UC Portal in order to identify financial waste, fraud, or abuse, especially since it contains highly sensitive PII about children, including photographs and medical records.

13. In my experience, HHS and CMS typically implemented the “principle of least privilege” when determining access to individuals’ sensitive data.

14. This industry standard information security practice seeks to protect the sensitive and confidential information stored by an entity by only granting users the minimum access to data that is required to complete a specific task or analysis.

15. This principle helps protect sensitive data not only from unauthorized access by government officials, but also reduces the cybersecurity risks to Americans’ data by minimizing the number of points of failure that might result in inadvertent disclosures to external parties, as well as minimizing the number of potential access points for hostile actors seeking to infiltrate government systems.

16. What HHS has described with respect to DOGE—providing blanket access to systems that contain individual records of highly sensitive PII without a clear and specific connection to identifying financial waste, fraud, or abuse—is incompatible with HHS’s typical practice of applying the “principle of least privilege” to protect American’s most sensitive data.

³ *Id.*

Executed this 1st day of May, 2025

/s/ John Doe