Report Summary

Social Security Administration Office of the Inspector General

June 2009

Objective

To determine the extent to which the Social Security Administration (SSA) implemented the recommendations from our September 2006 report, *The Social Security Administration's Electronic Mail Security Review*.

Background

Our September 2006 report found weaknesses in the Agency's electronic mail (e-mail) security control framework and made nine recommendations to address them.

To view the full report, visit http://www.ssa.gov/oig/ADOBEPDF/A-14-09-19044.pdf

Follow-up: The Social Security Administration's Electronic Mail Security Review
(A-14-09-19044)

Our Findings

Our initial review contained nine recommendations, of which the Agency agreed with seven. For these seven recommendations, we determined four were fully implemented, two were not fully implemented and one was not addressed. With respect to the two original recommendations with which SSA disagreed, we reaffirm our recommendations.

Our Recommendations

1. Ensure e-mail server settings are configured correctly in accordance with the National Institute of Standards and Technology (NIST) recommended standards.
2. Ensure the policies and procedures require compliance with least-privilege administrative access and appropriate chain of command approvals for e-mail account assignment.
3. Develop and document an SSA Microsoft Exchange Server Configuration Guide for e-mail settings in accordance with NIST recommended standards.
4. Continually monitor servers for compliance with SSA's Microsoft Exchange Server Configuration Guide.
5. Develop, document, and test the recovery/failover capability for the e-mail messaging infrastructure, to include external as well as internal e-mail communications.
6. Ensure appropriate risk assessments are performed on the entire e-mail system comprised of SSA's Microsoft Exchange Server 2003 and 2007 environments, the Office of Workforce Analysis system, and the e-mail security structure.