U.S. Department of Labor

Office of Inspector General—Office of Audit

OFFICE OF THE ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT

DOL NEEDS TO PERFORM ELECTRONIC MEDIA SANITIZATION MORE EFFECTIVELY PRIOR TO TRANSFER OR DISPOSAL

Date Issued: September 30, 2005
Report Number: 23-05-028-50-598

U.S. Department of Labor
Office of Inspector General
Office of Audit

BRIEFLY…

Highlights of Report Number: 23-05-028-50-598, to the Assistant Secretary for Administration and Management / Chief Information Officer.

WHY READ THE REPORT

This report contains information as to the effectiveness of the Department of Labor's electronic media sanitization procedures. This report includes findings and recommendations as to how the Department can better sanitize electronic media prior to its transfer or disposal.

WHY OIG DID THE AUDIT

News stories show a disturbing trend concerning the disposal of surplus electronic media. CNET news reported two Massachusetts Institute of Technology students purchased 158 used disk drives for less than $1000. These students found 129 disk drives were still working, and contained thousands of active credit card numbers, along with pharmaceutical records, legal correspondence, corporate memoranda, and email messages.

During survey work in 2003, OIG found that 85 percent of the computers that were ready to be transferred or disposed of contained varying degrees and combinations of licensed operating system software, licensed application software, and data of a sensitive, personal, and/or confidential nature. As a result of this survey work, the Department took immediate corrective action. To follow-up on the correction action taken by the Department, we initiated the audit and testing of the Department's policies and procedures regarding electronic media sanitization.

The objective of our audit was to determine if DOL is effectively sanitizing surplus electronic media prior to transfer or disposal in order to minimize the risk associated with unintentional release of information.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full agency response, go to: http://oig.dol.gov/public/reports/oa/2005/23-05-028-50-598.pdf

September 2005

DOL Needs To Perform Electronic Media Sanitization More Effectively prior to Transfer or Disposal

WHAT OIG FOUND

The OIG found that DOL regional office computer hard drives that were ready to be transferred or disposed of were properly sanitized. The OIG found that national office computer hard drives that were ready to be transferred or disposed of contained varying combinations of licensed operating system software, licensed application software, and unencrypted data of a sensitive, personal and/or confidential nature.

WHAT OIG RECOMMENDED

We recommended that the Assistant Secretary for Administration and Management take the following actions:

- Review the implementation of the department-wide electronic media sanitization policy for uniformity and develop verification procedures that include testing.
- Coordinate with each Agency's Information Technology Security Officer to ensure future IT specific security training includes proper sanitization of electronic media.
- Periodically verify agencies' effectiveness in sanitizing electronic media to assure adequate security.
- Research emerging technologies as an additional measure to protect DOL information assets.

The Office of the Assistant Secretary for Administration and Management generally agreed with the report and has begun taking actions to address the findings and recommendations.

Table of Contents

PAGE

PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Executive Summary

We conducted a performance audit of the Department of Labor (DOL) to determine if surplus electronic media were being effectively sanitized prior to transfer or disposal.

The results of a limited survey conducted by the Office of Inspector General (OIG) in 2003, found that 85 percent of the surplus computers tested contained varying degrees and combinations of licensed operating system software, licensed application software, and data of a sensitive, personal, and/or confidential nature. As a result of the survey, the OIG issued Alert Report Number 23-03-009-04-001, *Electronic Media Disposal*, to the Chief Information Officer (CIO) on March 27, 2003. In response to that report, the CIO took immediate corrective action, declaring a moratorium on the release of surplus electronic media, and updating disposal procedures to address the sanitization of electronic media. To follow up on the corrective action taken by the CIO, we initiated the audit and testing of the Department's policies and procedures regarding electronic media sanitization.

We performed this audit in accordance with *Generally Accepted Government Auditing Standards* issued by the Comptroller General of the United States.

The objective of our audit was to determine if DOL is effectively sanitizing surplus electronic media prior to transfer or disposal in order to minimize the risk associated with unintentional release of information.

Results

We found:

1. Regional office agencies' computer hard drives that were ready to be transferred or disposed of were properly sanitized; and

2. National office agencies' computer hard drives that were ready to be transferred or disposed of contained varying degrees and combinations of licensed operating system software, licensed application software, and unencrypted data of a sensitive, personal and/or confidential nature.

We attribute unsanitized computer hard drives to weaknesses and/or noncompliance with DOL procedures in assuring electronic media are being properly sanitized during the disposal phase of a system's development life cycle. The DOL and its agencies do have electronic media sanitation policies and procedures to protect licensed computer software and electronically stored data from unintentional release during the process of transfer or disposal. However, procedures for sanitizing electronic media allow for inconsistencies and/or bypassing certain steps.

Recommendations

We recommend the Assistant Secretary for Administration and Management (ASAM) take the following actions:

1. Review the department-wide electronic media sanitization policy for uniformity, develop verification procedures that include testing, and enforce the implementation of the updated procedures throughout the sanitization and disposal process.

2. Coordinate with each Agency's Information Technology (IT) Security Officer to ensure future IT-specific security training includes proper sanitization of electronic media.

3. As a part of the Office of Chief Information Officer's testing of DOL's information security program, periodically verify agencies' effectiveness in sanitizing electronic media to assure adequate security at the disposal phase of a system's life cycle.

Additionally, we recommend the ASAM take the following long-term action:

4. Research emerging technologies, e.g., file encryption software, as an additional measure to protect DOL information assets throughout the Department.

Office of Assistant Secretary of Administration (OASAM) and Management Response

OASAM management provided a written response to the draft report issued September 30, 2005. OASAM concurred with the findings and generally agreed with the recommendations. In their response, OASAM provided information on the actions taken to resolve the recommendations.

OIG Conclusion

Based on the OASAM response to the draft report, all four recommendations are resolved.

Following our recommendations, we have provided management's written response and the OIG's conclusion. The OIG's conclusion specifies the actions that need to be taken to close the recommendations.

U.S. Department of Labor

Office of Inspector General
Washington, DC 20210

Assistant Inspector General's Report

Patrick Pizzella
Assistant Secretary of Administration
and Management
Chief Information Officer

We conducted a performance audit of the DOL to determine if surplus electronic media were being effectively sanitized prior to transfer or disposal.

During our survey work in 2003, we found that 85 percent of the computers that were ready to be transferred or disposed of contained varying degrees and combinations of licensed operating system software, licensed application software, and data of a sensitive, personal, and/or confidential nature. As a result of this survey work, the Department took immediate corrective action. To follow up on the corrective action taken by the CIO, we initiated the audit and testing of the Department's policies and procedures regarding electronic media sanitization.

We tested 24 computer hard drives from the DOL regional offices and 22 computer hard drives from the DOL national offices. In the DOL regional offices, we found electronic media were properly sanitized. In the national office, we found 11 of the 22 computer hard drives tested were not properly sanitized. On those 11 computer hard drives, we found sensitive DOL information, financial information of DOL program participants and personal information as well as licensed DOL software and operating systems.

We performed this audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

Background information pertaining to our audit is detailed in Appendix A. Our audit scope, methodology, and criteria are detailed in Appendix B.

Objective – Is the Department of Labor effectively sanitizing surplus electronic media prior to transfer or disposal in order to minimize the risk associated with unintentional release of information?

Results and Findings

The table below shows the number of surplus computer hard drives tested by location, and the types of information found to be present.

Testing Results by Location				
Office Location	**# of Computer Hard Drives Tested**	**Licensed Operating System Found**	**Licensed Application Software Found**	**Sensitive, Personal, or Confidential Data Found**
National	22	11	8	5
Philadelphia	6	0	0	0
Denver	5	0	0	0
Chicago	3	0	0	0
Dallas	10	0	0	0
TOTALS	**46**	**11**	**8**	**5**

All DOL Regional Office Computer Hard Drives Were Sanitized

Of the 24 computer hard drives tested from the DOL regional offices, we found no computer hard drives containing sensitive, personal and/or confidential information, licensed operating system, or application software.

Half of DOL National Office Computer Hard Drives Were Not Properly Sanitized

Of the 22 computer hard drives tested from the DOL national offices, we found 11 computer hard drives contained sensitive, personal and/or confidential information, licensed operating system and/or application software.

From the 11 unsanitized computer hard drives, we identified the following:

- 11 Licensed Operating Systems: Windows 98 (3), Windows XP (4), Windows NT (3), and Solaris (1)
- 8 Licensed Software Applications: MS Office Suite

Also, from 5 of the 11 unsanitized computer hard drives, OIG recovered information that is considered sensitive, personal, and/or confidential. The types of sensitive, personal and/or confidential information included:

- Over 4,000 names and social security numbers of US service men and women who were Job Training Partnership Act clients;
- A draft report of the Department of Labor Critical Asset List, including system name and identification, physical location of system, function of system, and summary of impact if system becomes unavailable;
- An Employment Standards Administration (ESA) Voucher and Schedule of Payments for Federal Employees' Compensation Act (FECA) recipients, dated 7/26/2002. This report includes recipient name, address, banking account number, bank routing number, and amount of FECA check received for hundreds of recipients;
- A personal resume;
- A file containing an employee's system user ID and password; and
- A phone and address contact list for a Boy Scout troop.

The table below shows, by agency, the surplus computer hard drives OIG tested and the three types of information found to be present.

Testing Results by Agency

Agency	# of Computer Hard Drives Tested	Licensed Operating System Found	Licensed Application Software Found	Sensitive, Personal, or Confidential Data Found
OASAM	21	4	3	1
ETA	2	1	0	1
OIG	5	0	0	0
MSHA	1	1	0	0
ESA	17	5	5	3
TOTALS	**46**	**11**	**8**	**5**

OIG's testing results demonstrated that there are weaknesses with the Department's procedures to assure electronic media are being properly sanitized during the disposal phase of a system's life cycle.

We attribute unsanitized computer hard drives to the weaknesses and/or noncompliance with DOL procedures in assuring electronic media are being properly sanitized. Specifically, procedures for sanitizing electronic media allow for inconsistencies and/or bypassing certain steps, verification procedures are not working as designed, agencies are not properly transferring media to OASAM, and there is no requirement for training personnel. The following identify examples of the weaknesses:

- In evaluating departmental procedures, we reviewed a departmental memorandum dated January 26, 2005, reminding agencies of DOL procedures for disposing of computers and electronic media. In this memorandum there are different procedures for Departmental Management (DM) agencies[1], non-DM agencies[2] in the Frances Perkins Building, and other non-DM agencies not located in the Frances Perkins Building. Each of these three groups has distinct processes and procedures to follow, which allow for inconsistencies and/or bypassing certain steps at the national and regional offices. For DM agencies, the Computer Technology Center (CTC) is the responsible organization for sanitizing departmental agencies' electronic media. The memorandum also established that the CTC is responsible for completing verification of the sanitization's effectiveness. Establishing the CTC to be responsible for both sanitizing and verifying its own work led to the transfer and disposal of electronic media that contains inappropriate information.

- The same memorandum additionally states, as part of the disposal process, agencies are required to document the sanitization of electronic media prior to its transfer or disposal using the Electronic Media Disposal Sanitation Certificate (DL1-55A)[3]. Of the eight agencies' policies and procedures[4] we reviewed, procedures for two agencies, MSHA and ESA, specify the use of in-house forms rather than the use of the official form, DL1-55A. One agency, BLS, does not document the sanitization of electronic media prior to transfer or disposal.

- Prior to the January 26, 2005 memorandum, surplus computers were being transferred to the Business Operations Center (BOC) for disposal without the required disposition documentation. Of the 12 computers we selected from the Frances Perkins Building loading dock for testing; only 5 had complete documentation. BOC management acknowledged that 7 of the 12 computers selected were machines that were transferred to BOC for disposal without proper documentation. In addition, after the memorandum was issued, additional

[1] DM agencies are defined as agencies that utilize the services of Office of Assistant Secretary for Administration (OASAM) and Management for technical support, e.g., Office of Chief Financial Officer, Office of the Solicitor, Women's Bureau, and OASAM.
[2] Non-DM agencies are defined as agencies that maintain their own technology support staff: Occupational Safety and Health, Bureau of Labor Statistics, Office of Inspector General, Employment Training Administration, and Employment Standards Administration.
[3] This is not a new requirement; the memorandum reiterates and clarifies procedures previously issued by the Department of Labor Management Series.
[4] There are eight agencies in the department with policy and procedures for the sanitizing and disposal of electronic media, they are: OASAM, BLS, EBSA, ESA, ETA, MSHA, OIG, and OSHA.

computers containing unsanitized computer hard drives were found in DOL hallways.

- OASAM personnel stated that staff responsible for the proper sanitization of electronic media were not getting the necessary training.

The Federal Information Security Management Act (FISMA) of 2002 requires agencies to:

> . . . (b) Agency Program. . . (C) ensure that information security is addressed throughout the life cycle of each agency information system. . . .

National Institute of Standards and Technology (NIST) Guidance, Special Publication 800-26, establishes:

> . . . Like other aspects of an IT system, security is best managed if planned for **throughout the IT system life cycle** [emphasis added]. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and **disposal** [emphasis added]. . . .

The Department of Labor Manual Series, (DLMS) 9 – Information Technology, Chapter 300*, Management and Accountability of Information Resources*, section 306 C (11), page 9, states that Agency Heads are responsible to:

> Document that appropriate measures have been taken to protect against unintentional release of DOL information when information resources are processed through excess property procedures or donated outside of DOL.

Additionally, the DLMS 2 – Administration, Chapter 100, *DOL Property Management*, section 108 D (4), page 17 states:

> Electronic Media Disposal Sanitation Certificate (DL[1-]55A) must be completed for all sanitized electronic media.

The DLMS 9 - Information Technology, section 407 A, pages 4-8 states that the CIO:

> . . . must develop and implement the Department-wide ISS [Information System Security] program and ensure that agencies are carrying out agency-wide ISS programs.

The manual further states that the CIO is responsible to:

> . . . develop and/or oversee development of:
>
> - Information technology policies;

- Standards, plans and guidance;
- Architectures, processes, and methodologies

that ensure all information stored, disseminated, or transmitted by DOL-owned information systems or by other systems provided for DOL use under contract or subcontract is properly safeguarded against unauthorized access, use modification, destruction, or denial of service through he integration of management, operational, and technical controls.

OASAM memorandum, Reminder: Disposing of Computers and Electronic Media, dated January 26, 2005, states that any electronic media transferred to OASAM for disposal must be accompanied by a DL1-55A Electronic Media Sanitization Disposal Certificate that has been signed by the appropriate agency official. The memorandum also states that,

> . . . at no time should CPUs or other electronic media be left unattended in common areas, such as hallways. Instead, it must be stored in the internal office space of the DOL Agency to which it is assigned until it has been disposed of properly.

Without implementing and following consistent sanitization procedures and establishing a sound verification process that includes testing across the Department, adequate sanitization of electronic media cannot be assured and may lead to intentional and/or unintentional release of information, which may compromise the Department's security of its infrastructure, information assets, employees, and the public's trust.

Recommendations

We recommend the ASAM take the following actions:

1. Review the department-wide electronic media sanitization policy for uniformity, develop verification procedures that include testing, and enforce the implementation of the updated procedures throughout the sanitization and disposal process.

2. Coordinate with each Agency's Information Technology (IT) Security Officer to ensure future IT-specific security training includes proper sanitization of electronic media.

3. As a part of the Office of Chief Information Officer's testing of DOL's information security program, periodically verify agencies' effectiveness in sanitizing electronic media to assure adequate security at the disposal phase of a system's life cycle.

Additionally, we recommend the ASAM take the following long-term action:

4. Research emerging technologies, e.g., file encryption software, as an additional measure to protect DOL information assets throughout the Department.

Agency Response

OASAM management submitted to OIG their comments on the draft report. These comments were embedded into the draft report by OASAM and forwarded to OIG as an attachment to the Deputy Assistant Secretary for Operations, September 30, 2005, memorandum to the Assistant Inspector General for Audit. The comments are excerpted below.

1. OASAM management agrees with the first recommendation. The OASAM Office of the Chief Information Officer (OCIO) will review the Department's policies for electronic media sanitization to ensure consistency in the implementation of procedures throughout the agencies. Since the initial audit in December 2004, the Department has revised and implemented new procedures for sanitizing electronic media and its tracking disposal. Additionally, further guidelines have been drafted to ensure that procedures are consistent and that periodic reviews are performed to ensure that electronic media are properly sanitized and that all data are no longer retrievable. These guidelines will be issued in the first quarter of FY 2006.

2. OASAM management agrees with the second recommendation. The OCIO provided training on electronic media protection and sanitization in the FY '05 Computer Security Awareness and Training (CSAT) required for all DOL employees. Additionally, the users identified as having significant security responsibilities were required to take supplementary training via the USA Learning Karta library, which contains more specific information with respect to electronic media sanitization. In consultation with each Agency's Information Technology (IT) Security Officer, the OCIO will review the planned curriculum for the FY '06 CSAT to ensure that the topic continues to be adequately covered.

3. OASAM management agrees with the third recommendation. Updated guidelines have been drafted for electronic media sanitization. The guidelines specify that the Agency Information Security Officers (ISOs) are to perform periodic verification of media sanitization and that testing be performed based on the sensitivity of the data resident on the system or media. The guidance further calls for separation of duties between the Agency ISO and the staff performing the media sanitization process so that verification is an independent function. In addition, the OCIO will periodically evaluate the effectiveness of the electronic media sanitization policy and guidelines implementation. The updated guidelines will be issued in the first quarter of FY 2006.

4. OASAM Management agrees with the fourth recommendation and has an existing process that is well adapted to its implementation. Emerging technologies are reviewed and approved by the Technical Review Board (TRB) and its Subcommittees – Enterprise Architecture Subcommittee (EASC), IT Security Subcommittee (ITSSC) and the IT Architecture Subcommittee (ITASC). The ITASC proactively researches the industry to ensure the Department is abreast of new and emerging technologies. The ITASC is then responsible for providing recommendations to the EASC regarding the impact of the emerging technology on the Department's infrastructure. The ITSSC and the EASC review the technology from a security and overall infrastructure perspective to ensure there are no security risks associated with it's implementation and to ensure that the technology fits into the Department's and the Federated EA, which includes the use of secure technologies and standards. The TRB and its subcommittees are all comprised of representatives from each agency as well as advisors from each OCIO program area – Security, Capital Planning, and Enterprise Architecture. This existing representative body will continue to implement the governance process, referenced above, that ensures compliance to recommendation four.

OIG Conclusion

Based on the OASAM response to the draft report, all four recommendations are **resolved**.

To close recommendation 1 and recommendation 3, OASAM should provide the new guidelines to the OIG for testing to ensure the guidelines reduce the risk of unsanitized electronic media from leaving the Department.

To close recommendation 2, OASAM should provide the OIG access to review the FY '06 CSAT to ensure that the topic is adequately covered.

To close recommendation 4, OASAM should provide documentation of the TRB and subcommittee research of products for securing information at the desktop level, such as file level encryption.

Elliot P. Lewis
August 26, 2005

Appendices

PAGE HAS BEEN INTENTIONALLY LEFT BLANK

APPENDIX A

BACKGROUND

Current news stories show a disturbing trend concerning the disposal of surplus electronic media. CNET news reported two Massachusetts Institute of Technology students purchased 158 used disk drives for less than $1,000. These students found 129 disk drives were still working, and contained thousands of credit card numbers, medical records, and detailed personal and financial information. The Washington Post recently published an article stating 40 million computers became obsolete in 2001. Many of these obsolete computers are being shipped to foreign countries. In the past, reports have surfaced that federal agencies have disposed of surplus electronic media without taking appropriate measures to erase the information stored on the media. This can lead to disclosure of sensitive information, embarrassment to the agency, costly investigations, and other avoidable consequences.

In 2003, we conducted a survey of electronic media disposal in the Department of Labor. We tested 21 surplus computers from the OASAM loading docks at the national office, and found that 85 percent of them contained licensed software and/or recoverable data.

Federal Regulations mandate that government agencies protect data maintained about individual citizens from unauthorized release. Policies and procedures should be established to protect DOL licensed software and sensitive data stored on electronic media before release, transfer, or disposal. Our survey work during the planning phase indicated that DOL management had not established or implemented policies and procedures sufficiently specific to prevent the unintentional release of licensed software and sensitive data stored on electronic media. On March 27, 2003, an Alert Report was issued to the CIO recommending a moratorium on the release of surplus computers until hard disk drives could be sufficiently sanitized. We also recommended the CIO update policy and provide guidance to the agencies in this area. In response to that report, the CIO took immediate corrective action, declaring a moratorium on the release of surplus electronic media, and updating disposal procedures to address the sanitization of electronic media.

PAGE HAS BEEN INTENTIONALLY LEFT BLANK

APPENDIX B

OBJECTIVE, SCOPE, METHODOLOGY, AND CRITERIA

Objective

The following is the objective of the audit:

> Is the Department of Labor effectively sanitizing surplus electronic media prior to transfer or disposal in order to minimize the risk associated with unintentional release of information?

Scope

Our audit included a departmental level review of the sanitization and disposal of electronic media by agencies. We made a judgmental selection of electronic media that was being processed for disposal. We tested the disposed electronic media to determine if it was sanitized. If we determined that it was not sanitized, we performed additional tests to identify if there were any 1) licensed operations system, 2) licensed application system and 3) sensitive, personal or confidential information on the electronic media.

Audit fieldwork was conducted from December 21, 2004 through August 26, 2005, at DOL Headquarters in the Frances Perkins Building in Washington, DC, and at DOL regional offices.

Methodology

We conducted our audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States, and included tests on internal controls, as we considered necessary, to satisfy the objectives of the audit.

We acquired electronic media deemed for disposal from various sources and locations in DOL to determine if sanitation had occurred. We performed further analysis of DOL and its agencies' policies and procedures for compliance with Federal and its own policies and procedures.

We made a judgmental selection of electronic media that was being processed for disposal. In some instances, DOL employees contacted us when electronic media was transferred or disposed. We judgmentally selected the media based upon size and location of the disposed media. In addition, we selected media we found abandoned in

hallways. Our sampling was selected in this manner due to the infrequent disposal of media and the decentralization of DOL.

From those samples, we tested the media using procedures known as a keyboard attack, which consists of recovering information using tools and software that is readily available to any user.

To understand the Federal and DOL requirements of electronic media sanitization and disposal process, we obtained an understanding of the information listed in the criteria section.

We reviewed OASAM policies and procedures related to the disposal of surplus electronic media. We also reviewed the policies and procedures of the departmental agencies to ensure compliance with DOL policy.

Criteria

We used the following criteria to perform this audit:

- Government Accountability Office manual, *Federal Information System Controls Audit Manual (FISCAM)*
- *Federal Information Security Management Act 0f 2002 (FISMA)*
- DLMS 2 Administration, Chapter 100 – *DOL Property Management.*
- DLMS 9 Information Technology, Chapter 400 – *Security*
- DLMS 9 Information Technology, Chapter 300 – *Management and Accountability of Information Resources*
- Department of Labor *Systems Development Lifecycle Management Manual*, version 2.1
- Department of Labor Information Technology Center *Standard Operating Procedure: Media Sanitation for Surplus Equipment, National Office ECN*
- OASAM memorandum: Reminder: Disposing of Computers and Electronic Media, dated January 26, 2005
- NIST Special Publication 800-64 Rev. 1, *Security Considerations in the Information System Development Life Cycle*
- NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
- NIST Special Publication 800-26, *Self-Assessment Guide for Information Technology Systems*
- Public Law 93-579, 5 U.S.C. 552a*, The Privacy Act of 1974*
- Department of Labor *Computer Security Handbook*, version 2.0
- NIST *Media Sanitization Procedures*
- NIST Special Publication 800-18, *Guide for Developing Security Plans For Information Technology Systems*

PAGE HAS BEEN INTENTIONALLY LEFT BLANK

APPENDIX C
ACRONYMS AND ABBREVIATIONS

BLS	Bureau of Labor Statistics
BOC	Business Operations Center, OASAM
CIO	Chief Information Officer
CTC	Computer Technology Center
DOL	Department of Labor
EBSA	Employee Benefits Security Administration
ECAB	Employees' Compensation Administration Board
ESA	Employment Standards Administration
ETA	Employment and Training Administration
FECA	Federal Employees' Compensation Act
FISMA	Federal Information Security Management Act
FISCAM	Federal Information System Controls Audit Manual
MSHA	Mine Safety and Health Administration
NIST	National Institute of Standards and Technology
OASAM	Office of the Assistant Secretary of Administration and Management
OIG	Office of Inspector General
OSHA	Occupational Safety and Health Administration
SOL	Office of the Solicitor
WB	Women's Bureau

PAGE HAS BEEN INTENTIONALLY LEFT BLANK

APPENDIX D

AGENCY RESPONSE TO DRAFT REPORT

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

SEP 3 0 2005

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: EDWARD C. HUGLER
Deputy Assistant Secretary for Operations

SUBJECT: Electronic Media Sanitization
Draft Audit Report No. 23-05-018-50-598

This memorandum responds to the September 30, 2005 draft report of the Office of Inspector General's (OIG) Audit of the Department's Electronic Media Sanitization processes and procedures.

We recognize that there remains opportunity for improvement and acknowledge the need for refining our policies, procedures, and implementation guidance for the sanitization of electronic media prior to its disposal. OASAM's management responses have been incorporated into the draft audit report, following each of the OIG's recommendations.

We appreciate the opportunity to respond to the OIG's recommendations. If you have any questions regarding our response please contact me at (202) 693-4040, or have your staff contact either Al Stewart at Stewart.Milton@dol.gov or (202) 693-4021 or Tom Wiesner at Wiesner.Thomas@dol.gov or (202) 693-4200.

Attachment

cc: Patrick Pizzella, ASAM, CIO
Al Stewart, OASAM
Tom Wiesner, OASAM
Keith Galayda, OIG
Steve Fowler, OIG