OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

RISKS POSED BY
DIGITAL PHOTOCOPIERS
USED IN SOCIAL SECURITY
ADMINISTRATION OFFICES

May 2012 **A-06-11-11155**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: May 17, 2012 Refer To:

To: The Commissioner

From: Inspector General

Subject: Risks Posed by Digital Photocopiers Used in Social Security Administration Offices (A-06-11-11155)

OBJECTIVE

Our objective was to determine the status of corrective actions the Social Security Administration (SSA) took to address recommendations in our September 2008 report, *Risks Posed by Digital Photocopiers Used in Social Security Administration Offices* (A-06-08-28076).

BACKGROUND

The *Privacy Act of 1974*[1] provides the framework for regulating the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. In particular, the *Privacy Act* requires that each Agency

> . . . establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.[2]

The loss of personally identifiable information (PII) can lead to identity theft or other fraudulent use of the information, which could result in harm, embarrassment, and inconvenience to individuals. Accordingly, SSA should safeguard sensitive PII, including PII on its hard drives.

SSA's Office of Supply and Warehouse Management's Reprographic Management Team (RMT) procures and manages reprographic equipment (photocopiers), services,

[1] The *Privacy Act of 1974*, as amended, Pub. L. No. 93-579,88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[2] 5 U.S.C. § 552a(e)10.

and supplies for all SSA offices nationwide. According to SSA officials, all photocopiers purchased since September 2008 contain hard drives capable of storing images of copied or printed material. Leaving these hard drives unprotected or unaccounted for can increase the potential for identity theft. From January 1 through December 31, 2010, SSA disposed of 409 digital photocopiers that contained hard drives capable of storing document images.

Our 2008 audit found that SSA had not effectively mitigated the risks posed by the potential exposure of sensitive information. Specifically, SSA did not sanitize or destroy photocopier hard drives upon disposal, as required, or include a non-disclosure statement in its agreement with vendors that precluded the disclosure of sensitive information when photocopiers were taken off-site for repair. Additionally, SSA's inventory tracking system did not distinguish between stand-alone photocopiers with no hard drives and photocopiers with hard drives or account for purchases in a timely manner. Therefore, we recommended that SSA:

1. Establish procedures for sanitizing or destroying photocopier hard drives,

2. Amend the maintenance provision in blanket purchase agreements (BPA)[3] to include the required non-disclosure statement by the servicing vendor when photocopiers are sent off-site for repair,

3. Implement an automated photocopier inventory system that includes the capability of tracking the existence of hard drives, and

4. Record all digital photocopier purchases to the automated tracking system within a reasonable time after the equipment is received and installed.

The Agency agreed with all four recommendations. (See Appendix B for additional information on our scope and methodology.)

RESULTS OF REVIEW

SSA took action to address our 2008 recommendations. SSA established procedures for sanitizing or destroying photocopier hard drives and established a requirement that contractors certify they sanitized, removed, or destroyed hard drives before removing photocopiers from SSA premises. SSA incorporated hard drive sanitization policies into photocopier Blanket Purchase Agreements (BPA) and incorporated additional security provisions in photocopier maintenance agreements.[4]

---

[3] A BPA is a simplified method for filling anticipated repetitive needs for supplies or services by establishing the equivalent of "charge accounts" with qualified sources of supply.

[4] At the time of our review, SSA had incorporated hard drive sanitization requirements in maintenance agreements with 11 of 12 photocopier vendors. SSA is working with the 12th vendor to include similar requirements in the maintenance agreement.

SSA implemented a new automated system that tracks whether photocopiers have hard drives and improves the timeliness of recording photocopier purchases in its inventory records.

However, while SSA requires that contractors certify that photocopier hard drives were sanitized, removed, or destroyed prior to removal from SSA premises, we found that SSA rarely obtained the required certifications. Also, the automated inventory system SSA used to track photocopiers did not accurately identify the number of photocopiers in service at the time of the audit.

We are not aware of any incidents where PII breaches occurred as a result of loss of information stored on photocopier disk drives. However, as long as this vulnerability exists, SSA should continue proactively reducing the risk of exposing sensitive information to unauthorized individuals.

HARD DRIVE CERTIFICATIONS NOT OBTAINED

SSA continued disposing of photocopiers without obtaining verification that vendors erased or destroyed the hard drives. SSA requires completion of a hard drive certification form before vendors remove photocopiers from SSA's premises.[5] However, SSA could only provide required sanitization certifications for 1 of 30 sampled disposed photocopiers. RMT staff acknowledged that SSA did not require that vendors that removed old photocopiers complete these certifications.[6] SSA needs to ensure vendors follow Agency policies before removing photocopiers from SSA facilities.

AUTOMATED PHOTOCOPIER INVENTORY TRACKING SYSTEM

SSA's photocopier inventory included approximately 2,600 photocopiers that had been disposed of and were no longer in SSA's possession. RMT officials are required to maintain accurate reprographic equipment inventory records.[7]

According to RMT staff, problems with SSA's automated inventory system prevented deletion of thousands of photocopiers that were no longer in service. To determine the number or location of photocopiers in service, SSA had to rely on the corporate knowledge of RMT staff members familiar with photocopier purchases and disposals. RMT officials were aware of this problem and stated they were working with programmers to correct the error.

---

[5] Administrative Instructions Manual System (AIMS), Materiel Resources (MR) 03.08.03 A.2.

[6] AIMS, MR 03.08.03 B.7 requires that vendor technicians complete a hard drive sanitization certificate before removing a photocopier from SSA premises unless a general hard drive certification for a particular model is on file. RMT did not have general certifications on file for any of the copier models included in our sample.

[7] AIMS, MR 04.04.02 C.

CONCLUSION AND RECOMMENDATION

SSA had addressed our previous recommendations; however, further improvement is needed to ensure photocopier hard drives are erased or destroyed before disposal. Therefore, we recommend that SSA enforce its requirement that photocopier vendors certify in writing that photocopier hard drives are erased or destroyed before removal from SSA premises.

AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with our recommendation. See Appendix C for the Agency's comments.

Patrick P. O'Carroll, Jr.

Appendices

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Agency Comments

APPENDIX D – OIG Contacts and Staff Acknowledgments

Acronyms

AIMS	
BPA	Blanket Purchase Agreement
MR	Materiel Resources
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
RMT	Reprographic Management Team
SSA	Social Security Administration
U.S.C.	United States Code

Scope and Methodology

To accomplish our objectives, we:

- Reviewed the applicable sections of the *Privacy Act of 1974*, Federal Acquisition Regulations, Administrative Instructions Manual System, and Information Systems Security Handbook.
- Considered the security implications of the Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.
- Reviewed relevant Office of the Inspector General reports.
- Reviewed inventory print screens, Blanket Purchase Agreements, and Task Orders.
- Interviewed Social Security Administration (SSA) employees from the Division of Property Management's Radiographic Management Team.
- Performed limited testing on SSA's photocopier inventory list.
- Obtained a listing identifying all photocopiers SSA disposed during Calendar Year 2010, and reviewed disposition documentation for 30 randomly selected photocopiers.

We performed audit work between May 2011 and February 2012 in Dallas, Texas. We tested the data obtained for our audit and determined them to be sufficiently reliable to meet our objective. The entity audited was SSA's Office of Supply and Warehouse Management under the Office of the Deputy Commissioner for Budget, Finance and Management. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: May 14, 2012 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Dean S. Landis /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "Risks Posed by Digital Photocopiers Used in Social Security Administration Offices" (A-06-11-11155)—INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Amy Thompson at (410) 966-0569.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "RISKS POSED BY DIGITAL PHOTOCOPIERS USED IN SOCIAL SECURITY ADMINISTRATION OFFICES" (A-06-11-11155)

Recommendation 1

Enforce its requirement that photocopier vendors certify in writing that photocopier hard drives are erased or destroyed before removal from SSA premises.

Response

We agree.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Ron Gunia, Director, Dallas Audit Division

Jason Arrington, Audit Manager

Acknowledgments

In addition to those named above:

Ashley Moore, Auditor

For additional copies of this report, please visit our Website at http://oig.ssa.gov/ or contact the Office of the Inspector General's Public Affairs Staff at (410) 965-4518. Refer to Common Identification Number A-06-11-11155.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.