U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico

DOE/IG-0735

August 2006

Department of Energy
Washington, DC 20585

August 3, 2006

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico"

BACKGROUND

The Department of Energy's Sandia National Laboratory-New Mexico develops science-based technologies in support of national security in areas such as nuclear weapons, nonproliferation, military technologies, and homeland security. In fulfilling its national security mission, Sandia utilizes classified computer systems extensively. Department policy requires that all classified removable electronic media be strictly controlled and provides specific policies and procedures for its destruction when it is no longer needed.

The Office of Inspector General received information regarding potential internal control weaknesses at Sandia associated with the disposal of classified computer hard drives. As a result, we initiated an inspection to determine if internal controls for the destruction of Sandia's classified hard drives were adequate to assure the protection and control of the classified material. During our preliminary inquiries, we determined that in June 2004 Sandia suspended its off-site destruction of classified hard drives due to concerns that had arisen. In addition, an October 2004 National Nuclear Security Administration Sandia Site Office review found that classified hard drives were only being degaussed, not destroyed in accordance with DOE policy, and that Sandia's internal tracking database was incorrectly annotated to indicate that the classified hard drives had been destroyed. Our review subsequently followed up on these issues and examined other internal controls related to the handling and protection of classified hard drives.

RESULTS OF INSPECTION

We concluded that internal controls for the destruction of Sandia's classified hard drives were not adequate to assure the protection and control of the classified material. Specifically, our inspection confirmed that although classified hard drives were degaussed, they were not destroyed as required by Department policy. We also found that, contrary to policy, Sandia did not:

- Maintain an audit trail for accountable classified removable electronic media through actual destruction, to include properly annotating destruction records;

- Assure that classified hard drives were destroyed the same day they were removed from the site;

Printed with soy ink on recycled paper

- Obtain Department approval prior to using an off-site destruction facility; and,

- Assure that the destruction of classified hard drives was accomplished by an appropriately cleared person and that the destruction of accountable classified hard drives was witnessed by an appropriately cleared individual.

In October 2005, the Laboratory obtained Sandia Site Office approval of a new security plan for the destruction of its classified hard drives. Subsequently, we conducted additional field work to determine whether the new security plan addressed the above internal control weaknesses. We determined that the plan specified that an off-site destruction facility would be used to destroy the drives, so the Site Office's approval of the plan addressed the requirement for the Laboratory to obtain Department authorization prior to using an off-site destruction facility. However, the plan did not address the other internal control weaknesses; thus, the resumption of off-site destruction of classified hard drives resulted in continuing noncompliance with applicable Department policy.

Miscommunication and differing interpretations of Department policy led to the problems we identified, particularly with regard to the role degaussing plays in the accountability, declassification, and destruction of classified media. This is an issue that has significant implications with respect to the protection of some of the most sensitive information in this Nation. Therefore, we recommended that the Chief Information Officer, in coordination with the Director of the Office of Security and Safety Performance Assurance and the Associate Administrator for Defense Nuclear Security, (1) fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media and (2) based upon that analysis, issue specific policy on the role degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media. Pending the outcome of these actions, we recommended that Sandia suspend the off-site destruction of its classified media.

MANAGEMENT REACTION

In responding to a draft of this report, the Chief Information Officer, whom Department directives assign responsibility for cyber security policy, concurred with the report recommendations and agreed that internal controls for the destruction of Sandia's classified hard drives were not compliant with Department policy or adequate to assure the protection and control of classified material. The Director of the Office of Security and Safety Performance Assurance confirmed that under current Department cyber security policy degaussing is not an approved method of destruction for media and that there are risks associated with the use of degaussing as a method for declassifying classified media. The Director stated that, due to the complicated technical nature of this subject and since no apparent related National policy exists, the Office of the Chief Information Officer has queried its National Security Agency Customer Advocate requesting information to be used in determining the extent to which degaussing may be used to destroy magnetic media or reliably and permanently purge all data from such media.

The National Nuclear Security Administration's Associate Administrator for Management and Administration stated that the National Nuclear Security Administration believes that internal controls at Sandia are adequate and in full compliance with Department regulations for disposing of classified material. He also stated that once classified hard drives have been degaussed, they

are no longer classified and are released from accountability. This position was inconsistent with the position expressed by the Department's Chief Information Officer. Although the Associate Administrator did not state whether or not he concurred with our recommendations, his specific comments made it clear that he did not believe that any further action was warranted.

Management's verbatim comments are provided at Appendix B of the report. We found the Chief Information Officer's and the Director of the Office of Security and Safety Performance Assurance's comments to be responsive to our report findings and recommendations. We found the National Nuclear Security Administration's comments to be contrary to Department policy. This policy is contained in directives that specifically state they are applicable to the National Nuclear Security Administration. Admittedly, this is a complex issue with important national security ramifications; thus, we believe it is incumbent upon the Department to implement a complex-wide policy based upon a sound risk assessment.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary of Energy
Under Secretary of Science
Chief of Staff
Director, Office of Security and Safety Performance Assurance
Manager, Sandia Site Office
Director, Policy and Internal Controls Management (NA-66)
Director, Office of Internal Review (CF-1.2)
Audit Liaison, Sandia Site Office

DESTRUCTION OF CLASSIFIED HARD DRIVES AT SANDIA NATIONAL LABORATORY-NEW MEXICO

TABLE OF CONTENTS

OVERVIEW

Introduction and Objective..... 1

Observations and Conclusions..... 1

DETAILS OF FINDINGS

Destruction of Hard Drives……..... 3

Adherence to Policy……. 3

Continuing Concerns…… 5

Policy…….. 6

RECOMMENDATIONS…… 8

MANAGEMENT COMMENTS…… 8

INSPECTOR COMMENTS…… 10

APPENDICES

A. Scope and Methodology…… 11

B. Management Comments……... 12

Overview

INTRODUCTION AND OBJECTIVE

The Department of Energy's (DOE's) Sandia National Laboratory-New Mexico (Sandia) develops science-based technologies in support of national security in areas such as nuclear weapons, nonproliferation, military technologies, and homeland security. In fulfilling its national security mission, Sandia utilizes classified computer systems extensively. Sandia has at least 1,400 pieces of classified removable electronic media. DOE policy requires that all classified hard drives be strictly controlled and provides specific policies and procedures for their destruction when they are no longer needed. Sandia is administered by the National Nuclear Security Administration (NNSA) and is operated for NNSA by Sandia Corporation, a subsidiary of Lockheed Martin Corporation.

The Office of Inspector General received information regarding potential internal control weaknesses at Sandia associated with the disposal of classified computer hard drives. As a result, we initiated an inspection to determine if internal controls for the destruction of Sandia's classified hard drives were adequate to assure the protection and control of the classified material.

During our preliminary inquiries, we determined that in June 2004 Sandia suspended its off-site destruction of classified hard drives because it perceived a "requirements gap" in its contract with respect to the allowable methods and processes for destroying classified computer media. In addition, an October 2004 Sandia Site Office Safeguards and Security survey report identified that "Classified hard drives, including . . . ACREM[1] [accountable classified removable electronic media], are being degaussed[2], but not destroyed in accordance with DOE policy," and Sandia's "accountability records [internal tracking database] are incorrectly annotated to indicate that the classified hard drives have been destroyed." Our review subsequently followed up on these issues and examined other internal controls related to the handling and protection of classified hard drives.

OBSERVATIONS AND CONCLUSIONS

We concluded that internal controls for the destruction of Sandia's classified hard drives were not adequate to assure the protection and control of the classified material. Our inspection confirmed

[1] ACREM is media classified at the Secret/Restricted Data level and above, to include Sigmas 1, 2, 14, and 15, and is more strictly controlled than other classified removable electronic media (i.e., Secret/Formerly Restricted Data, Secret/National Security Information, and below).
[2] Degaussing is a method to magnetically erase data from magnetic media.

that classified hard drives were degaussed but were not destroyed as required by DOE policy and that Sandia did not properly annotate its internal tracking database. We also found that, contrary to DOE policy, Sandia did not:

- Maintain an audit trail for ACREM through actual destruction, to include properly annotating destruction records;
- Assure that classified hard drives were destroyed the same day they were removed from the site;
- Obtain DOE/NNSA approval prior to using an off-site destruction facility;
- Assure that the actual destruction of classified hard drives was accomplished by an appropriately cleared person; and
- Assure that the actual destruction of accountable classified hard drives was witnessed by an appropriately cleared individual.

On October 6, 2005, after the majority of our inspection fieldwork was completed, Sandia obtained Site Office approval of a security plan that included the use of an off-site destruction facility in another State. Subsequently, on October 11, 2005, Sandia lifted its suspension of off-site destruction of classified hard drives and began shipping its backlog to the off-site destruction facility.

Subsequently, we conducted additional field work to determine whether the new security plan addressed the above internal control weaknesses. While the Site Office approval of the security plan addressed the requirement to obtain authorization to use an off-site destruction facility, this plan did not address the other internal control weaknesses detailed above. Thus, the resumption of off-site destruction of classified hard drives resulted in continuing noncompliance with applicable DOE policy.

Miscommunication and differing interpretations of DOE policy regarding the destruction of classified hard drives have led to the problems identified in this report, particularly with regard to the role degaussing plays in the accountability, declassification, and destruction of classified media. Thus, we believe that the destruction of classified media by Sandia should cease until the policy issues have been fully resolved.

DESTRUCTION OF HARD DRIVES

We confirmed that classified hard drives were degaussed but were not destroyed as required by DOE policy and that Sandia did not properly annotate its internal tracking database.

DOE policy requires that classified matter be destroyed beyond recognition to preclude reconstruction or recovery of any information it contained. Authorized destruction methods include pulverizing, smelting, incinerating, disintegrating, or other appropriate methods. However, we determined that Sandia did not destroy its classified hard drives accordingly. Instead, Sandia degaussed the classified hard drives, to include both ACREM and non-accountable classified removable electronic media, and incorrectly recorded the accountable hard drives as "destroyed" in the Laboratory Administrative Document System, which is Sandia's internal tracking database.

After degaussing, Sandia relinquished control of the classified hard drives to private companies not cleared for access to classified material. Specifically, on 13 occasions from June 2002 to May 2004, Sandia used an uncleared private transportation company to ship thousands of pounds of degaussed classified hard drives to an uncleared recycling facility in another State, where this material was to be recycled and/or destroyed.

ADHERENCE TO POLICY

We also found that, contrary to DOE policy, Sandia did not:

- Maintain an audit trail for ACREM through actual destruction, to include properly annotating destruction records. DOE policy requires that an audit trail be maintained that provides documentary evidence of processing or other actions related to the security of an automated information system. Each piece of ACREM must be assigned a unique identification number and tracked from inception through destruction. The destruction of ACREM must be documented on DOE Form 5635.9, Record of Destruction, or a similar form, and the form must be signed by both the individual destroying the matter and a witness. We determined that Sandia used its Receipt for Classified Information as its record of destruction, and the receipt was marked "destroyed" and the audit trail for the ACREM was terminated when the associated ACREM was degaussed, not when it was actually destroyed. No record was prepared to document the actual destruction of the ACREM, nor were there any signatures of the person destroying the ACREM or a witness.

- Assure that classified hard drives were destroyed the same day they were removed from the site. DOE policy requires that if classified matter cannot be destroyed on-site, it must be destroyed at a public destruction facility by a cleared individual on the same day it is removed from the site. However, the "Certificate of Destruction & Recycling" issued by the recycling facility was routinely dated anywhere from one to six days after the shipping date. Furthermore, a representative of the recycler told us that the hard drives the company received were accumulated in bins for two to three months until the bins were full and that, in all likelihood, they were sent to the recycler's sister company in another State for extraction of precious metals. As a result, destruction may not have taken place for months after the hard drives left Sandia.

- Obtain DOE/NNSA approval prior to using an off-site destruction facility. DOE policy requires that the DOE security office approve the use of public destruction facilities. However, the Sandia Site Office was not aware that classified hard drives were being sent to an out-of-State recycling facility and did not approve the use of this facility for off-site destruction of the classified hard drives. Further, the Sandia Site Office was not aware that the recycling facility was likely sending the hard drives to its sister company in another State and did not approve the use of this second facility.

- Assure that the actual destruction of classified hard drives was accomplished by an appropriately cleared person. DOE policy requires that the destruction of classified matter be accomplished by an individual who has appropriate access authorization for the classification of the matter to be destroyed. However, Sandia shipped both accountable and non-accountable classified hard drives to an uncleared facility, where their destruction was accomplished by uncleared personnel.

- Assure that the actual destruction of accountable classified hard drives was witnessed by an appropriately cleared individual. DOE policy requires that the destruction of accountable classified matter be witnessed by an appropriately cleared individual other than the person destroying the matter. However, we were told by a representative of the recycling facility, which had no cleared employees, that no cleared individual accompanied the shipments of classified media during the June 2002 to May 2004 time frame to witness destruction.

CONTINUING CONCERNS

On October 6, 2005, after the majority of our inspection fieldwork was completed, Sandia obtained Site Office approval of a security plan that included the use of an off-site destruction facility in another State. On October 11, 2005, Sandia lifted its suspension of off-site destruction of classified hard drives and began shipping its backlog to the off-site facility for destruction. While the Site Office approval addressed the requirement to obtain authorization to use an off-site destruction facility, this plan did not address the other internal control weaknesses detailed above. Thus, the resumption of the destruction of classified hard drives resulted in continuing noncompliance with applicable DOE policy. Specifically, the Site Office allowed Sandia to:

- Disregard maintaining an audit trail for ACREM through actual destruction. The plan allowed Sandia to remove classified markings from degaussed hard drives prior to shipment and co-mingle accountable classified media with other degaussed classified and unclassified media. The approved security plan did not provide for an audit trail using the item's unique identification number as required by DOE policy. Instead, the approved security plan provided for tracking ACREM as bulk items commingled with unclassified material.

- Destroy classified hard drives up to several days after leaving the Laboratory. The plan allowed Sandia to destroy hard drives "the same day they are received" at the off-site destruction facility, with a grace period of up to 72 hours, despite DOE policy requiring destruction the same day classified matter is removed from the site.

- Ignore the requirement that the destruction of classified hard drives be accomplished by a cleared person. The plan allowed Sandia to use uncleared personnel from the off-site destruction facility to handle and destroy the classified hard drives.

- Degrade the requirement that the destruction of ACREM be witnessed by an appropriately cleared individual. Sandia's plan provided for a cleared individual to accompany the shipments of classified hard drives and to witness destruction. However, since the plan allowed Sandia to co-mingle accountable classified media with non accountable classified media and unclassified media, there was no way a witness could attest to the actual destruction of the accountable material.

POLICY

Miscommunication and differing interpretations of DOE policy regarding the destruction of classified hard drives have led to the problems identified in this report, particularly with regard to the role degaussing plays in the accountability, declassification, and destruction of classified media.

Miscommunication on Policy

The internal control weaknesses that existed until the June 2004 suspension of off-site destruction appeared to be the result of a miscommunication between NNSA and Sandia that lead Sandia to assume it had authorization to consider all degaussed classified media as destroyed. A December 4, 2002, memorandum from the then Albuquerque Operations Office, which had cognizance over Sandia at the time, approved an October 15, 2002, request from the Sandia Manager of Security Operations to use specific types of degaussers at Sandia. However, also included in Sandia's request was the statement that "The degaussers would be used to **destroy** [emphasis added]" magnetic computer media up to and including Top Secret Restricted Data. While the Albuquerque Operations Office approval memorandum only addressed the request to use specific degausser equipment, Sandia interpreted the approval as an authorization to treat degaussing as destruction.[3]

The internal control weaknesses that subsequently existed, however, were the result of the Sandia Site Office's October 2005 approval of Sandia's security plan. The premise for this plan was primarily based on a March 2005 memorandum from the Site Office Manager that stated the Associate Administrator for Defense Nuclear Security advised that ACREM may be considered non-ACREM after it had been degaussed and that continued accountability of the degaussed media was no longer required. The security plan then went beyond this and allowed ACREM to be co-mingled with other degaussed classified and unclassified hard drives and treated as "unclassified protected [Sandia] property" prior to actual destruction.

Differing Interpretations of Policy

Sandia Site Office officials told us that they believe degaussing classified media constitutes declassification of that media under existing policy and that the approved security plan reflects this position. The Site Office further said that since degaussed classified removable electronic media (including ACREM) was no longer classified, it could be co-mingled and treated as "unclassified protected Sandia property." The Site Office officials told us that NNSA was coming out with new policy to clarify and support

[3] On three occasions prior to the December 4, 2002, Albuquerque Operations Office memorandum, Sandia had already shipped degaussed classified media to the uncleared recycling facility.

this position. An NNSA official confirmed that NNSA intended to issue policy clarification in this area.

The DOE policies and procedures that govern the destruction of classified hard drives are promulgated by two DOE organizations: the Office of Security and Safety Performance Assurance (SSA) and the Office of the Chief Information Officer (OCIO). These policies, which specifically state they are applicable to NNSA, do not identify degaussing as an authorized method for declassification of classified media. DOE policy specifically assigns the OCIO responsibility for Department-wide cyber security policy and guidance. An official from the OCIO told us that ACREM must be treated as classified from creation through destruction. In addition, the official told us that the OCIO does not support the position that degaussing classified media constitutes declassification of that media because there is too much margin for error in the degaussing process. The official questioned how this risk was being evaluated and accepted by NNSA.

Further, Sandia's continuing treatment of degaussed classified media as unclassified contravenes a May 2005 finding by SSA's Office of Independent Oversight and Performance Assurance. This office found that "NNSA . . . has interpreted Departmental policy on media destruction and ACREM storage to contradict established DOE requirements, and has provided those interpretations [and] clarifications to the field elements." SSA also noted that NNSA indicated to the Sandia Site Office by e-mail that degaussing alone allows ACREM to be removed from accountability, which contradicts the long-established DOE precept of establishing accountability upon media generation, and accountability termination upon media destruction.

DOE policy only recognizes degaussing as a form of sanitization, and several factors must work together to make it effective and assure that information can never be reconstructed or recovered. These factors include the utilization of authorized and appropriate degaussing equipment, proper calibration of that equipment, and user training and compliance with manufacturer recommendations. As part of our inspection, the Office of Inspector General, in coordination with the United States Secret Service, examined 32 degaussed Sandia classified hard drives using various types of forensic analysis. The degaussing process is supposed to wipe out the service area of the drive, making the drive unrecognizable to the computer. However, the service area on one of the hard drives appeared to operate normally. Although no data was observed, this

illustrates the need to destroy classified matter beyond recognition to preclude reconstruction or recovery of any information it may contain.

Given the differing interpretations of existing Department policy on the declassification and destruction of classified media and the lack of specific Department policy that degaussing may be used as a method for declassifying classified media and removing it from accountability, we believe that Sandia should suspend the off-site destruction of media that has been used for classified processing until the policy issues raised herein have been fully resolved.

RECOMMENDATIONS

We recommend that the Chief Information Officer, in coordination with the Director of the Office of Security and Safety Performance Assurance and the Associate Administrator for Defense Nuclear Security:

1. Fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media, and, based upon that analysis, issue specific policy on the role degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media.

We also recommend that the Associate Administrator for Defense Nuclear Security take appropriate action to ensure that:

2. Sandia suspends the off-site destruction of media that has been used for classified processing until the policy issues identified in this report have been fully resolved.

3. Sandia's declassification and destruction of classified media complies with Department policy and that any deviations from policy are appropriately processed.

MANAGEMENT COMMENTS

Management's comments are summarized below and are included in their entirety at Appendix B of this report.

The Chief Information Officer concurred with the report recommendations and agreed that internal controls for the destruction of Sandia's classified hard drives were not compliant with DOE policy or adequate to assure the protection and control of classified material.

The Director of SSA stated that determining whether degaussing is a form of destruction for magnetic media that contains classified information falls within the purview of the OCIO and that under current DOE cyber security policy, degaussing is not an approved method of destruction for media. The Director stated that the risk associated with the use of degaussing as a method for declassifying classified media is that some of the classified information may remain on the media after the media has been degaussed, recoverable by a typical user or through technical means.

With regard to Recommendation 1, the Director stated that, due to the complicated technical nature of this subject and since no apparent related National policy exists, the OCIO has queried its National Security Agency (NSA) Customer Advocate requesting information to be used in determining the extent to which degaussing may be used to destroy magnetic media or reliably and permanently purge all data from such media. The Director stated that if new information is acquired by the OCIO or his office from NSA or other means, degaussing as an approved means of destroying magnetic media may be codified in DOE cyber security policy.

The NNSA Associate Administrator for Management and Administration stated that NNSA believes that internal controls at Sandia are adequate and in full compliance with DOE regulations for disposing of classified material. With regard to Recommendation 1, the Associate Administrator stated that the correct use of degaussing products ensures that classified data is no longer retrievable and that since classified data is no longer on the media, the hard drives are no longer classified or accountable. The Associate Administrator stated that "As shown, we have analyzed this position and believe that we meet the intent of the IG's recommendation. We do not believe that any new policy is applicable."

With regard to Recommendation 2, the Associate Administrator stated that hard drives that have gone through degaussing no longer meet the criterion to remain in accountability. He also stated that although media that previously contained classified data must be physically destroyed, the controls are not the same as for classified removable electronic media; therefore, it may be destroyed off-site.

With regard to Recommendation 3, the Associate Administrator stated that the Sandia Site Office approved Sandia's plan for destruction of classified media and that Sandia is not required to submit a deviation from policy. He stated that Sandia tracks

"formerly accountable hard drives from end to end" and "can identify which formerly accountable hard drive was in which container number that was shredded and recycled." He also stated that the Site Office conducted a survey of Sandia that included the destruction of classified media, and no deficiencies were found. The Associate Administrator stated that NNSA believes it has met the intent of the recommendation.

INSPECTOR COMMENTS

We found the comments from the Chief Information Officer and the Director of SSA to be responsive to the report recommendations. However, we found the NNSA Associate Administrator's comments to be inconsistent with DOE policy and the comments provided by the Chief Information Officer and the Director of SSA. Specifically, under current DOE cyber security policy, degaussing is not an approved method of declassification or destruction for classified media. NNSA's comments did not cite specific Department policy to the contrary or to otherwise support its position. Therefore, we stand by our recommendations.

Appendix A

SCOPE AND METHODOLOGY

The fieldwork for this inspection was completed in May 2006. We interviewed Sandia and DOE officials knowledgeable about the destruction of classified hard drives at the Laboratory. We also interviewed officials from the private companies associated with the destruction of Sandia's classified hard drives. We gathered and reviewed relevant documentation, including DOE Orders, Notices, and Manuals; Sandia Site Office reports and memoranda; and Sandia procedures, memoranda, electronic mails, corrective action plans, subcontracts, Laboratory Administrative Document System listings, Receipts for Classified Information, and Bills of Lading.

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Department of Energy
Washington, DC 20585

July 12, 2006

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: GLENN S. PODONSKY
DIRECTOR
OFFICE OF SECURITY AND SAFETY
PERFORMANCE ASSURANCE

SUBJECT: COMMENTS FOR IG DRAFT INSPECTION REPORT – Destruction of Classified Hard Drives at Sandia National Laboratory (sic), New Mexico (SO5IS047)

The Office of Security and Safety Performance Assurance (SSA) has reviewed the subject draft inspection report provided by the Inspector General's memorandum of June 16, 2006, and provides the following comments.

Recommendation:

We recommend that the Director of the Office of Security and Safety Performance Assurance, the Chief Information Officer, and the Associate Administrator for Defense Nuclear Security:

1. Fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media, and issue specific policy on the role degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media.

Management Response:

Within DOE and its contractor community, determining whether degaussing is a form of destruction for magnetic media that contains classified information falls within the purview of the DOE Office of the Chief Information Officer (OCIO). The Office of Security and Safety Performance Assurance (SSA) determines the criteria and requirements for determining classification level and accountability of matter.

Due to the complicated technical nature of this subject and since no apparent related National policy exists, OCIO has queried its National Security Agency (NSA) IAD-Customer Advocate requesting information to be used in determining the extent to which degaussing may be used to destroy magnetic media or reliably and permanently purge all

Printed with soy ink on recycled paper

data from such media. If new information is acquired by OCIO or SSA, from NSA or other means, degaussing as an approved means of destroying magnetic media may be codified in DOE cyber security policy.

In general, the risk associated with the use of degaussing as a method for declassifying classified media is that some amount of classified information may remain on the media after the media has been degaussed. First, it is possible all of the information is not purged from the media through the degaussing process, allowing a typical user to directly access some amount of classified information from the degaussed media. Second, if all of the information has been appropriately exposed to the degaussing process, it may be that technical means exist to recover the data.

It is known that the strength of a degaussing process and the total residual risk posed by degaussed media are dependent on multiple factors, including the operating characteristics of the specific degaussing equipment, and the coercivity and physical configuration of the media to be degaussed. Furthermore, the working condition of a degausser may deteriorate over time or due to malfunction. However, it is also recognized that under certain conditions, degaussing as destruction may be sufficient to meet the intent of absolutely preventing unauthorized access to classified information.

Currently, under DOE cyber security policy, degaussing is not an approved method of destruction for media. If, following further study, OCIO identifies degaussing as an approved form of media destruction, the prescribed degaussing process must absolutely preclude the recovery of any information from media destroyed this way. If this can be assured, then it might be appropriate to re-designate this media as unclassified and/or non-accountable, thus "destroyed", even though it has not been physically destroyed. In these cases, specific requirements for validating that no classified information can be recovered from degaussed media must include formal certification, testing and accreditation of all associated technology, equipment and processes. Additionally, performance testing criteria and a quality assurance program, such as a sampling of the degaussed media to ensure that the degaussing equipment is functioning properly will need to be established. If any information may be directly accessed, or otherwise recovered, after the media has been degaussed, then the media must retain its previous status regarding classification and accountability.

In short, DOE is currently engaged in the technical and policy investigations that will ensure that the cited recommendation will be fully addressed. The precise timing of these investigations depends upon when technical data becomes available from other government agencies, as noted above.

cc: Thomas Pyke Jr., IM-1
Bill Hunteman, IM-30
Adrian Gardner, IM-30
Michael Kilpatrick, SP-1
Lesley Gasperow, SP-1.2
Barbara Stone, SP-60

Department of Energy
Washington, DC 20585

July 18, 2006

MEMORANDUM FOR ALFRED K. WALTER
ASSISTANT INSPECTORGENERAL FOR INSPECTIONS
AND SPECIAL INQUIRIES

FROM: THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER

SUBJECT: Draft Inspection Report on *Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico* (SO5ISO47)

In response to your request for comments on the subject inspection, the Office of the Chief Information Officer concurs with each recommendation. Based on our review of the draft inspection report we agree that internal controls for the destruction of Sandia's classified hard drives were not compliant with Department of Energy (DOE) policy or adequate to assure the protection and control of classified material. As noted in the draft inspection report, contrary to DOE policy, Sandia did not:

- Maintain an audit trail for accountable classified removable electronic media through actual destruction, to include properly annotating destruction records;
- Assure that classified hard drives were destroyed the same day they were removed from the site;
- Obtain DOE/National Nuclear Security Administration approval prior to using an off-site destruction facility;
- Assure that the actual destruction of classified hard drives was accomplished by an appropriately cleared person; and
- Assure that the actual destruction of accountable classified hard drives was witnessed by an appropriately cleared individual.

The draft inspection report outlines the following recommendation that the Director of the Office of Security and Safety Performance Assurance, the Chief Information Officer, and the Associate Administrator for Defense Nuclear Security should take:

> Fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media and issue specific policy on the role that degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media.

Printed with soy ink on recycled paper

In response to the above recommendation, the following table identifies corrective actions that will be taken by the Department:

Planned Corrective Action	Responsible Organization	Target Date for Completion of Action
1. Fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media	Office of the Chief Information Officer	30 days following the formal issuance of the Inspection Report
2. Issue guidance on the role that degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media	Office of the Chief Information Officer	60 days following the formal issuance of the Inspection Report

If you have any questions or comments, please contact Bill Hunteman on (202) 586-4775.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

JUL 24 2006

MEMORANDUM FOR Alfred K. Walter
Assistant Inspector General
for Inspections and Special Inquiries

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Classified Hard Drive Destruction Draft Report; S05IS047/2006-23761

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Destruction of Classified Hard Drives at Sandia National laboratory-New Mexico." We understand that this inspection was the result of an allegation that the Internal Controls for the disposal of classified hard drives were inadequate.

While we appreciate the IG's efforts, NNSA believes that the Internal Controls at Sandia are adequate and in full compliance with DOE regulations for disposing of classified material. We provide our rationale in our response to each of the recommendations, as follows.

Recommendation 1

> Fully analyze the risk associated with allowing degaussing to be used as a method for declassifying classified media, and issue specific policy on the role degaussing plays in the requirements pertaining to the accountability, declassification, and destruction of classified media.

Departmental Manuals 470.4-4; 205.1; and the National Industrial Security Program Operating Manual specify that degaussing, commonly called erasure, leaves the domains in random patterns with no preference to orientation, thereby rendering previous data unrecoverable. Proper degaussing ensures that there is insufficient magnetic remanence to reconstruct the data. Degaussing is specified in both Departmental and National policy as an approved method for sanitizing certain types of media. The correct use of degaussing products ensures that classified data is no longer retrievable. Since classified data is no longer on the

Printed with soy ink on recycled paper

media, the hard drives are no longer classified. The Information Security Manual provides the criteria for determining whether specific matter is accountable. Any media that meet this criterion must be maintained in accountability. However, if magnetic accountable electronic media are properly sanitized they no longer contain any of the information that required them to be accountable, therefore, releasing them from accountability. As shown we have analyzed this position and believe that we meet the intent of the IG's recommendation. We do not believe that any new policy is applicable.

Recommendation 2

> Ensure that Sandia suspends the off-site destruction of media that has been used for classified processing until the policy issues identified in this report have been fully resolved.

While the report identified hard drives as classified hard drives after degaussing, as described in our comment to recommendation 1, hard drives that have gone through degaussing no longer meet the criterion to remain in accountability. Since all classified data is removed the hard drive may be removed from Classified Matter Protection and Control and is not subject to accountability, as stated. Media that previously contained classified data is required to be physically destroyed, but not under the same controls as Classified Removable Electronic Media, therefore, it may be destroyed off-site.

Recommendation 3

> Ensure that Sandia's declassification and destruction of classified media complies with Department policy and that any deviations from policy are appropriately processed.

Sandia Site Office's Safeguards and Security office and the Designated Accreditation Authority approved the Classified Matter Protection and Control Destruction Plan for the Laboratory in October 2005. The Laboratory is not required to submit a deviation from policy. The Laboratory has and continues to track formerly accountable hard drives from end to end. The practice employed can identify which formerly accountable hard drive was in which container number that was shredded and recycled. Destruction documentation is on file and attached to the respective bill of lading that pertains to the transport of the hard drives to the approved commercial destruction facility. Additionally, personnel security controls are in place with appropriately cleared personnel at the time it is transferred from the Laboratory to the commercial destruction site.
There is no requirement to survey the commercial destruction facility. In April

3

2006, the Site Office conducted a survey of the Laboratory, which included destruction. Results concluded that no deficiencies were found. NNSA believes, therefore, that we have met the intent of the recommendation.

Should you have any questions related to this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: William Desmond, Associate Administrator for Defense Nuclear Security
Patty Wagner, Manager, Sandia Site Office
David Boyd, Senior Procurement Executive
Karen Boardman, Director, Service Center

IG Report No. DOE/IG-0735

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message clearer to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith at (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.