LIMITED DISTRIBUTION

The Social Security Administration's Information Security Program and Practices for Fiscal Year 2019 A-14-18-50717

October 2019 **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 engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year (FY) 2019 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 2019 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 established an Agency-wide information security program and practices, we identified a number of deficiencies related to Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, 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 DHS reporting metrics. We issued 14 overarching recommendations related to the causes of these deficiencies that if implemented and consistently executed, 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. 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; (2) prevent unauthorized access to the sensitive information the American public entrusts to SSA; and (3) detect malicious or inappropriate activity and prevent data exfiltration.

SSA management generally agreed with our findings; however, management self-assessed their program's maturity at one level higher compared to our results. Management's response does not impact the results, findings, and conclusion of our audit.