U.S. Department of Labor
Office of Inspector General
Audit

BRIEFLY…

FY 2023 FISMA DOL INFORMATION SECURITY REPORT: MAKING IMPROVEMENTS TOWARD AN EFFECTIVE PROGRAM

December 06, 2023

WHY OIG CONDUCTED 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.

WHAT OIG DID

We contracted with KPMG LLP (KPMG) to conduct an independent performance audit on DOL's Fiscal Year (FY) 2023 information security program for the period October 1, 2022, through June 30, 2023. To determine the effectiveness of the program, we evaluated security controls in accordance with applicable legislation, guidelines, directives, and other documentation. Findings were also based on testing relevant security controls and targeted penetration tests.

WHAT OIG FOUND

KPMG reported seven findings for DOL's information security program within two of five Cybersecurity Framework Functions and four of nine FISMA Metric Domains, which resulted in determining DOL's information security program was not effective, according to guidance from the Office of Management and Budget.

Although DOL established and maintained its information security program, 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 Cybersecurity Framework Functions: Identify, Protect, and Recover. A security program is only considered effective if the calculated score of the Cybersecurity Framework Functions is rated at least Managed and Measurable (Level 4).

While the Office of Chief Information Officer (OCIO) has made improvements in its information security program from previous years, we identified areas of improvement required to reach a Managed and Measurable, or effective, program. DOL's information security program did not fully adhere to applicable FISMA requirements and other guidance, and KPMG noted further deficiencies in the development and implementation of supply chain risk management security controls, Plan of Action and Milestones reviews, configuration management controls, and the enforcement of rules of behavior acknowledgement. Based on these issues, we continue to be concerned about the remaining corrections needed in OCIO's oversight and accountability over DOL's information security control environment.

WHAT OIG RECOMMENDED

KPMG made three new recommendations to strengthen DOL's information security program. Based on our testing, we determined that 38 prior year recommendations were closed, and 31 recommendations remained open.

READ THE FULL REPORT

https://www.oig.dol.gov/public/reports/oa/2024/23-24-001-07-725.pdf