Report Summary

Social Security Administration Office of the Inspector General

September 2009

Objective

To address information security concerns expressed by the Information Security and Privacy Advisory Board (ISPAB) and to ensure the Agency complied with the National Institute of Standards and Technology Special Publication guidance. This evaluation provides a status of the Agency's efforts to implement a security performance metrics program.

Background

On July 30, 2008, the Chairman of ISPAB sent a letter to the Office of Management and Budget expressing concerns with current information security performance metrics developed under the *Federal Information Security Management Act.* We performed this evaluation to provide a status of the Agency's efforts to develop a performance metrics program for its security program as well as offer suggestions for management's consideration.

To view the full report, visit http://www.ssa.gov/oig/ADO BEPDF/A-14-10-11002.pdf

Quick Response Evaluation: Implementation of the Social Security Administration's Security Performance Metrics Program (A-14-10-11002)

Our Findings

Based on our analysis, we identified some areas the Agency should be aware of as it moves forward in developing a more comprehensive security metrics program. An information security measures development process consists of two major activities:

- Identification and definition of the current information security program.
- Development and selection of specific measures to gauge the implementation, effectiveness, efficiency, and impact of the security controls.

The Social Security Administration (SSA) needs to ensure the above activities are an integral part of its process for developing information technology security performance metrics.

Matters for Consideration

We understand the Agency is developing an information security performance metrics program. We acknowledge and applaud SSA for being proactive in developing this program despite it not being required or mandated at this time. We encourage the Agency to continue these efforts and take the necessary steps to fully develop its information security performance metrics program.

- Ensuring the information security metrics performance program addresses the key measure development steps recommended by the National Institute of Standards and Technology.

- Implementing an Agency-wide information security performance metrics program in accordance with applicable Federal guidance. These measures should be measurable, repeatable, consistent, and actionable.