# BRIEFLY...

**FY 2024 FISMA DOL INFORMATION SECURITY REPORT: CONTINUED IMPROVEMENT OF INFORMATION SYSTEM SECURITY PROGRAM**

## WHY WE DID THE AUDIT

Under the Federal Information Security Modernization Act of 2014 (FISMA), the U.S. Department of Labor (DOL) Office of Inspector General (OIG) is required to perform annual independent evaluations of the Department's information security program and practices.

This effort assesses the effectiveness of information security controls over information resources that support federal operations and assets, and it also provides a mechanism for improved oversight of information security programs. This includes assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

We contracted with KPMG LLP (KPMG) to conduct an independent performance audit on DOL's Fiscal Year (FY) 2024 information security program for the period October 1, 2023, through June 30, 2024. To determine the effectiveness of the program, KPMG evaluated and tested security controls in accordance with applicable legislation, guidelines, directives, and other documentation.

## WHAT WE FOUND

DOL's information security program continues to mature and improve; however, certain Cybersecurity Framework Functions are preventing DOL from maintaining an effective information security program. KPMG reported eight findings for DOL's information security program. The findings were identified in two of five FISMA Cybersecurity Framework Functions and in four of the nine FISMA Metric Domains. As a result, DOL's information security program was determined to be not effective, according to the Office of Management and Budget's guidance.

A security program is considered effective if the calculated score of the Cybersecurity Framework Functions is at least Managed and Measurable (Level 4). However, KPMG found weaknesses that demonstrated the information security program had not achieved a maturity rating of Managed and Measurable (Level 4) in three of the five FISMA Cybersecurity Framework Functions: Identify, Protect, and Recover. Specifically, KPMG identified deficiencies in the monitoring of DOL cloud service providers, multi-factor authentication enforcement, security training compliance, and the implementation of privacy-focused role-based training.

In addition, DOL's information security program did not fully adhere to applicable FISMA requirements, Office of Management and Budget policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines. For example, DOL's system-level security policies have not been updated to comply with NIST Special Publication 800-53, Revision 5.1, Release 5.1.1, Security and Privacy Controls for Information System and Organization. The OIG remains concerned that this prior year finding of compliance with the NIST publication remains outstanding. By not updating DOL's policies and procedures to be compliant, the Chief Information Officer is not taking necessary steps in mitigating IT risk for DOL.

## WHAT WE RECOMMENDED

KPMG made seven new recommendations to strengthen DOL's information security program. KPMG also determined 10 prior year recommendations were closed, 2 remain open, and 7 were not submitted for closure. DOL management generally concurred with the findings and recommendations; however, management disagreed with KPMG's conclusion that DOL's information security program was ineffective

## READ THE FULL REPORT

For more information, go to: https://www.oig.dol.gov/public/reports/oa/2025/23-25-002-07-725.pdf.