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

BRIEFLY…

September 30, 2016

FISMA FISCAL YEAR 2015: ONGOING SECURITY DEFICIENCIES EXIST

WHY OIG CONDUCTED THE EVALUATION

Congress, the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Government Accountability Office (GAO) have identified the information security of federal agencies as a continuing area of high risk. To ensure federal information assets are properly secured, Congress passed the Federal Information Security Modernization Act (FISMA) in 2002, and revised it in 2014. FISMA requires all executive agencies to use standards put forth by the National Institute of Standards and Technology (NIST) to protect their information and information systems.

Under FISMA, federal agencies are required to independently evaluate their information security programs and practices every year.

WHAT OIG DID

We conducted an evaluation to determine the following:

> Did DOL implement effective FISMA minimum information security requirements?

For FY 2015, we tested 15 nonfinancial systems (10 DOL agency systems and 5 contractor systems) and 8 financial systems (5 DOL systems and 3 contractor systems), using Office of Management and Budget/Department of Homeland Security metrics, National Institute of Standards and Technology guidance, and DOL policies and procedures.

READ THE FULL REPORT

To view the report, including the scope, methodologies and full agency response, go to: http://www.oig.dol.gov/public/reports/oa/2016/23-16-002-07-725P.pdf

WHAT OIG FOUND

DOL controls had not been fully implemented or were not operating effectively to meet minimum FISMA security requirements. Our testing of selected controls identified 116 deficiencies across 8 of the 10 FISMA security areas. Of those 116 deficiencies, 60 were related to identity and access management, a key control area for ensuring an authenticated user accesses only what they are authorized to access and no more. Numerous deficiencies were also identified in the areas of contingency planning (20) and configuration management (17).

Despite many previous reports that identified similar control weaknesses, these deficiencies continue to exist or reoccur, and represent ongoing, unnecessary risks to the confidentiality, integrity, and availability of DOL's information. The deficiencies identified in this report occurred because the internal control framework in the eight FISMA control areas has not been effective. The ineffectiveness of the internal control framework was due, in part, to the CIO not having the independence and authority at the department level for implementing and maintaining an effective information security program.

WHAT OIG RECOMMENDED

We recommended the Assistant Secretary for Administration and Management realign the organizational structure as it relates to the CIO to address the organizational independence issue identified in this report. Additionally, we recommended the CIO work with Program Agency management to develop corrective actions for the deficiencies identified in this report.

The CIO generally agreed to the findings in the report, but indicated further linkage to risks would have been beneficial. The CIO stated a corrective action program has been implemented to address the reported and other information security deficiencies. The CIO disagreed with the OIG's recommendation to realign the organizational structure to address the CIO independence issue. She asserted the CIO reporting arrangement is defined in a way that best works for DOL and is aligned with the Office of Management and Budget's Federal Information and Technology Acquisition Reform Act CIO assignment plan.