IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AMERICAN FEDERATION OF LABOR AND CONGRESS OF INDUSTRIAL ORGANIZATIONS, et al., Plaintiffs, v. DEPARTMENT OF LABOR, et al., Defendants.	Case No1:25-cv-00339-JDB Judge John D. Bates

DECLARATION OF RICKY J. KRYGER

I, Deputy Chief Information Officer for the U.S. Department of Labor, Ricky J. Kryger, being of lawful age, state the following:

1. I am the Deputy Chief Information Officer (Deputy CIO) for the Office of the Chief Information Officer (OCIO) for the United States Department of Labor (DOL) located in Washington, DC, and am responsible for Department-wide planning, implementation, modernization, cybersecurity, and operational information technology (IT) functions that support defined DOL mission responsibilities.
2. In my role as Deputy CIO, I am responsible for overseeing the Department's compliance with information security laws, regulations, and policies, including but not limited to Federal Information Technology Acquisition Reform Act of 2014 (FITARA), Federal Information Security Modernization Act of 2014 (FISMA), Modernizing Government Technology (MGT) Act, E-Government Act of 2002, Clinger-Cohen Act of 1996, Paperwork Reduction Act of 1995 (PRA), The Privacy Act of 1974, as well as the Department's information management policies and procedures for complying with restrictions on dissemination of information and data, such as Rule 6(e) of Federal Rules of Criminal Procedure on criminal penalties for giving access to, reviewing, and disclosing grand jury information, 26 U.S.C. § 7213 on criminal penalties for giving access to, reviewing, and disclosing federal taxpayer information covered by Internal Revenue Code

§ 6103, 18 U.S.C. § 1832 Trade Secrets Act, and 42 U.S.C. § 1320d-6 on criminal penalties in violation of HIPAA.

3. As Deputy CIO, I oversee OCIO's implementation of the Federal Records Act of 1950, and Section 508 of the Rehabilitation Act of 1973, which includes planning, directing, and supervising related work at DOL.
4. On January 20, 2025, Executive Order 14158 titled *Establishing and Implementing the President's "Department of Government Efficiency"* was signed establishing the Department of Government Efficiency to implement the President's Department of Government Efficiency (DOGE) Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.
5. The United States DOGE Service (USDS) employees have been tasked to support DOL's IT modernization efforts under the Executive Order including: (1) Providing software engineering, modern architecture and system design, project and team leadership, software delivery, security and site reliability engineering, data engineering, engineering management, and/or executive leadership expertise to champion and deliver modern technology; and (2) Being responsible for a wide range of activities including debugging, software testing, and programming. This includes quickly adapting and learning by problem-solving within legacy systems and organizational constraints while working collaboratively for rapid prototyping; (3) Assessing the state of current projects in agencies; planning or leading interventions where major corrections are required; (4) Assisting on IT projects including infrastructure, implementing safeguards to prevent fraud, and ensuring the integrity and success of these efforts; and (5) Championing data strategies and building interoperability with other agencies as well as internal and external stakeholders.
6. DOL intends to retain employees—who may be either direct DOL hires or employees detailed to DOL—to perform work required by the Executive Order.
7. A DOL supervisor will oversee employees carrying out the President's order, whether they are detailees or DOL employees. The supervisor will facilitate all support and oversight of the team's work and needs. The supervisor will also serve as the day-to-day point of contact for working discussions and personnel matters with USDS.

8. In accordance with my duties, guidelines have been established for employees carrying out the Executive Order, to protect the integrity of DOL's information systems. These guidelines include the following measures.

9. Relevant employees will provide 24 hours' notice before seeking access to each DOL IT system to allow DOL an opportunity to meet its obligations to ascertain and mitigate any conflicts of interest; establish confidentiality protocols; and identify and account for any system that may contain legally protected information. DOL systems can only be accessed where there is a need. Therefore, each employee requiring access to a process or a system with a valid need-to-know will review and sign all required access agreements for each process or system and complete a required request form to access DOL information systems.

10. The Request to Access DOL Information Systems form completed by the employee requires the establishment of a DOL Point of Contact (DOL POC); states the type of access requested; explicitly requests the names of any additional personnel the requester will grant permission to access the system and/or information, data or documents; notifies the requester in writing of the restrictions and sensitive information requirements of the specific IT system's sensitive information that may raise specific legal and or other concerns if accessed or disclosed; requires the requester to acknowledge a list of certifications relating to cybersecurity risk, the Privacy Act, and additional governing statutes or directives that DOL is responsible for complying with; and requires the requester to securely maintain and properly dispose of sensitive data when no longer needed for official purposes.

11. No user of the data, information, or documents from DOL information systems is allowed to share this data, information, or documents outside of DOL information systems without the specific approval of DOL OCIO.

12. DOL has the right to deny access to a system until all forms are fully executed; and employees engaged in carrying out the President's Executive Order, regardless of whether they are detailed or employed at DOL, cannot attempt to access a DOL process or system without first alerting the DOL POC and executing an access agreement. To access without proper approvals would subject the individual to potential criminal prosecution.

13. As of this date, there is one relevant worker who is now a DOL employee working solely on budget review. He has only been provided a standard laptop with standard office productivity applications, such as Outlook, Word, and Excel, but has not been given access

to any sensitive IT systems. No other relevant DOL employee or detailee has been issued equipment and/or has been given access to any sensitive IT systems.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed on this 13th day of February, 2025.

Ricky J. Kryger
Deputy Chief Information Officer
Office of the Chief Information Officer
U.S. Department of Labor
200 Constitution Ave, N.W.
Washington, DC 20210