Grant Thornton

The Social Security Administration’s Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013

November 2013 **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 2013 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 performance of 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 other 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 overall 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

- Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) 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 current access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.

- Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.

- Address weaknesses identified within the comments of Appendix B by implementing our recommendations provided throughout the audit in our Notices of Finding and Recommendation.