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

BRIEFLY…

FY 2022 FISMA DOL INFORMATION SECURITY REPORT: DOL’S INFORMATION SECURITY PROGRAM NOT REMAINING CURRENT WITH SECURITY REQUIREMENTS

February 10, 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) 2022 information security program for the period October 1, 2021, through June 30, 2022. 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 the security controls and targeted vulnerability assessments.

WHAT OIG FOUND

KPMG reported nine findings for DOL’s information security program within five of five Cybersecurity Framework Functions and six of nine FISMA Metric Domains, which resulted in the U.S. Department of Homeland Security’s FISMA reporting system determining DOL’s information security program was not effective for FY 2022.

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 four of the five Cybersecurity Framework Functions: Identify, Protect, Detect, and Recover. A security program is only considered effective if the majority of the Cybersecurity Framework Functions are rated at least Managed and Measurable (Level 4).

The information security program’s scores showed some decline from FY 2021, which was caused by DOL’s delayed implementation of National Institute of Standards and Technology Special Publication 800-53, Revision 5. KPMG noted further deficiencies in the performance of security control assessments, account management controls, and contingency planning controls.

Based on the issues identified by KPMG, we continue to be concerned about the remaining corrections needed in the Office of Chief Information Officer’s oversight and accountability over DOL’s information security control environment.

WHAT OIG RECOMMENDED

KPMG made eight recommendations to strengthen DOL’s information security program.

READ THE FULL REPORT

https://www.oig.dol.gov/public/reports/oa/2023/23-23-001-07-725.pdf