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

BRIEFLY...

FY 2020 FISMA DOL INFORMATION SECURITY REPORT: PROGRESS NEEDED TO IMPROVE RISK MANAGEMENT AND CONTINUOUS MONITORING INFORMATION SECURITY CONTROLS

December 22, 2020

WHY OIG PERFORMED THE AUDIT

The U.S. Department of Labor (DOL) spends approximately $666 million annually on its Information technology (IT) assets that support the programs needed to fulfill DOL's mission. As IT plays an integral role in providing the services and operations needed to fulfill DOL's mission, it is imperative that DOL maintain a strong IT security program to protect these assets. Ineffective information security programs increase the risk of unavailable service, security breaches, and unreliable information. Under the Federal Information Security Modernization Act of 2014 (FISMA), Inspectors General are required to perform annual independent evaluations of their agency's information security program and practices.

WHAT OIG DID

We contracted with KPMG LLP to conduct an independent audit of DOL's Fiscal Year (FY) 2020 information security program, for the period October 1, 2019, to September 30, 2020. KPMG partly based its determinations on tests of a selection of DOL's entity-wide security controls and system-specific security controls across 20 DOL information systems.

READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2021/23-21-001-07-725.pdf

WHAT THE AUDIT FOUND

KPMG reported 18 findings for DOL's information security program in 4 of the 5 FISMA cybersecurity functions. These findings were based on the testing of 20 DOL systems and entity-wide controls. As a result of the issues identified, the Department of Homeland Security's (DHS) FISMA reporting system determined DOL's information security program was not effective for FY 2020.

To be considered an effective information security program, DHS requires implementation of security controls to a level identified as "Managed and Measurable" for a majority of the cybersecurity functions. While the results determined DOL's information security program had achieved a level of consistently implemented for all 5 cybersecurity functions, the weaknesses identified demonstrated that the program had not achieved the level of managed and measurable in 3 of the 5 cybersecurity functions: Identify, Detect and Recover.

Additional progress is needed in 3 of its domains: Configuration Management, Identity and Access Management, and Data Protection and Privacy. These domains within the Protect Function did not fully achieve the Managed and Measurable rating and will need to be a focus of DOL in order to maintain the overall rating.

The information security program's scores showed some improvements from FY 2019, which may indicate the adoption and implementation of new tools to address the issues previously identified. However, based on the issues identified, we remain concerned about the continued improvements 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 25 recommendations to improve DOL's information security program, including establishing performance metrics. Management generally concurred with the findings and recommendations identified and described in our report. OCIO stated it has addressed or has developed plans to address all recommendations.