Report Summary

Social Security Administration Office of the Inspector General

November 2011

Objective

Our objective was to determine whether the Social Security Administration's (SSA) overall security program and practices complied with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) for Fiscal Year (FY) 2011.

Background

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget, Department of Homeland Security and Congress on the adequacy and effectiveness of their security programs. FISMA requires that each agency develop, document, and implement an agency-wide information security program.

To view the full report, visit http://oig.ssa.gov/audits-and-investigations/audit-reports/A-14-11-01134

Fiscal Year 2011 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 (A-14-11-01134)

Our Findings

We determined that SSA's security programs and practices were generally consistent with FISMA requirements for FY 2011. SSA continues to work toward maintaining a secure environment for its information and systems. However, there were some areas that needed improvement. SSA should ensure

- continued improvements in change and access control processes;
- continued improvements in its risk management process;
- proper incident handling and reporting;
- protection of personally identifiable information;
- contractors receive security awareness and specialized training;
- continued implementation of its continuous monitoring strategy; and
- contractor system oversight.

Our Recommendations

1. Establish a timeframe for contractor personnel to complete security awareness training and ensure all contractor personnel complete security awareness training before being granted access to Agency systems;
2. Provide additional guidance to assist SSA components to identify contractors with significant information security responsibilities and ensure these contractors received specialized training;
3. Ensure implementation of its *Strategy for Information Security Program Continuous Monitoring* to fully meet the current and anticipated Federal requirements and address all gaps identified in the strategy and this report; and
4. Ensure the Chief Information Security Officer has access to all Agency Continuous Monitoring data.