OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S CONTROLS FOR ENSURING THE REMOVAL OF SENSITIVE DATA FROM EXCESSED COMPUTER EQUIPMENT

November 2010 **A-14-10-11003**

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: November 10, 2010 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Controls for Ensuring the Removal of Sensitive Data from Excessed Computer Equipment (A-14-10-11003)

OBJECTIVE

Our objective was 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),[1] and followed its policies and procedures for the disposal[2] of workstations and servers.[3]

BACKGROUND

SSA donates excess IT equipment[4] when possible. The Agency may also sell or destroy the equipment. SSA policy[5] requires that IT media be sanitized or destroyed before its disposal. At Headquarters, IT equipment disposal is centrally performed. At

[1] We recommended SSA improve its security procedures for disposing of excess laptops. This should include a risk assessment to determine the appropriate level of cleaning of the excess laptops. The Agency should also designate an employee from each component to be responsible for certifying and erasing all information from the excess laptops according to SSA's disposal procedures for Headquarters. The laptops should be tested, on a sample basis, to verify that all programs and data are effectively erased prior to donation.

[2] SSA policy indicates that disposal methods for personal property include certain donations, sale, abandonment, and destruction, among others. Administrative Instructions Manual System (AIMS) *Materiel Resources Manual (MRM) Section* 04.29.03. SSA policy also indicates that prior to releasing to vendors, disposing, or donating information technology (IT) media, the media must be sanitized or destroyed in a manner that prevents unauthorized disclosure of sensitive information. SSA, Information System Security Handbook (ISSH), Section 10.3.1.

[3] A server is a computer that provides services used by other computers.

[4] Excess IT equipment is equipment retired by SSA for various reasons, such as equipment refreshment and replacing equipment that stopped functioning.

[5] ISSH, Section 10.3.1.

all other SSA locations, each office disposes its own IT equipment. See Appendix C for a description of these processes.

In our December 2002 report, we identified two laptops that were not properly sanitized[6] before disposal. In fact, our forensic investigators were able to restore personally identifiable information (PII)[7] from these laptops.[8] As a result, we recommended SSA improve its security procedures for disposing of excess laptops, including testing laptops, on a sample basis, to verify that all programs and data are effectively erased before their donation.

The *Privacy Act of 1974* requires that each Federal agency establish safeguards to ensure the security and confidentiality of the records it maintains.[9] Furthermore, the Office of Management and Budget (OMB) has issued several memorandums[10] to stress the importance of the protection of PII maintained by the Government. Federal agencies are required to apply National Institute of Standards and Technology (NIST) guidance to sanitize information system media before disposal,[11] and the General Services Administration's Federal Management Regulation (FMR) requires that Federal agencies implement policies and procedures for removing sensitive or classified information from property before disposal.[12]

---

[6] Sanitization refers to the process of removing data from storage media, such that there is reasonable assurance the data may not be easily retrieved and reconstructed.

[7] PII refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[8] We found 5,308 Social Security numbers, wage information, and names on the hard drives of the 2 laptops.

[9] Pub. L. No. 93-579 § 552a(e)(10), 5 U.S.C. § 552a(e)(10). This section of the Privacy Act also requires that such safeguards protect against any anticipated threats or hazards to the security and integrity of such records, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

[10] OMB Memorandums M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006; M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006; and M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

[11] The *Federal Information Security Management Act of 2002* (FISMA) requires compliance with information security standards promulgated under § 11331 of Title 40, which includes standards promulgated by NIST. Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(B)(i), 44 U.S.C. § 3544(a)(1)(B)(i). NIST recommends organizations sanitize information system media prior to disposal, release out of organizational control, or release for reuse. NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Appendix F, *Security Control Catalog*, Page F-74, MP-6, *Media Sanitization*, August 2009

[12] FMR, Subchapter B §102-35.30(c).

The scope of our 2002 review was limited to testing excess laptops[13] at Headquarters. In our current review, we tested workstations, laptops, and servers that were sanitized and awaiting disposal at SSA's Headquarters and Philadelphia Region. In total, we tested 274 hard drives.[14] Based on the results identified in the following section, we performed additional testing in some of SSA's regions. See "Other Matters" section of this report. For additional Background and Scope and Methodology, see Appendices B and C, respectively.

RESULTS OF REVIEW

We found the Agency had partially implemented Recommendation 5 from our 2002 report to improve its security procedures for disposing of excess laptops. We also 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.

SSA PARTIALLY IMPLEMENTED OUR PRIOR RECOMMENDATION AND SHOULD REVISE ITS IT MEDIA DISPOSAL POLICIES AND PROCESS

In our 2002 report, we recommended SSA improve its security procedures for disposing of excess laptops. This should include

1. assessing risk to determine the appropriate level of cleaning of the excess laptops;
2. designating an employee from each component to be responsible for certifying and erasing all information from the excess laptops according to SSA's disposal procedures for Headquarters; and
3. testing laptops, on a sample basis, to verify that all programs and data are effectively erased before their donation.

Since our 2002 review, SSA has established an agencywide security policy in its ISSH requiring that before disposal, the IT media must be sanitized or destroyed in such a way that prevents unauthorized disclosure of sensitive information.[15] The policy also

---

[13] See Footnote 4.

[14] The hard disk drive is the main, and usually largest, data storage device in a computer. The operating system, software titles, and most other files are stored on the hard disk drive.

[15] ISSH, Chapter 10, *Disposal of Information Technology Media Policy*, Section 10.3.1, *Disposal/Donation of Information Technology Equipment*.

requires specific sanitization and destruction methods to be applied in a manner that makes all data unrecoverable.[16] Therefore, a risk assessment, as required by our previous recommendation, is not needed to determine the appropriate level of cleaning of the excess laptops.

SSA's policy does not require that each component designate an employee to certify that excess equipment is properly sanitized. According to NIST, organizations should ensure that property management officials are included in documenting the media sanitization process to establish proper accountability of equipment and inventory control.[17] At Headquarters, designated personnel oversee the performance of sanitization contracts, which require sanitization documentation. In the regions, however, this documentation is not required.

SSA policy for Headquarters and its regions also does not require that workstations, laptops, or servers be tested, on a sample basis, to verify that all programs and data are effectively erased prior to donation. NIST guidance states that verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality.[18] A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained.[19] Based on the above discussion, we concluded that SSA partially implemented our prior recommendation.

Moreover, SSA's policy[20] on "*Disposal of Personal Property"* does not reference the ISSH IT media disposal policy. The AIMS instruction had not been updated since 1996. As a result, Agency staff may not have been aware of proper sanitization procedures for IT equipment before disposal.

[16] To sanitize IT media, one of the following methods must be used: 1) approved overwrite utilities; 2) degaussing; or 3) physical destruction of the media. The overwrite utility must completely overwrite the media with repetitive characters, making the data unrecoverable. Degaussing must be performed with a certified tool designed for the media being degaussed. Certification of the tool is required to ensure the magnetic flux applied to the media is strong enough to render the information irretrievable. Examples of physical destruction include shredding, pulverizing, and burning. ISSH,supra.

[17] NIST SP 800-88, *Guidelines for Media Sanitization*, Section 4.8, September 2006.

[18] NIST SP 800-88, supra at Section 4.7.

[19] Id.

[20] SSA, AIMS, MRM § 04.29.

Although SSA had an IT media disposal policy[21] and process, the following enhancements are needed.

1. Designate one or more employees within each region to certify and erase all information from IT media.
2. Require that workstations, laptops, and servers be tested, on a sample basis, to verify that all programs and data are effectively erased before disposal.
3. Identify and resolve the gaps between SSA's IT media sanitization policy located in the ISSH and its procedures located in AIMS.

IT EQUIPMENT SANITIZATION AND DISPOSAL PROCESS

We tested 274 hard drives of excess IT equipment identified by Agency staff as **sanitized and awaiting disposal** to determine whether they were, in fact, properly sanitized. At Headquarters, we selected 45 hard drives from workstations for testing; no laptops or servers were available during our audit period. We also selected 229 hard drives from workstations, laptops, and servers at 5 sites in the Philadelphia Region.[22] As shown in Tables 1 and 2 below, we found:

- 5 of 253 workstation hard drives (2 percent) were not properly sanitized. SSA staff stated that SSA's contractor sanitized the five workstation hard drives; however, four of the five contained PII.

- Hard drives were missing from 39 workstations and 2 laptops. SSA could not provide documentation that the hard drives were properly disposed of.

Table 1: OIG Hard Drive Test Results by Type of Equipment

Number of Hard Drives Tested by Type of Equipment				
Type of Equipment	Workstations	Laptops	Servers	Total
Total Tested	253	2	19	274
Not Sanitized	**5**	**0**	**0**	**5**
Contained PII	**4**	**0**	**0**	**4**
Hard Drives Missing	**39**	**2**	**0**	**41**

[21] See Footnote 15.

[22] Philadelphia Hearing Office; Philadelphia Regional Office; Richmond Downtown Field Office, Camp Springs Field Office, and Postal Plaza Field Office.

Table 2: OIG Hard Drive Test Results by Site

Number of Hard Drives Tested by Site							
Test Sites	HQ	Site 1	Site 2	Site 3	Site 4	Site 5	Total
Sanitization Performed by SSA Staff	0	7	66	6	47	33	159
Sanitization Performed by a Contractor	45	13	0	57	0	0	115
Total Tested	45	20	66	63	47	33	274
Not Sanitized	**0**	**4**	**0**	**1**	**0**	**0**	**5**
Contained PII	**0**	**3**	**0**	**1**	**0**	**0**	**4**
Hard Drives Missing	**5**	**0**	**34**	**0**	**2**	**0**	**41**

We also found incidents where the Agency released IT equipment that was not properly sanitized. In May 2009, a private citizen called the police after the words "Social Security" appeared when accessing hard drives purchased over the Internet. In March 2010, Office of the Inspector General (OIG) investigators found SSA laptops purchased at a General Services Administration auction had not been sanitized. While the numbers of hard drives containing PII may be relatively small, the above examples reflect the potential risk of negative publicity as well as the risk of disclosing PII.

IT Media Awaiting Disposal Contained PII

We found four of the five unsanitized workstation hard drives contained PII. Our initial testing of server hard drives indicated that some of the hard drives contained data. However, further testing was required to determine the data content of the server hard drives. We performed the additional testing and determined the server hard drives were successfully sanitized of all PII and contained no significant data.

Federal agencies are required to apply NIST guidance to sanitize information system media before disposal.[23] However, SSA's policy and process had some weaknesses. As previously stated, SSA policy does not require testing a sample of sanitized media to verify all data and programs are erased before disposal, nor does it require an employee be designated to certify excess equipment as properly sanitized. A single hard drive can contain a significant amount of PII; therefore, SSA was at risk of a significant PII breach.

[23] See Footnote 11.

During our site visits, we found the following control issue that may also be a contributing factor to why hard drives had not been properly sanitized. At our site visits, we observed that some equipment identified as sanitized was not physically marked as sanitized. This was evident at locations where hard drives were found not to be sanitized. For example, we found workstations marked with Post-It Notes. However, the notes did not stick well, and many had fallen on the floor around the area where the workstations were stored. Therefore, some equipment that had not been sanitized could easily have been mixed up with equipment that had been sanitized. We recommend SSA use a better mechanism to mark IT equipment as sanitized or unsanitized. A better system to identify sanitized equipment will help ensure unsanitized equipment does not leave SSA.

As a result of our testing and findings, the Agency issued a memorandum to all SSA Regional Commissioners outlining procedures for excessing workstations.[24] The memorandum instructed offices to confirm the sanitization of workstations when performed by a contractor and mark sanitized workstations with a sticker or marker. We commend the Agency for its prompt attention to this matter; however, additional controls are necessary to prevent a breach of PII.

SSA should implement an agencywide policy to verify and document the sanitization of IT equipment. The policy should require marking all sanitized equipment and documenting the serial number of the IT media, if removed from the equipment. Furthermore, the policy should require that the sanitization method, date and type of disposal, and the recipient of the equipment be documented. Finally, the policy should require a representative sampling of IT media be tested for sanitization.

IT Media from Equipment Awaiting Disposal Was Missing

We found that hard drives from some equipment awaiting disposal could not be accounted for. NIST guidance states it is critical that an organization maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media.[25]

We found the Agency does not track the serial numbers of hard drives. As shown in Table 2 above, 41 pieces of tested equipment (5 at Headquarters and 36 in the Philadelphia Region) did not contain hard drives. Agency staff stated that hard drives were removed for destruction when they could not be sanitized. In addition to these 41 missing hard drives, the Office of Publications and Logistics Management's Center for Office Property management stated that servers received from Headquarters

[24] SSA Memorandum, *Disk Wiping Procedures for Excessing Workstations – INFORMATION*, February 24, 2010.

[25] NIST SP 800-88, *Guidelines for Media Sanitization*, Section 4.8, September 2006.

components for disposal generally do not contain hard drives. Since the Agency did not track the serial numbers of hard drives, there was no documentation to confirm the removed hard drives' disposition.

In our 2009 report on SSA's compliance with FISMA,[26] we indicated that SSA needed to comply with OMB Memorandum M-06-19 and ensure proper handling of security incidents from the time of detection to final resolution. SSA management stated it strives to comply with OMB timeframes;[27] however, the Agency conducts additional research to confirm a PII incident actually occurred. The circumstances surrounding the 41 missing hard drives make it virtually impossible for SSA to confirm that the missing hard drives constitute a PII incident because SSA does not know whether the hard drives are within SSA's control, destroyed, or in the public domain.

The 41 missing hard drives may contain PII. The Agency stated hard drives are removed for destruction when they cannot be sanitized. SSA, by the very nature of its mission, collects, stores, and maintains a vast amount of PII. OMB requires that agencies report all security incidents involving electronic or physical PII to the U.S. Computer Emergency Readiness Team (US-CERT).[28] OMB guidance indicates that agencies should not distinguish between suspected and confirmed breaches of PII.[29] Accordingly, we believe the Agency should report the 41 missing IT equipment hard drives identified in this report and any future missing IT equipment hard drives to US-CERT.

Further, the five missing hard drives at SSA Headquarters revealed another concern regarding SSA's monitoring of its sanitization contractors. The workstations we selected for testing at Headquarters were awaiting donation and should have contained hard drives. Although the Agency stated the hard drives were removed for destruction and the workstations were erroneously placed on a skid for donation, documentation indicated the five hard drives had been successfully sanitized. SSA stated this documentation was provided by the contractor.[30] Further, the Agency stated it will require the contractor to correct its documentation. However, if the contractor's documentation cannot be relied on, the Agency cannot be assured its hard drives are sanitized and destroyed. We recommend SSA monitor sanitization contractors to ensure tasks are completed properly and correctly documented.

---

[26] FISMA Report: *Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act* (A-14-09-19047), November 2009.

[27] OMB Memorandum M-06-19, *Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investments,* July 12, 2006, requires agencies to report all security incidents involving PII within 1 hour of discovering the incident.

[28] Id. US-CERT is a Federal incident response center located in the Department of Homeland Security.

[29] OMB M-06-19, supra.

[30] We picked up our sample of hard drives from SSA Headquarters workstations on December 4, 2009. We were told this was the sanitization contractors second day at SSA.

On December 31, 2009, the Agency issued a new Request for Quote (RFQ)[31] to provide sanitization and destruction of hard drives in excessed equipment at Headquarters. In this RFQ, the Agency added the requirement to record the serial numbers from the removed hard drives, if destroyed. We commend the Agency for its prompt action; however, the RFQ applies to excessed equipment only at Headquarters. To mitigate the risk of a PII breach, the Agency must ensure all dispositions of IT media removed from equipment are properly tracked.

CONCLUSION AND RECOMMENDATIONS

Our review found that the Agency partially implemented Recommendation 5 from our 2002 report. We also 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 and prevent a breach of PII. Therefore, SSA should:

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 located in the ISSH and its procedures located in AIMS.
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 US-CERT.

[31] An RFQ is a solicitation document used to obtain price, delivery, and other information from prospective contractors.

AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with five of six of our recommendations. The Agency partially agreed with Recommendation 4. The Agency indicated it can revise its policies and procedures to secure hard drives that have been removed from desktops until destruction. We agree that these revisions will assist SSA to prevent a PII breach. However, we believe that tracking the serial numbers of removed hard drives would further assist the Agency to ensure that these hard drives have been properly accounted for. SSA's comments are included in Appendix D.

OTHER MATTERS

After the conclusion of field work, we tested the Agency's disposal of excess IT equipment in four regions[32] to determine if conditions similar to those noted in this report existed in the regions. In two regions, we again observed that some equipment identified as sanitized was not physically marked as sanitized. We found that all 20 server hard drives tested were properly sanitized; however, 2 of 291 workstation hard drives tested were not properly sanitized. One of the workstation hard drives contained PII. No laptops were available to test at the sites we visited.

Based on these results, we determined there is a similar need to improve controls over the disposal of excessed IT equipment outside of SSA's Headquarters and Philadelphia Region. To that end, the corrective action taken in response to the above recommendations should be agencywide.

Patrick P. O'Carroll, Jr.

[32] We performed testing in SSA's Atlanta, Chicago, New York, and Seattle Regions.

Appendices

Acronyms

AIMS	Administrative Instructions Manual System
COP	Center for Office Property
FISMA	*Federal Information Security Management Act of 2002*
FMR	Federal Management Regulation
ISSH	Information System Security Handbook
IT	Information Technology
MRM	Materiel Resources Manual
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPLM	Office of Publications and Logistics Management
OTSO	Office of Telecommunications and Systems Operations
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
RFQ	Request for Quote
SP	Special Publication
SSA	Social Security Administration
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Scope and Methodology

To meet our objective, we:

- Researched related internal and external reviews;
- Researched Agency policies and procedures regarding the disposal of personal property, including the
  - *Information Systems Security Handbook,* Chapter 10.0*, Disposal of Information Technology Media Policy*;
  - *Administrative Instructions Manual System (AIMS), Materiel Resources Manual,* Chapter 04*, Property Management ,* Instruction Number 29*, Disposal of Personal Property*; and
  - *AIMS, Materiel Resources Manual,* Chapter 04*, Property Management,* Instruction Number 31*, Donation of Computer Equipment for Educational Purposes.*
- Reviewed the following criteria:
  - *The Privacy Act of 1974, as amended, 5 U.S.C. 552a;*
  - Office of Management and Budget (OMB) Memorandum M-06-15, *Safeguarding Personally Identifiable Information (PII),* May 22, 2006;
  - OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of PII,* May 22, 2007;
  - OMB Memorandum M-06-19, *Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006;
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009;
  - NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006; and
  - General Services Administration's Federal Management Regulation, Subchapter B – *Personal Property*, Part 102-35 – *Disposition of Personal Property*.
- Reviewed the contracts and records for contractors involved in the sanitization of Agency equipment;
- Interviewed SSA personnel from the Offices of
  - Disability Adjudication and Review, Region III;
  - Operations, Region III;

  - Publications and Logistics Management, Office of Property Management, Center for Office Property; and
  - Systems, Office of Telecommunications and Systems Operations.
- Tested the hard drives of excessed equipment identified as sanitized from Headquarters and the Philadelphia Region to determine whether they were effectively sanitized. We tested the hard drives of equipment at each location in the region within 24 hours of notification.

At Headquarters, we examined 45 workstations identified as sanitized and awaiting donation. Although the Agency had laptops awaiting disposal at Headquarters, we were unable to test their hard drives because the hard drives had not yet been sanitized. Also, no server hard drives were available for testing at Headquarters.

In the Philadelphia Region, we examined all the excessed IT equipment reported as having been sanitized at the Philadelphia Regional Office, one hearing office, and three field offices. The hard drives of two pieces of equipment were damaged and unreadable. We performed additional testing in four of SSA's regions.

We performed our audit at SSA Headquarters and field locations in the Philadelphia Region from January through March 2010. 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.

The Social Security Administration's Media Sanitization Processes

At Headquarters, excess workstations, laptops, and servers were provided to the Office of Publications and Logistics Management's (OPLM) Center for Office Property (COP). Although each component was responsible for removing Social Security Administration (SSA) records and files from the hard drives of its excessed equipment,[1] OPLM's COP oversaw a contractor to sanitize or destroy the hard drives prior to disposal. The Agency stated the Contracting Officer Technical Representative for this contract tested some equipment marked by the contractor as sanitized to ensure sanitization was performed. Hard drives that could not be sanitized by OPLM's COP were taken to the contractor's facility and destroyed.

Further, based on discussions with Agency staff, SSA's components can forward hard drives to the Office of Telecommunications and Systems Operations (OTSO) for destruction. According to OTSO procedures, OTSO sanitizes the hard drives upon receipt, and they are then taken to the contractor's facility and destroyed.

In the Philadelphia Region, each office disposed of its own workstations, laptops, and servers. Sanitization was generally performed by SSA staff; however, offices had the option to have a contractor sanitize old workstations upon installation of replacement workstations. For some sites we visited, SSA staff stated that it tested the sanitized media before disposal. If hard drives could not be sanitized, they were sent to OTSO for destruction by a contractor.

[1] SSA AIMS, *MRM 04.31.05 A.1.*

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: October 8, 2010 Refer To:

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

From: James A. Winn /s/
Executive Counselor
to the Commissioner

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Controls for Ensuring the Removal of Sensitive Data From Excessed Computer Equipment" (A-14-10-11003)—INFORMATION

Thank you for the opportunity to review the draft report. Attached is our response to the report recommendations.

Please let me know if we can be of further assistance. Please direct staff inquiries to Rebecca Tothero, Acting Director, Audit Management and Liaison Staff, at (410) 966-6975.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S CONTROLS FOR ENSURING THE REMOVAL OF SENSITIVE DATA FROM EXCESSED COMPUTER EQUIPMENT" A-14-10-11003

Thank you for the opportunity to review the subject draft report. We offer the following comments.

Recommendation 1

Evaluate its information technology (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.

Comment:

We agree. We have evaluated our IT policies and procedures, and we are preparing a comprehensive update to our Administrative Instructions Manual System (AIMS) guide, Materiel Resources Manual (MRM) 04.29, Disposal of Personal Property, in which we will designate regional employees to assume these roles. As stated in the Information Systems Security Handbook (ISSH), Appendix B, the Site LAN Coordinator (SLC), and the Local Area Network (LAN) administrator are working to implement LAN security standards. Our revised AIMS MRM 04.29 will designate the SLC to follow the ISSH workstation replacement procedures and erase or wipe clean all hard drives before removal from the worksite, or the SLC must oversee the workstation replacement contractor's performance. In addition, we will designate property managers, custodial officers (CO), and alternate custodial officers (ACO) to certify data erased from IT media. Our updated AIMS MRM 04.29 will include instructions to the COs and the ACOs to follow the ISSH procedures and test a representative sample of IT media based on the volume of excessed equipment to ensure we have erased all data.

In our headquarters offices, we will continue to monitor contractor performance to sanitize or destroy the hard drives prior to disposal. In June 2010, we conducted the first sample testing of the headquarters contractor and detected no problems or errors. In the future, we will randomly test the contractor's performance for all services.

Recommendation 2

Identify and resolve the gaps between its IT media sanitization policy located in the ISSH and its procedures located in AIMS.

Comment:

We agree. We will completely update AIMS MRM 04.29 using current ISSH policies and procedures and applicable security references. We will complete the draft guide and make it available for inter-component review.

Recommendation 3

Properly mark excess IT equipment with hard drives as sanitized immediately after sanitization has been performed.

Comment:

We agree. On March 1, 2010, we awarded the sanitization and destruction services contract to Turtle Wings (Data Killers), the headquarters' contractor. The current contract extends through fiscal year 2015 and includes our amended language to mark excess IT equipment.
We are developing a standard label for purchase and distribution to all offices. The label will show pertinent information such as "Pass/Fail Sanitized," "Date Sanitized or Attempted," "SSA Names/Position Titles or Contractor Names for Erasure and Certification," and "Serial Number of Removed Hard Drive(s)." Our new AIMS update will include these new procedures.

Recommendation 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.

Comment:

We partially agree. While working with the OIG we readily agreed to amend the language in the headquarters' blanket purchase agreement sanitizing contract for hard drives marked for destruction. The contractor now includes all information listed in this recommendation in its report to our Office of Publications and Logistics Management.

However, after closer examination of the fifth recommendation in this report and the requirements to implement this process agency-wide we now offer other options. We fully concur with this recommendation for servers that contain multiple hard drives. The vendor provides the hard drive serial numbers associated with each server upon initial acquisition of the

equipment. System's Change, Asset, and Problem Reporting System (CAPRS) tracks the serial numbers of the hard drives in servers, and the information is available from the time of purchase to removal of the hard drives. Desktops present a big challenge. Neither CAPRS nor Sunflower (our property accountability system) includes the hard drive serial number associated with each central processing unit (CPU) desktop. The serial number is unknown, and to obtain the information would prove to be very labor-intensive for our property managers while adding little value to the risk of losing personally identifiable information (PII). While awaiting destruction, the real concern is unauthorized access to these hard drives once removed from the CPU. We can implement the recommendation by revising current policies and procedures in the AIMS guide that require SLCs, property managers, and contractors to remove the hard drives and place them in a secure location with restricted access while awaiting destruction and to destroy laptops and Blackberries if they fail the disk wipe procedures.

Recommendation 5

Properly monitor sanitization contractors to ensure tasks are completed properly and correctly documented.

Comment:

We agree. We amended the March 2010 contract for headquarters and in April 2010 worked with the contractor on our requirements. The contractor performed acceptable services during a visit in June 2010. As needed, we will contact the contractor for future headquarters sanitization and destruction services. For the regional offices, we will add these requirements to our revised AIMS guide that will apply to our employees and contractors.

While some contracts include provisions for the vendor to perform IT media sanitization, it is the responsibility of each of our offices to monitor the vendor properly. When the vendor sanitizes IT media during warranty repair, the vendor is required to maintain a secure chain of custody and provide a monthly report accounting for any recovered IT media.

Recommendation 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 (US-CERT).

Comment:

We agree. We will follow the PII loss procedures in ISSH and will tell our National Network Service Center to relay the information to the US-CERT. We will add these current procedures to our revised AIMS procedures.

[SSA also provided a technical comment that has been addressed, where appropriate, in the report.]

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Audit Manager

Acknowledgments

In addition to those named above:

Michael Zimmerman, Auditor

For additional copies of this report, please visit our Website at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-10-11003.

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.