Summary of the Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2012 A-14-12-12120

November 2012 **Social Security Administration Office of the Inspector General**

Objective

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.

Background

FISMA provides the framework for securing the Government's information and information systems. FISMA requires that each agency develop, document, and implement an agency-wide information security program. FISMA also requires that each agency's Inspector General, or an independent external auditor, perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.

Our Findings

For Fiscal Year 2012, we determined that SSA's overall information security program and practices were generally consistent with FISMA requirements. However, weaknesses in some of the program's components limited the program's overall effectiveness to adequately protect the Agency's information and information systems. We noted that Grant Thornton, LLP, (GT) reported a material weakness over SSA's internal controls for the Agency's financial statement audit. After considering this material weakness, its underlying causes, and the results of our FISMA-related work, we concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a significant deficiency under FISMA.

Our Recommendations

To improve the effectiveness of SSA's overall information security program and to address the material weakness, GT recommended that SSA management consider timely implementing:

- Monitoring controls designed to identify configurations in the SSA network and systems environment that do not comply with the SSA system configuration policy.
- A comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Comprehensive enterprise-wide security vulnerability testing to identify critical weaknesses in the information technology environment that may not be identified by the current control processes.
- A comprehensive profile and access recertification program.
- Additional controls to prevent unauthorized programmer access to the production environment.

We reiterate GT's recommendations and believe these recommendations address the financial statement audit material weakness and FISMA significant deficiency.