Report Summary

Social Security Administration Office of the Inspector General

November 2010

Objective

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) 2010.

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 (OMB) 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://www.ssa.gov/oig/ADOBEPDF/A-14-10-20109.pdf

Fiscal Year 2010 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-10-20109)

Our Findings

We determined that SSA's security programs and practices generally complied with FISMA for FY 2010; however, some improvements were needed. SSA continues to work toward maintaining a secure environment for its information and systems.

Our Recommendations

We recommend SSA:

1. Continue to implement security controls to resolve the significant deficiency identified in this report.
2. Establish a separate chapter in its Information Systems Security Handbook to outline all required security tasks for Contractor Systems Oversight according to OMB requirements.
3. Require that contracts include Federal security requirements.
4. Ensure compliance with the Federal requirements and Agency's policy for Contractor Systems Oversight.
5. Complete the Access to Financial Institutions (AFI) Certifications and Accreditation prior to further expanding AFI application to more States.
6. Work with the Office of the Inspector General (OIG), Office of Investigations to establish policy and procedures on what types of personally identifiable information (PII) incidents should be reported to law enforcement and OIG and in what timeframes.
7. Revise its policy, guidance, procedures, and timeframes for reporting of PII incidents to law enforcement, including the OIG.
8. Ensure all PII incidents are reported within the established timeframes.
9. Provide additional guidance for determining the training needs for its employees with significant security responsibilities, require retention of documentation for such training, and establish guidance to assess the effectiveness of its security training program.