BRIEFLY...

FY 2025 FISMA DOL Information Security Report: Evaluation of DOL's Information 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 DOL'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 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) 2025 information security program for the period of October 1, 2024, through June 30, 2025. 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; however, certain insufficient cybersecurity controls are preventing DOL from maintaining an effective information security program. KPMG reported 14 findings for DOL's information security program. The findings were identified in 3 of 6 FISMA Cybersecurity Framework Functions and in 6 of the 10 FISMA Metric Domains. As a result, DOL's information security program was determined to be not effective, according to guidance from the Office of Management and Budget.

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 six FISMA Cybersecurity Framework Functions (Govern, Identify and Recover).

Specifically, KPMG found 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 standards and guidelines. KPMG noted deficiencies in the monitoring of DOL cloud service providers, multi-factor authentication enforcement, and the implementation of cybersecurity profiles. Furthermore, deficiencies were noted in user access provisioning and deprovisioning controls across systems within the DOL IT system portfolio.

As a result of the insufficiencies in DOL's information security program, DOL may face challenges in identifying and prioritizing cybersecurity risks effectively, which could lead to inadequate protection against cyber threats, increased vulnerabilities, and compromised data integrity. Furthermore, staffing vacancies and inadequate resources may result in a lack of oversight and effective operation of security controls and key IT processes, potentially impacting DOL's operational capabilities and compliance with federal cybersecurity mandates.

What We Recommended

KPMG made nine recommendations to strengthen DOL's information security program. KPMG also determined that eight prior year recommendations were closed, two remained open, and six were not submitted for closure by DOL management. DOL management concurred with the findings and recommendations.

Read the Full Report

For more information, go to: https://www.oig.dol.gov/public/reports/oa/2026/23-26-001-07-725.pdf.