OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

STATE DISABILITY DETERMINATION SERVICES REMOVAL OF SENSITIVE INFORMATION FROM EXCESSED COMPUTERS

August 2005 **A-14-05-15063**

AUDIT REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: August 4, 2005 Refer To:

To: The Commissioner

From: Inspector General

Subject: State Disability Determination Services' Removal of Sensitive Information from Excessed Computers (A-14-05-15063)

OBJECTIVE

Our objectives were to examine the policies and procedures that the State Disability Determination Services (DDS) follow when excessing computer equipment and to ensure that sensitive information is removed prior to the computer's disposition.

BACKGROUND

In February 2004, we were made aware of audit results from a North Carolina State Auditors[1] report in which they had selected a sample of computers that were excessed by a variety of State agencies. The auditors found that the majority of these machines had hard drives that were readable, and data files that were accessible, which included password files and other sensitive information. Some of these computers were from the North Carolina Department of Health and Human Services, which is the parent agency for the North Carolina DDS.

The Social Security Administration's (SSA) Office of Federal Disability Determination Services (FDDS) and the 54 DDSs make disability determinations and process disability claims. DDSs use various software applications, known as case processing systems, to develop, review and process disability determinations. These case processing systems run on various hardware platforms,[2] which store and process sensitive information. This information includes individual names and addresses, Social Security numbers and medical information of disability claimants.

---

[1] The State of North Carolina, Office of the State Auditor, *Information Security Assessment: Implementation of Enterprise Security Standard S003, Permanent Removal of Data from Electronic Media,* February 2004.

[2] The type of computer on which a given operating system or application runs.

Wang computers were used by 26 of the DDSs and the FDDS as their hardware platform. Each of these sites has migrated from using Wang computers to IBM iSeries (AS/400) computers as their hardware platform, with the exception of Nebraska, which is in the process of migrating to an SSA-standard server platform. As of January 25, 2005, SSA data showed that of the 27 Wang computers, 12 have been disposed of and the remaining 15 are still on-site at the DDSs.

According to SSA's Disability Determination Services Security Document (DSD),[3] DDSs are required to run the SSA approved Wipe Disk software utility on equipment that was used for the storage of sensitive information (servers, laptops, workstations, etc) prior to its disposal or donation to another entity. Wipe Disk is a software program that "wipes" or erases a disk drive of its data by overwriting the entire drive with repetitive characters, making the data irretrievable.

To test whether equipment had been properly cleansed of sensitive data prior to its being excessed, we selected four DDS sites and requested a list of computer equipment on-site ready for disposal. Table 1 below shows the equipment selected from each DDS site for testing.

TABLE 1

DDS Site	Servers	Laptops	Workstations	Total
District of Columbia	0	0	10	10
North Carolina	0	5	5	10
Pennsylvania	2	12	7	21
Delaware	0	0	6	6
Total	**2**	**17**	**28**	**47**

[3] Disability Determinations Services Security Document (September 2003), page 36.

RESULTS OF REVIEW

Data on all servers, laptops and workstations that we forensically tested at the four selected sites had been properly removed with the Wipe Disk utility. However, we identified two issues which potentially affect equipment used in a significant number of the DDSs. These issues relate to the limitations of the Wipe Disk utility and its ability to remove sensitive data from computer equipment in the DDSs.

First, DDSs are potentially excessing Wang computers without ensuring that data is irretrievable from the hard drives. The Wipe Disk utility does not work on Wang computers. Therefore, the Wang computers still on-site at the DDSs are at risk of being excessed with sensitive data intact.

Second, two of the four selected DDSs had boxes of obsolete server tapes on-site.[4] Because these tapes were used as server back-ups[5] they may contain sensitive information. Systems personnel at these DDSs informed us that they were storing the tapes because they were unaware of any guidance from SSA on how to remove data before disposal of the tapes.

Wang computers are potentially being excessed with sensitive data intact

DDSs are potentially excessing Wang computers without ensuring that data is irretrievable from their hard drives. As noted previously in the Background section, Wang computers were used by 26 of the DDSs and the FDDS. As a result, claimants' medical or personal information, as well as sensitive SSA data is at risk of being compromised. When equipment is taken out of service and prepared for disposal, the Wipe Disk utility must be used by DDSs to cleanse the hard drive of sensitive information. Of the four DDSs we selected for testing, two still had their obsolete Wang computers on-site and the remaining two DDSs did not use Wangs.

An individual from the Office of Public Service and Operations Support provided guidance to the regions via e-mail stating that there is not a utility, such as Wipe Disk, that can be used on the Wang computers. This individual recommended that the regions reformat the hard drives to make the data irretrievable. However, reformatting a hard drive does not make the information stored irretrievable, as there are software utilities that can reformat the data back into its original content. For example, the audit report issued by the North Carolina State Auditors noted that they were able to rebuild and gain access on all of the hard drives that had been reformatted prior to their being excessed.[6] If the hard drives had been reformatted for any of the previously excessed Wang computers, these drives may still contain sensitive data.

[4] The obsolete server tapes retained at the two DDSs were from both Wang and non-Wang equipment.
[5] Back-up is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.
[6] The State of North Carolina, Office of the State Auditor, *Information Security Assessment: Implementation of Enterprise Security Standard S003, Permanent Removal of Data from Electronic Media,* February 2004, page 7.

Ideally, the Agency would seek a software utility similar to Wipe Disk to use for the disposition of the Wang computers still on site at the DDSs. However, it appears that no such utility exists. Until such time, it is advisable for SSA to instruct the DDSs to remove or physically destroy the hard drives prior to the disposal or donation of these computers to another entity. Once the Agency determines an appropriate method of ensuring that data is irretrievable from these computers, official guidance should be disseminated to the DDSs.

Obsolete server tapes are still being held

Two of the four selected DDS sites stored old magnetic tapes from obsolete servers. These tapes were used for server back-ups and may contain sensitive information. The DSD mandates the use of Wipe Disk on equipment used for data storage such as hard drives, but does not address how to ensure sensitive data is removed from other storage media with which Wipe Disk utility is incompatible. One such storage medium with which Wipe Disk is incompatible is magnetic media tapes.

SSA's Program Operations Manual System (POMS) requires disposal of any claimant data in such a manner as to make the data irretrievable to unauthorized personnel and that magnetic tapes are to be erased before the tapes are released to other users.[7] However, POMS does not address the method for erasing the data. Some methods of erasing data will not make it irretrievable to unauthorized personnel. The Wipe Disk utility only overwrites the hard drive or drives on a device and does not work on magnetic tapes.

The DDS systems personnel in these two offices stated they were unaware of SSA guidance on how to dispose of these tapes. While the DSD is intended to supplement existing policies and procedures in the POMS, the guidance relevant to systems security for DDSs needs to be uniform. The Agency should determine an appropriate method of ensuring that data is removed from obsolete server tapes and other media. Once determined, the DSD and POMS should be updated to reflect this method. SSA also needs to ensure that DDS employees are aware of the appropriate policy.

[7] POMS, section DI 39566.080.

CONCLUSIONS AND RECOMMENDATIONS

The DSD requires DDSs to run the SSA approved Wipe Disk utility on equipment that was used for the storage of sensitive information prior to its disposal or donation to another entity. Data had been properly removed from all excess servers, laptop and desktop computers that we forensically tested. However, there is not an appropriate method of ensuring that data is irretrievable from obsolete Wang computers. In addition, the DSD does not clearly mandate a method for removing data from other storage media such as server tapes. As a result sensitive information on obsolete Wang computers and server tapes are at risk.

We recommend SSA:

1. Direct DDSs either to ensure data is irretrievable or physically remove and destroy the hard drives on computers to be excessed.

2. Modify or update the DSD and POMS to ensure the Agency's guidance is complete and consistent regarding the proper method of removing data from and disposing of obsolete server tapes.

3. Ensure DDS personnel are aware of the policy and procedures to dispose of any claimant data in such a manner as to make the data irretrievable to unauthorized personnel.

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix C for the text of SSA's comments.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

DDS	Disability Determination Services
DSD	Disability Determination Services Security Document
FDDS	Office of Federal Disability Determination Services
OIG	Office of the Inspector General
POMS	Program Operations Manual System
SSA	Social Security Administration

Scope and Methodology

Our objectives were to examine the policies and procedures that the State Disability Determination Services (DDS) follow when excessing computer equipment and to ensure that sensitive information is removed prior to the computer's disposition.

To accomplish these objectives, we selected four DDS sites (North Carolina, District of Columbia, Pennsylvania and Delaware) and requested a list of computer equipment, if any, that they had on-site and were ready for disposal:

- From the District of Columbia equipment list, we selected 10 out of 33 pieces of equipment for testing, and we performed our testing on-site.

- We selected 10 out of 22 pieces of equipment for testing from the North Carolina inventory of surplus equipment. Five of these items were tested on-site. The remaining five were brought back to the Office of the Inspector General's (OIG) headquarters in Baltimore for testing.

- From the Pennsylvania equipment list, we selected all 21 pieces of equipment for testing, and we performed our testing on-site.

- From the Delaware equipment list, we selected 6 out of 49 pieces of equipment for testing and we requested that the DDS systems personnel remove the hard drives from 6 workstations that were being excessed. These hard drives were then transported back to the OIG headquarters and tested.

To accomplish our testing we used EnCase®, a forensic software product that enabled us to read the contents of the hard drives being tested. We also interviewed DDS personnel as to the policies and procedures they followed for disposing computer equipment to verify that they were following Social Security Administration policy. Our work was performed at the selected sites from June 2004 to February 2005 in North Carolina, District of Columbia, Pennsylvania, Delaware and Maryland. We conducted our review in accordance with generally accepted government auditing standards.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

34321-24-1358
Refer To: S1J-3

Date: July 15, 2005

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

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "State Disability Determination Services' Removal of Sensitive Information from Excessed Computers" (Audit No. 22005015)—INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report are attached.

Please contact me if you have any questions. Staff questions may be referred to Candace Skurnik, Director of the Audit Management and Liaison Staff, at extension 54636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "STATE DISABILITY DETERMINATION SERVICES' REMOVAL OF SENSITIVE INFORMATION FROM EXCESSED COMPUTERS" (A-14-05-15063)

Thank you for the opportunity to review and provide comments on this OIG draft report. We agree with the thrust of the report. The Social Security Administration (SSA) has a responsibility to protect our clients' sensitive data from compromise during the disposal process, and we take that responsibility very seriously. SSA maintains and enforces effective policies and procedures for protecting sensitive data during its disposal. As noted in this OIG report, the data disposal issues at Disability Determination Service (DDS) offices are limited in scope. We are working to resolve these issues to ensure that sensitive data is not compromised.

Recommendation 1

Direct DDSs either to ensure data is irretrievable or physically remove and destroy the hard drives on computers to be excessed.

Comment

We agree. We are working to develop appropriate methods to ensure that sensitive data is removed from all electronic media prior to its disposal. Until the procedures are ready, we have instructed the DDSs that have Wang processors and backup tapes not to excess them until we are sure the data can be completely destroyed.

The draft report highlights two problem areas: 1) limitations of the Wipe Disk utility as it applies to Wang servers; and 2) DDSs storing obsolete server tapes in lieu of guidance from SSA on how to dispose of them. SSA is working with a contractor to design an optimal process to ensure that sensitive data is eradicated from the Wang proprietary hardware prior to its disposal. As noted in the OIG draft report, Nebraska is the only State still using a Wang server and they are migrating away from it. Of the 15 Wang servers mentioned in the OIG report, 14 are currently out of production and the 15th soon will be.

In the area of tape disposal, we are working to finalize a proposal that, once implemented, will resolve this issue. In the interim, the DDSs and other SSA offices are temporarily storing tapes until they can be degaussed, rather than risking the inadvertent release of sensitive data.

Recommendation 2

Modify or update the DDS Security Document (DSD) and Program Operations Manual System (POMS) to ensure the Agency's guidance is complete and consistent regarding the proper method of removing data from and disposing of obsolete server tapes.

Comment

We agree. The DSD and POMS (subchapter DI 39566.000 DDS' Privacy and Security) will be updated once we have developed the appropriate methods to ensure that sensitive data is removed from all electronic media prior to its disposal including the data from the Wang processors and backup tapes.

Recommendation 3

Ensure DDS personnel are aware of the policy and procedures to dispose of any claimant data in such a manner as to make the data irretrievable to unauthorized personnel.

Comment

We agree. On June 8, 2005, we provided a reminder to SSA regional offices requesting that they instruct the DDSs that have Wang processors and backup tapes not to excess them until we are sure the data can be completely destroyed. Once we have developed appropriate methods for ensuring that sensitive data is removed from the subject electronic media prior to its disposal, we will provide any necessary additional reminders to SSA regional offices and the DDSs. Currently, the DSD provides instructions to the States regarding disposal of claimant data. We will ensure that the DSD and POMS are updated to include language that the data should be irretrievable to unauthorized personnel.

[In addition to the information listed above, SSA also provided technical comments which have been addressed, where appropriate, in this report.]

OIG Contacts and Staff Acknowledgments

OIG Contacts

Albert Darago, Acting Director, Data Analysis and Technical Audits Division (410) 965-9710

Phil Rogofsky, Audit Manager, Network Security and Telecommunications Branch (410) 965-9719

Acknowledgments

In addition to those named above:

Greg Thompson, Senior Auditor

Annette DeRito, Writer/Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-14-05-15063.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

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, Subcommittee on Human Resources

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

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

Chairman and Ranking Minority Member, Committee on Governmental Affairs

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 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 our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Executive Operations (OEO). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises 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 and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity 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 OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG 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. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.