Report Summary

Social Security Administration Office of the Inspector General

September 2009

Objective

Our objective was to determine whether the Social Security Administration (SSA) had implemented the recommendations in our June 2001 report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044).

Background

Our June 2001 report stated that SSA lacked a strong framework for overall security administration, policy development, and policy implementation. We made five recommendations, which included that SSA: (1) Centralize its systems security management structure to comply with applicable laws; and (2) Develop a more inclusive system security plan for the mainframe and distributed computing environments.

To view the full report, visit http://www.ssa.gov/oig/ADOBEPDF/A-14-09-19048.pdf

Follow-up: The Social Security Administration's Computer Security Program Compliance (A-14-09-19048)

Our Findings

SSA considered each of the five prior recommendations to be implemented and closed. Our follow-up review determined that SSA had implemented Recommendations 2 and 4. However, SSA had not fully addressed Recommendations 1, 3 and 5. Despite SSA's efforts to address these recommendations, our current review found that:

- SSA continued to have a decentralized/fragmented information security management structure;
- the Office of the Chief Information Officer did not have sufficient delegated authority and resources to carry out its responsibilities for SSA's information security program;
- SSA had not sufficiently documented its policy and procedures to ensure all systems users receive timely notification of imminent security incidents; and
- SSA's Information Systems Security Handbook (ISSH) did not cover all security areas and contained outdated and inaccurate information.

Our Recommendations

We recommend that SSA:

1. Centralize its security management structure to ensure a coordinated approach to its agency-wide information security program.
2. Clearly delineate roles, responsibilities, and lines of communication that report to a single management focal point.
3. Ensure the Chief Information Officer has sufficient delegated authority and resources to fulfill required security responsibilities according to applicable laws, regulations and guidance.
4. Update its Agency-wide Information Security Program Plan.
5. As appropriate, ensure written polices and procedures require notification of all Agency systems users for certain computer incidents.
6. Update the ISSH with the most current and accurate information and consider further delineating security roles.