The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017
A-14-18-50258

October 2017 **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.

Background

SSA's Office of the Inspector General engaged us, KPMG LLP (KPMG), to conduct the Fiscal Year (FY) 2017 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 performing necessary additional testing procedures. For the FISMA performance audit, we used the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* as the basis for our evaluation of SSA's overall information security program and practices.

Findings

Although SSA had established an Agency-wide information security program and practices, we identified a number of control deficiencies related to Risk Management, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. Many of the weaknesses we identified were similar to the deficiencies reported in past FISMA performance audits. SSA's information security program was "Not Effective" according to DHS criteria.

Recommendations

While SSA continued executing its risk-based approach to strengthen controls over its information systems and address weaknesses, we continued identifying persistent deficiencies in both the design and operation of controls related to the Department of Homeland Security reporting metrics. We issued 10 overarching recommendations related to the causes of these control deficiencies that, if implemented, should strengthen SSA's information security program and practices to be consistent with FISMA. To address these weaknesses, we believe SSA must strengthen its information security risk management framework and enhance information technology oversight and governance to address these weaknesses. SSA should make protecting its 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 sensitive information. We provided detailed recommendations throughout the performance audit for each weakness identified. Additional recommendations can be found in the Conclusions and Recommendations section of this report.