Report Summary

Social Security Administration Office of the Inspector General

October 2010

Objective

To assess the Social Security Administration's (SSA) policy and procedures for approving and monitoring software on employee and contractor computers.

Background

SSA's Information Systems Security Handbook states that SSA managers and users must take appropriate actions to secure and prevent the improper use, damage, or destruction of SSA hardware and software. Further, the only software authorized for use on SSA computers is software purchased through the Agency-sanctioned requisition process or developed, evaluated, and documented in-house. Personally owned software is prohibited on SSA computers unless its use is critical to an SSA function and there is no comparable Agency software solution.

To view the full report, visit http://www.ssa.gov/oig/ADOBEPDF/A-14-10-21082.pdf

The Social Security Administration's Approval and Monitoring of the Use of Software (A-14-10-21082)

Our Findings

Based on our evaluation, we determined that SSA had a software approval and monitoring policy for employees' and contractors' use of software on Agency computers. However, we determined the Agency's software approval and monitoring policy needed improvement. In addition, we found SSA employees, managers, and contractors did not always comply with the Agency's software approval policy by obtaining a waiver before installing non-standard software. Further, in five of seven software-related security incidents reviewed, we determined that no documented disciplinary action had been taken against the employee for not complying with the Agency's software approval policy. In addition, we found SSA's monitoring of known Agency-wide software configurations was not sufficient. Moreover, we were unable to determine whether local management was effectively monitoring software because only one software waiver was submitted for approval.

Matters for Consideration

The Agency should consider:

1. centralizing its software approval process.
2. revising its software security policy to clearly indicate that software authorized by the local manager must first go through the waiver approval process.
3. sending reminders on the Agency's policy that prohibits the use of personal/unapproved software.
4. having all software monitoring directed by the Office of Telecommunications and Systems Operations with implementation by local managers.
5. obtaining electronic tools to inventory all types of software on Agency computers and tools that prevent unauthorized software from being installed.

During our review, the Agency implemented our third Matter for Consideration and issued a reminder that installation and use of unauthorized software is prohibited.