Report Summary

Social Security Administration Office of the Inspector General

November 2010

Objective

To determine whether the Social Security Administration (SSA) implemented Recommendation 5 from our December 2002 report, *Physical Security for the Social Security Administration's Laptop Computers, Cellular Telephones, and Pagers* (A-14-02-32061), and followed its policies and procedures for the disposal of workstations and servers.

Background

SSA policy requires that information technology (IT) media be sanitized or destroyed before its disposal. In our December 2002 report, we identified two laptops that were not properly sanitized. As a result, we recommended SSA improve its security procedures for disposing of excess laptops.

To view the full report, visit http://www.ssa.gov/oig/ADOBEPDF/A-14-10-11003.pdf

The Social Security Administration's Controls for Ensuring the Removal of Sensitive Data from Excessed Computer Equipment

(A-14-10-11003)

Our Findings

We found that SSA generally complied with its IT equipment disposal policies and procedures. However, there are opportunities to enhance the Agency's IT equipment disposal policies and procedures. Our review identified the following issues.

- SSA partially implemented our prior recommendation and should revise its IT media disposal policies and process.
- IT media awaiting disposal contained PII.
- IT media from equipment awaiting disposal was missing.

Our Recommendations

We recommend that SSA:

1. Evaluate its IT media sanitization policies and procedures to ensure compliance with federal laws, regulations, guidelines, standards, and best practices. At a minimum, SSA should
   a. Designate one or more employees within each region who will certify and erase all information from IT media.
   b. Test a representative sample of sanitized IT media to ensure all data and programs are effectively erased before disposal.
2. Identify and resolve the gaps between its IT media sanitization policy and procedures.
3. Properly mark excess IT equipment with hard drives as sanitized immediately after sanitization has been performed.
4. Properly track IT media (i.e. hard drives) through the sanitization and disposal process, and document the:
   a. serial numbers of hard drives that have been removed from IT equipment such as servers or desktops,
   b. sanitization method used,
   c. date and type of disposal, and
   d. recipient of the equipment.
5. Properly monitor sanitization contractors to ensure tasks are completed properly and correctly documented.
6. Report the 41 missing IT equipment hard drives identified in this report and any future undocumented disposal of IT equipment hard drives to the United States Computer Emergency Readiness Team.