Grant Thornton

The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015
A-14-16-50037

November 2015 **Report Summary**

Objective

Our objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), as defined by the Department of Homeland Security (DHS).

Background

SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year (FY) 2015 FISMA performance audit in accordance with Government Auditing Standards. We assessed the effectiveness of SSA's information security controls including its policies, procedures, and practices on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and by performing additional testing procedures as needed. We used the DHS OIG FY 2015 Inspector General (IG) FISMA reporting metrics as the basis for our assessment of SSA's overall information security program and practices.

Findings

Although SSA had established an information security program and practices that were generally consistent with FISMA requirements, we identified a number of deficiencies related to continuous monitoring management; configuration management; identity and access management; incident response and reporting; risk management; security training; contingency planning; and contractor systems. Many of the weaknesses we identified were similar to the deficiencies reported in past FISMA assessments. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. We concluded that the risk and severity of the weaknesses constituted a significant deficiency in internal controls over FISMA and as defined by Office of Management and Budget (OMB) guidance, M-14-04.

Recommendations

While SSA continued executing its risk-based approach to strengthen controls over its information systems and address weaknesses during FY 2015, we identified persistent deficiencies in both the design and operation of controls related to the DHS reporting metrics. We believe that SSA must strengthen its information security risk management framework and enhance information technology (IT) oversight and governance to address these weaknesses. SSA must make the protection of the Agency's networks and information systems a top priority, and dedicate the resources needed to (1) ensure the appropriate design and operating effectiveness of information security controls and (2) prevent unauthorized access to the sensitive information. We provided detailed recommendations throughout the performance audit for each weakness identified. Additional recommendations can be found within the conclusions and recommendations section of this report.

SSA management generally agreed with the findings and recommendations, however, management disagreed with our assessment of compliance for some risk management metrics. Management responses and Grant Thornton's response can be found within the views of responsible officials section of this report.