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

BRIEFLY...

FY 2021 FISMA DOL INFORMATION SECURITY REPORT: INFORMATION SECURITY CONTINUOUS MONITORING CONTROLS REMAIN DEFICIENT

January 28, 2022

WHY OIG PERFORMED 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 audit on DOL's fiscal year (FY) 2021 information security program for the period October 1, 2020, through September 30, 2021. 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.

READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2022/23-22-001-07-725.pdf

WHAT THE AUDIT FOUND

KPMG reported 16 findings for DOL's information security program within 4 of 5 Cybersecurity Functions and 6 of 9 FISMA Metric Domains. Based on the CyberScope calculations and results, KPMG also determined DOL's information security program was not effective because a majority of the FY 2021 Inspector General (IG) FISMA Reporting Metrics were rated Consistently Implemented (Level 3).

A security program is only considered effective if the majority of the FY 2021 IG FISMA Reporting Metrics are rated at least Managed and Measurable (Level 4). Although DOL established and maintained its information security program and practices for its information systems for the five Cybersecurity Functions and nine FISMA Metric Domains, KMPG found weakness that demonstrated that the information security program had not achieved a Managed and Measurable (Level 4) in three of the five Cybersecurity Functions: Identify, Detect, and Recover.

The information security program's scores showed some improvements from FY 2020, which may indicate the continuing adoption and implementation of new tools to address the issues previously identified. However, based on the issues identified, we remain concerned about the remaining corrections needed in the Office of Chief Information Officer's (OCIO) oversight and accountability over the Department's information security control environment.

WHAT OIG RECOMMENDED

We made 18 recommendations for the specific issues identified in the systems identified in our scope of work, to strengthen DOL's information security program. Management generally concurred with the findings and recommendations identified and described in our report. OCIO stated it has addressed or will develop plans to address all recommendations.