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

BRIEFLY...

FY 2019 FISMA DOL INFORMATION SECURITY REPORT: IMPLEMENTATION OF SECURITY TOOLS HINDERED BY INSUFFICIENT PLANNING

December 23, 2019

WHY OIG PERFORMED THE EVALUATION

DOL spends approximately $730 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 IT 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 IT security program and practices.

WHAT OIG DID

We contracted with KPMG LLP to conduct an independent evaluation of the DOL Fiscal Year (FY) 2019 information security programs, for the period October 1, 2018, to September 30, 2019. 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/2019/23-20-002-07-725.pdf

WHAT THE EVALUATION FOUND

KPMG reported findings for all FISMA cybersecurity functions, and 6 of 8 FISMA metric domains into Department of Homeland Security's FISMA reporting system, which determined DOL's information security program was not effective for FY 2019.

DOL's Office of Chief Information Officer (OCIO) was unable to provide timelines and plans for any of the information security tools that were not fully implemented, indicating the utilization of these tools was not properly managed. For ten of the FISMA metrics, OCIO did not meet a higher score because it had not fully implemented the necessary tools. In these ten metrics, the score for FY 2019 was the same as it had been in FY 2018, indicating a lack of progress in implementing a tool to address the issue at hand. The ten metrics where OCIO had not fully implemented the necessary tools covered areas including Risk Management, Configuration Management, and Identity and Access Controls.

We believe the OCIO should strive for accurate self-assessments of its information security progress. Where the OCIO had accurate self-awareness of the condition of its information security program, such as in the area of Security Training, KPMG identified positive progress in improving DOL's position. Security Training was responsible for 6 of the 21 upward trending ratings in FY 2019. Conversely, in the area of Risk Management, where the OCIO had the lowest accuracy rate of self-awareness, KPMG found non-concurrence in 8 of the 12 questions. The better the accuracy of OCIO's self-assessment, the more effective OCIO will be at addressing unresolved issues in other domain areas.

Based on these issues, we remain concerned about the continued improvements needed in the OCIO's oversight and accountability over the Department's IT control environment.

WHAT OIG RECOMMENDED

We made twenty recommendations to improve information security and establish performance metrics. The CIO concurred with most of these recommendations.