Grant Thornton

The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014 A-14-14-24083

October 2014 **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 Management Act of 2002* (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 2014 FISMA performance audit in accordance with *Government Auditing Standards*, commonly referred to as the "Yellow Book," which sets forth generally accepted government auditing standards. We assessed the effectiveness of SSA's information security 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 through additional testing procedures as needed. We determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and supporting applicable regulations, standards, and guidance applicable during the audit period.

Our Findings

We determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. However, weaknesses in some of the program's components limited the program's effectiveness to adequately protect the Agency's information and information systems. We concluded that these weaknesses constituted a significant deficiency under FISMA.

Our Recommendations

- Implement requirements or appropriately justify deviations associated with the United States Government Configuration Baseline for Windows components.
- Continue, as part of the SSA threat and vulnerability management processes, prioritization and implementation of risk mitigation strategies and plans of action and milestones.
- Develop comprehensive policies and procedures related to application and system-software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and control monitoring.
- Continue, as part of the SSA profile quality program, additional profile content reviews and profile improvement initiatives.
- Enhance current information technology oversight and governance processes to ensure SSA information technology risk management requirements are effectively and consistently implemented.
- Address security awareness training weaknesses identified as well as other weaknesses noted within the comments of Appendix B by implementing our recommendations provided throughout the audit.

SSA agreed with our recommendations.