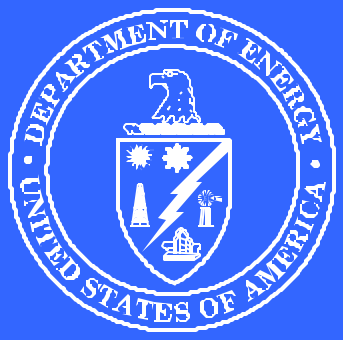
DOE/IG-0472

INSPECTION REPORT



U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

INSPECTION OF SURPLUS COMPUTER EQUIPMENT MANAGEMENT AT THE SAVANNAH RIVER SITE

JUNE 2000

U.S. DEPARTMENT OF ENERGY
Washington, DC 20585

June 1, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (signed)
Inspector General

SUBJECT: INFORMATION: Report on "Inspection of Surplus Computer Equipment Management at the Savannah River Site"

BACKGROUND

By letter dated November 1, 1999, Senator Strom Thurmond advised the Office of Inspector General of an allegation that computer equipment containing over 40 computer hard drives reportedly containing classified or sensitive information were surplused and sold by the Department's Savannah River Site (SRS). The letter raised the concern that the release of this information might pose a threat to the national security of the United States. The management and operating contractor at SRS, Westinghouse Savannah River Company (Westinghouse), is responsible for the final disposal of surplus equipment, including computer hard drives.

The purpose of our inspection was to review the allegation concerning the sale of surplus computer equipment. The objectives of our inspection were to determine whether: (1) surplus computer equipment was disposed of in accordance with Federal and Department requirements, and (2) Government-owned computer equipment at SRS was properly cleared of sensitive information prior to disposal.

RESULTS OF INSPECTION

The inspection disclosed that Westinghouse failed to comply with Department and SRS requirements for disposal of surplus computer equipment. Specifically, despite Departmental requirements, Westinghouse had not cleared stored information from all surplus computers nor did it certify that the computers were sanitized prior to disposal.

Prior to our inspection, Westinghouse initiated a "preliminary inquiry" when an employee of an off-site buyer of computer equipment reported discovering a floppy disk labeled "Secret-Restricted Data" (Secret) among equipment purchased from SRS. Westinghouse reviewed a sample of 23 hard drives and 17 floppy disks found in surplused computer equipment off-site, and found that "very few of the drives [in the sample] had been cleared." SRS officials later determined the secret disk did not contain classified information. However, some of the hard drives and floppy disks sampled did contain Unclassified Controlled Nuclear Information (UCNI) and other sensitive unclassified information. The release of UCNI appears to have violated section 148 of the Atomic Energy Act. Further, computer equipment containing UCNI is considered high risk personal property the disposal of which is subject to specific Department of Energy requirements.

We learned that the disk marked secret, as well as hard drives and floppy disks containing UCNI, were among two trailer loads of computer equipment being processed for a September 1999 shipment to the People's Republic of China (PRC). This computer equipment was reacquired and destroyed. However, the inspection disclosed that other SRS computer equipment had been shipped to the PRC in the July 1999 timeframe. The shipper told us that he believed the shipment did not contain hard drives. But, he acknowledged that no inventory records of the shipment were kept. Thus, we had no way to determine the exact content of this shipment. We noted that over 16,000 computers and computer related items were sold publicly by SRS during Fiscal Years 1998 and 1999.

Following the off-site discovery of computer equipment containing sensitive unclassified information and UCNI, Westinghouse decided that all future surplus computers and related equipment would be destroyed to prevent the release of sensitive information. We concluded that the blanket destruction of all surplus computers and related equipment is not required by Department of Energy property disposal regulations. Savannah River management commented that Westinghouse has now reversed the policy of destroying all surplus computer equipment.

Our report made several recommendations to the Manager of the Savannah River Operations Office that addressed weaknesses in the SRS property management program. Based on recurring problems with the disposal of high risk personal property, we recommended that the Director, Office of Procurement and Assistance Management, require a review of high risk property management systems Department-wide. We also recommended that the Director, Office of Security and Emergency Operations, determine whether any security vulnerabilities resulted from the release of UCNI and security/privacy information.

Management concurred with the recommendations in our report and agreed to take corrective actions.

cc: Deputy Secretary
Under Secretary
Acting Under Secretary for Nuclear Security/Administrator for Nuclear Security

INSPECTION OF SURPLUS COMPUTER EQUIPMENT MANAGEMENT AT THE SAVANNAH RIVER SITE

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

On November 1, 1999, the Office of Inspector General (OIG) received information from Senator Strom Thurmond concerning an allegation regarding the sale of surplus computer equipment at the Savannah River Site (SRS). In summary, it was alleged that SRS surplused and sent off-site over 40 computer hard drives that reportedly contained classified or sensitive information; and that the release of this information might pose a threat to the national security of the United States. The Department's major operating contractor at SRS, Westinghouse Savannah River Company (Westinghouse), is responsible for the final disposal of surplus equipment, including computer hard drives.

The OIG initiated an inspection to determine whether: (1) surplus computer equipment is disposed of in accordance with Federal and Departmental requirements, and (2) Government-owned computer equipment at SRS is properly cleared of sensitive information before it is excessed to the public.

OBSERVATIONS AND CONCLUSIONS

In reviewing the process to surplus and dispose of computer equipment at SRS, the OIG found that Westinghouse failed to comply with Departmental and site property management requirements by not properly preparing surplus computer equipment for disposal. Specifically, Westinghouse did not clear stored information from all surplus computers and certify that the computers were sanitized prior to disposal as required by Section 109-43.307-53, title 41, Code of Federal Regulations (CFR).

Prior to the OIG inspection of the sale of surplus computer equipment at SRS, Westinghouse's Computer and Information Security Section conducted a "preliminary inquiry" by sampling 23 hard drives and 17 floppy disks taken from computer equipment that had been sold as excess/surplus to a private business. The November 1999 Westinghouse security report (see Summary of Report, Appendix B) found that "very few of the drives [in the sample] had been cleared." In addition, some of the hard drives contained Unclassified Controlled Nuclear Information (UCNI)[1] and other sensitive unclassified information.

By selling computer equipment containing UCNI, Westinghouse appears to have violated Section 148 of the Atomic Energy Act of

[1] Unclassified Controlled Nuclear Information - Certain unclassified government information prohibited from unauthorized dissemination under Section 148 of the Atomic Energy Act of 1954, as amended "whose unauthorized dissemination, as determined by a Controlling Official, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security . . . ." (10 CFR Section 1017.3)

1954. This matter has been referred to the appropriate investigative officials. Westinghouse also violated the Department's requirements for disposing of high risk personal property.[2] Westinghouse's Computer and Information Security Section initiated its inquiry when an employee of an off-site buyer, Allied Fabricators and Constructors, Incorporated (Allied), reported discovering a floppy disk labeled "Secret-Restricted Data" (Secret) among computer equipment purchased from SRS. SRS officials later determined this floppy disk did not contain any classified information. The owner of Allied provided the OIG a copy of a shipping notice that indicated that the floppy disk was among two trailer loads of computer equipment being processed and loaded for a September 1999 shipment to the People's Republic of China (PRC). Westinghouse's preliminary inquiry determined that some of this computer equipment contained sensitive unclassified and UCNI information. Computer equipment used for UCNI is considered high risk property, and its off-site release was contrary to DOE property management requirements. Based on this discovery, Westinghouse repurchased all of the computer equipment from Allied and ordered the equipment destroyed. As a result of the decision to destroy this equipment without further examination, no one can be sure exactly what information existed on the unexamined computer equipment. Also, due to the internal control weaknesses, no one can be sure exactly what information may have been on other computer equipment sold directly to other private individuals and companies.

Although the computer equipment pending shipment to the PRC in September 1999 was eventually destroyed, the owner of Allied told us that, around July 1999, other SRS computer equipment was shipped to the PRC. Although he believed the shipment did not contain hard drives, the owner of Allied told us that no records were kept of the earlier PRC shipment. Therefore, the OIG had no way to determine the volume or the exact content. We noted that over 16,000 computers and computer related items were sold publicly by SRS during Fiscal Years 1998 and 1999. Also, there are approximately 147 classified computer systems in use at SRS.

Following the off-site discovery of computer equipment containing sensitive unclassified and UCNI information, Westinghouse

[2] High risk personal property – Property that, because of its potential impact on public health and safety, the environment, national security interests, or proliferation concerns, must be controlled, and disposed of in other than the routine manner. The categories of high risk property are automated data processing equipment, especially designed or prepared property, export controlled information or property, hazardous property, nuclear weapon components or weapon-like components, proliferation sensitive property, radioactive property, special nuclear material, and unclassified controlled nuclear information. (41 CFR Section 109-1.100-51)

decided that all future surplus computers and related equipment would be destroyed to prevent the release of sensitive information. We concluded that the blanket destruction of all surplus computers and related equipment is not required by DOE property disposal regulations.

On November 2, 1999, the DOE/Savannah River Operations Office (SRO) Organizational Property Management Officer who had been delegated authority to approve changes to the Contractor's Property Management System, approved a Westinghouse plan to shred all surplus Government-owned computer equipment. The method of destruction chosen was shredding in a device commonly used to shred "junk" automobiles. At the time of our inspection, Westinghouse had begun shredding all surplus computers and computer equipment, including hard drives. SRS storage warehouses contain over 2,100 surplus personal computer systems (monitor, central processing unit, keyboard, and mouse) which had been individually boxed and stacked in April and July 1999 and were awaiting destruction. Although these systems were considered "old" technology (IBM 386 or 486 processors and Apple Macintosh II systems), we were told that each system had been determined by site computer personnel to be operational.

The proper disposal by DOE and its contractors of excess personal property, including surplus computer equipment, has been a concern addressed previously by the OIG and the General Accounting Office (GAO). The OIG has issued a number of reports on property disposal weaknesses within the Department. These reports are identified in Appendix C. In June 1995, GAO issued a report entitled "Department of Energy – Procedures Lacking to Protect Computerized Data," Report Number GAO/AIMD-95-118. As a result of the GAO report, Department officials developed and issued policies and procedures governing management and control of automated data processing equipment (ADPE). For the purposes of this report, we will refer to ADPE as computer equipment. The policies and procedures included controls for establishing high risk personal property improvements for managing export controlled property, and increased requirements for proper disposal of computer equipment.

Our inspection of the sale of surplus computer equipment at the SRS identified weaknesses in the Department's administration of property management programs. As part of its implementation of the Government Performance and Results Act of 1993 (GPRA), the Department has established program goals, and measures

performance against these goals. Consequently, SRO established the Savannah River Site Strategic Plan. The plan defines strategic goals, key success measures, objectives and strategies in the business lines of National Security, Nonproliferation, Environmental Quality, and Science and Technology. This inspection has documented methods to assist the Department in meeting its goals and improving the efficiency of Federally funded programs.

Details of Findings

Requirements for Sanitizing/Clearing Computer Equipment

The Department of Energy Property Management Regulations at 41 CFR 109-43.307-53, require that DOE automated data processing equipment be sanitized before being excessed to ensure that all data, information, and software has been removed. The regulations further require that designated computer support personnel certify that the equipment has been sanitized by attaching a tag to the item.

Reasons for proper implementation of the above property management regulations include, among other things, protecting information such as classified Restricted Data and UCNI from unauthorized dissemination. The unauthorized dissemination of both classified Restricted Data and UCNI is prohibited by the Atomic Energy Act of 1954, as amended. The DOE implementing regulations for protecting UCNI, at 10 CFR Section 1017.3, include in the definition of "unauthorized dissemination" the intentional or negligent transfer, in any manner, by any person, of UCNI information or material to any unauthorized person.

Process for Sanitizing/Clearing Classified Computer Equipment

The process for ensuring that all classified information is properly cleared before classified computer systems are released to anyone outside of SRS is similar to the process explained below for unclassified computer systems. The notable exception is that Westinghouse procedures require classified storage media (i.e., hard drives, floppy disks, etc.) to be sanitized by overwriting, degaussing[3] or destroying. Specific procedures govern the application of each of these methods and when they are used. Additionally, the procedures require all markings identifying the former use of the system to be removed before the system is turned over to property management officials for disposal. Theoretically, this procedure should prevent classified media from ever reaching the property management officials who arrange for excess property sales and donations.

Process for Sanitizing/Clearing Unclassified Computer Equipment

Westinghouse computer security procedures assign responsibility to the Computer System Security Officer (CSSO) for ensuring that all unclassified information, to include sensitive unclassified and UCNI, is properly cleared before a computer system is released to anyone outside SRS. Different organizations within Westinghouse have different CSSOs. Westinghouse computer users are also assigned similar responsibilities for ensuring that all unclassified magnetic media assigned to them are cleared before release.

[3] Degaussing is a process whereby the magnetic field is removed or neutralized.

SRS Property Sales

Westinghouse had established a sales agreement/contract with Allied from August 1, 1998, through July 31, 1999, for purchasing and removal of excess computers and accessories from SRS at a rate of about 10¢ per pound. XS Computers[4] was responsible for receiving, managing and storing computer equipment for Allied. Additionally, the General Services Administration auctioned some of SRS's computer equipment to the public during this time.

Security System Data Sold

During Westinghouse's preliminary inquiry, it was determined that five of the 23 sampled hard drives contained UCNI files that are restricted from release under the Atomic Energy Act of 1954. For example, two memory disk drives examined after being sold to and then recovered from Allied still contained data from the SRS Electronic Safeguards and Security System, also know as the E3S VAX[5] security system. These E3S security system memory disk drives were two of 32 memory disk drives disposed of by Westinghouse along with an E3S VAX computer in approximately mid-1999. According to a Westinghouse Safeguards and Security official, the E3S system serves as an umbrella for other software modules, covering all automated physical security for the site including alarm systems, intruder detectors, vault rooms, access control, security badge information, and closed circuit televisions. E3S information is considered UCNI.

According to a Westinghouse Safeguards and Security Engineering official, the E3S memory disk drives that were disposed of served as storage devices similar in operation to the 3½ inch disks utilized by most personal computers. The memory disk drives are physically much larger than a floppy disk, and had a storage capacity of approximately 300 megabytes. According to the engineering official, the memory disk drives stored executable files, maps and database tables, and archived historic information. These memory disk drives had been located within the SRS Central Alarm Station and were connected to the E3S Local Area Network and Wide Area Network.

During our inspection, Westinghouse was unable to locate the other 30 E3S memory disk drives that had been excessed. In the conclusions of its November 1999 preliminary inquiry, Westinghouse's Computer and Information Security Section

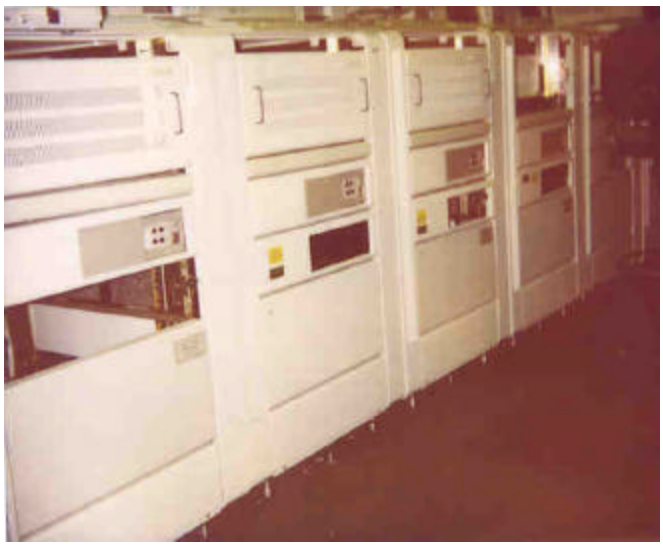
[4] XS Computers is a subsidiary of Allied Fabricators.

[5] VAX computers are 32-bit supermicrosystems manufactured by Digital Equipment company and are designed to support a high-performance, multi-programming environment. Multi-programming enables simultaneous execution of many applications and interactive development of applications programs. VAX systems are designed for real-time, timesharing, and batch applications and offer a choice of operating systems, high-level languages, information management software, and programmer productivity tools.

assumed that the E3S data had been totally compromised to an adversary, but concluded that the potential impact of all 32 E3S memory disk drives being lost was minimal. With respect to the compromised memory disk drives, the Westinghouse preliminary inquiry report stated that "Information that could be revealed is the social security numbers of those individuals with access to the E3S system." Further, the report stated that "The alarm sectors of the E3S system detailing what alarms are in a specific monitoring sector would be revealed" and "The software used to monitor the E3S system is revealed . . . ." The report noted that no passwords were revealed and that the software involved was purchased commercially. The report stated that no connections existed between the E3S system and SRS classified computing systems and concluded that, in the opinion of the writers, an adversary could not use the information revealed by this compromise to successfully attack SRS's security system.

We believe that the compromise of the 32 memory disk drives from the SRS umbrella security system is a significant security and privacy concern which warrants further review by security officials with detailed knowledge of physical, personnel, and computer security safeguards systems. Therefore, we briefed officials from DOE's Office of Security and Emergency Operations on this issue and are recommending they conduct or direct an appropriate review. Although Westinghouse has taken some action with respect to the security of the E3S in its current configuration, additional actions may be necessary, to include, at a minimum, notifying the personnel involved that their social security numbers and/or other personal identifying information may have been compromised so they can take appropriate precautions.

The SRS VAX systems in the photograph are similar to the system sold by Westinghouse.



Computer Equipment Returned to Westinghouse

In addition to the equipment identified by Westinghouse, the owner of Allied provided us with a listing of other hard drives, optical media discs,[6] and diskettes that he had voluntarily returned at various times to Westinghouse officials. The list included 47 hard drives, 63 optical media discs, 16 5¼ inch floppy diskettes, and 25 3½ inch floppy diskettes. Allied's owner stated that he had returned the listed items to Westinghouse between June and October 1999. He stated that he had directed his employees to look for and pull hard drives during their walk through the storage area because of the concerns raised after locating and returning the 63 optical media discs. He had read recent newspaper articles of instances where security might have been jeopardized because government sensitive information had been released to China. Allied's owner told us he returned the diskettes and drives he had received from Westinghouse because he was concerned they might also contain sensitive information. The OIG was informed by Westinghouse officials that Westinghouse had begun developing procedures to prevent the release of sensitive computer equipment in the future. With respect to the computer equipment returned by Allied's owner, a Westinghouse manager told us that all of these hard drives, optical media discs, and floppy diskettes have since been destroyed. Consequently, it is impossible to determine if sensitive information was contained on the drives/diskettes and the optical media discs.

Weaknesses in Sanitizing/Clearing Computer Equipment

Despite DOE regulations, Westinghouse did not certify that computer equipment was properly cleared before being excessed, and that diskettes were properly overwritten or destroyed. Also, Westinghouse did not ensure all computer equipment had a single review by the responsible official, to ensure it was cleared before it was sold. Our finding is consistent with the Westinghouse security preliminary inquiry report. Specifically, the report states:

> It is apparent that this responsibility was exercised differently by different organizational CSSOs. Some would take the initiative to contact Computer and Information Security or Digital Controls and Services [Systems] (DC&S) for assistance in clearing/degaussing the drives and excessing the systems; some however, apparently thought that this would be done after they placed the equipment in Excess.

[6] Optical media discs – A storage medium from which data is read and to which it is written by lasers. Optical discs can store much more data (6 billion bytes) than most portable magnetic media, such as floppies.

The Manager of Westinghouse's Digital Controls and Systems (DC&S) Department, tasked with providing technical assistance and expertise to those who are clearing hard disk drives for non-personal computers,[7] stated that users of computer equipment do not always request DC&S services to clear hard drives. The manager said if users or owners of computer equipment felt that they could clean their system then they would not request DC&S services for clearing the computer equipment.

We noted that there are approximately 147 classified computer systems at SRS. The OIG did not find evidence during this inspection that classified information or Restricted Data had been inappropriately released. However, this inspection did not specifically review the disposition of all classified systems surplused/excessed in recent years. The classified computer equipment disposal process may have experienced weaknesses similar to those in the disposal process for computers used for UCNI, as demonstrated by the discovery at Allied of the floppy disk labeled "Secret - Restricted Data." Since the computer equipment recovered by Westinghouse from Allied was destroyed without further examination, no one can be certain what information, if any, was on the unexamined equipment when it was destroyed. We also do not know what information may have been contained in computers disposed of to other private individuals or companies, e.g., school donations, auctions, etc.

Westinghouse officials recently awarded a contract to exchange Government-owned personal computers (desktops) for leased systems. This will involve approximately 12,000 personal computers used by Westinghouse personnel. With respect to clearing information from leased computer drives, the terms of the contract assign the contractor responsibility for clearing personal computer hard drives and attaching a label to the system prior to transferring the system for final disposal. Personal computers used by DOE Federal and contractor personnel, with the exception of Westinghouse, will not be included in the leasing program.

[7] Non-personal computers – Non-singular user ADP system, generally a larger item consisting of the central processing unit (CPU), expansion cards, etc., that form a composite workstation (i.e., VAX systems, UNIX systems, stations/servers).

Shipment of Computer Equipment to the People's Republic of China

The floppy disk labeled "Secret-Restricted Data," and other computer equipment found by Westinghouse and later determined to contain sensitive unclassified and UCNI information, was originally pending shipment to the PRC. Specifically, the owner of Allied provided us a copy of a shipping notice indicating that two trailer loads of computer equipment received from SRS were being processed for shipment to the PRC. The shipping notice showed that a California company purchased the equipment for delivery to Nanhal Sanshan Harbor, a region within the PRC. Westinghouse was unable to provide documentation indicating the planned shipment had been cleared of sensitive information. The sale of uncleared computer equipment that contained UCNI information appears to have violated the Atomic Energy Act of 1954. It also violated DOE disposal requirements for high risk property. Further, though this pending shipment to the PRC was stopped, two trailer loads of previous SRS excessed computer equipment had been shipped to the PRC around July 1999.

High Risk Disposal Requirements

Computer equipment used to process UCNI is subject to Department regulations which govern high risk property disposal. Property management regulations and DOE policy require computer equipment used for UCNI to be identified, marked, and controlled to assure proper treatment at disposal and to prevent unauthorized disclosure. Westinghouse property management officials responsible for disposal of the computer equipment had considered the equipment to be scrap without meeting high risk property disposal requirements. Specifically, Allied's owner told us two containers with former SRS computer equipment he purchased as scrap, had been shipped to the PRC. The owner stated that the shipment was "around July 1999;" however, he did not have a copy of the shipping document nor the dollar amount of the sale. He believed the shipment included monitors, keyboards, cables, but no hard drives. The owner said that due to press reports regarding Chinese espionage, he contacted a Westinghouse procurement official and informed the official that the business had a shipment bound for China. He reportedly was told that a Westinghouse procurement official would contact him if there were any concerns. Allied's owner also said he waited approximately two weeks for the official to contact him before he allowed the computer equipment to be shipped to the PRC.

The Westinghouse export control officer told us that she had been contacted by the Westinghouse procurement official regarding this pending shipment to the PRC. The export control official stated that she then contacted the Westinghouse General Counsel's office and informed an attorney that she was attempting to locate the

broker responsible for arranging a shipment to the PRC. According to the export control official, the procurement official later informed her that he had not been given the name of the broker and the shipment had already taken place. Because the export control official was never able to identify the broker prior to shipment, she was unable to determine if the broker was on the Federal Denied Parties List that identifies individuals and companies whose export privileges have been denied. Subsequently, the export control official identified the broker and confirmed the broker was not on the Federal Denied Parties List.

Shredding of Computer Equipment

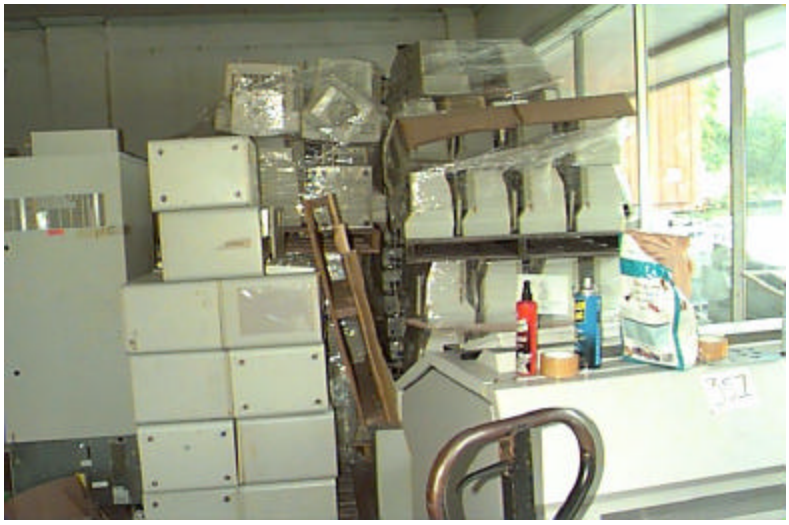
Once the sale of computer equipment containing sensitive unclassified and UCNI information to Allied was discovered, Westinghouse officials repurchased and destroyed all computer equipment sold to or located at Allied.

We noted that Westinghouse had paid Allied over $59,000 and was awaiting a decision to make final settlement for the computer equipment repurchased. Of the over $59,000 paid, over $9,000 was paid for withdrawal of a pending shipment to the PRC and $50,000 was paid as "good faith" money for retrieving computer equipment from Allied while awaiting a final repurchase agreement. According to the sales agreements, Westinghouse received approximately $41,000 for computer equipment sold to Allied during execution of the contract. Later, Westinghouse officials requested permission from SRO to shred all surplus computer equipment components reasoning that it takes too many staff-hours to validate which equipment was a security risk.

On November 2, 1999, the DOE Organizational Property Management Officer approved a plan to allow Westinghouse to shred all components of surplus Government-owned computer equipment. Upon the Organizational Property Management Officer's approval, Westinghouse began the process of shredding all computer equipment components. Subsequent to the approval by SRO, Westinghouse began transporting all excess computer equipment to West Columbia, South Carolina, for destruction in a large shredder.

Allied's outside storage area. The computer equipment at right was later repurchased and shredded by Westinghouse.

Allied's indoor storage showing equipment in good condition that was later repurchased and shredded by Westinghouse.



Personal Property Disposal Considerations

The blanket destruction of all surplus computer equipment is not required by property disposal regulations. As stated earlier, DOE regulations require that high risk personal property, such as computer equipment used for UCNI, be identified, marked, and controlled to assure proper treatment at disposal. Normally, non-sensitive surplus computer equipment is disposed of through sales at prices which are fair and reasonable, and not disposed of for less than could reasonably be expected to be obtained if the personal property was offered for competitive sale.

During our inspection, the computer equipment that had already been sent or that was awaiting shipment to the shredder contractor included storage arrays, printers, plotters, disk drives, controllers, mini-CPUs, tape drives, and video printers. Additionally, we observed that a total of over 2,100 PCs including IBM (386 and

486 processors) and Apple Macintosh II systems had been boxed and stacked in April and July 1999 and were awaiting shredding. Although the 2,100 PCs were considered by Westinghouse to be old technology, we were told that each PC (CPU, monitor, keyboard, and mouse) had been determined to be operational prior to boxing.

Recommendations

We recommend that the Director, Office of Procurement and Assistance Management:

1. Require a review of the Department's Property Management Systems to ensure disposal of High Risk Personal Property is processed in accordance with the Department's Property Management Regulations.

We recommend the Director, Office of Security and Emergency Operations Office:

2. Determine whether there are any possible security vulnerabilities resulting from the release of UCNI and security/privacy information.

We recommend that the General Counsel:

3. Evaluate whether the public release of personal identifying information (such as badge office data and social security numbers) by Westinghouse was contrary to the Privacy Act and take appropriate action regarding the legal implications of this release.

We recommend that the Manager, Savannah River Operations Office:

4. Evaluate Westinghouse's actions in disposing of computer equipment, disallow the costs incurred for any actions not consistent with contract terms, and consider these actions when determining payments from the available fee pool.

5. Require Westinghouse officials to ensure CSSO's or custodians inspect and certify all computer equipment for proper clearance prior to turning in the equipment for disposal.

6. Require Westinghouse officials to ensure all computer equipment will be checked for certification to confirm that

magnetic media and diskettes are properly cleared before being declared excess.

7. Require Westinghouse officials to review contract requirements for selling excess computer equipment to ensure terms and conditions of future sales adhere to Departmental requirements.

8. Conduct a thorough review of Savannah River's High Risk Personal Property control process and its excess sales processes as it relates to high risk property.

9. Require Westinghouse to comply with the Department's Property Management Regulations regarding disposal of High Risk Personal Property by submitting written procedures for approval by the Contracting Officer.

10. Determine whether Westinghouse's policy of shredding all computer equipment is in the best interest of the Government. If this policy is not in the best interest of the Government, direct Westinghouse to cease its current policy.

11. Require Westinghouse to seek approval of the Contracting Officer prior to implementing any changes to its property management policy.

12. Evaluate the process used by Westinghouse to protect Privacy Act information which is maintained on behalf of the Department.

Management Comments

Departmental management provided responses to the draft report and concurred with all the report's recommendations. Specific responses are outlined below.

The Director, Office of Procurement and Assistance Management, stated that his office concurred with Recommendation 1. The Director stated his office "will require all field sites to review their federal office/contractor's property management procedures to ensure that High Risk Personal Property is being disposed of in accordance with the Department's Property Management Regulations (DOE/PMRs)." The Director also stated the "field sites will be required to provide a summary of their findings for each federal office/contractor reviewed. If necessary, Headquarters can then do a random sampling of the federal offices/contractors to ensure the procedures are efficient, cost-effective and in compliance with Regulations."

The Director, Office of Security and Emergency Operations, stated that his office concurred with Recommendation 2. The Director stated his office is planning to organize, schedule and conduct a joint Office of Safeguards and Security and Environmental Management damage assessment investigation to be completed by June 15, 2000. The investigation will focus on the potential compromise of classified information, UCNI, the SRS automated access control and physical security system, and other possible security vulnerabilities.

The General Counsel's Office stated they do not have any comments or objections regarding Recommendation 3.

Savannah River Operations (SRO) management concurred with Recommendations 4-12, and provided general comments on the contents of the draft report. SRO agreed to determine appropriate action for Recommendation 4 by June 30, 2000. For Recommendations 5-7, 9 and 11, SRO agreed to take appropriate action by May 31, 2000. For Recommendation 8, SRO agreed to conduct a review of the High Risk personal property control process by July 31, 2000.

For Recommendation 10, SRO agreed and stated that actions to cease the practice of shredding computer equipment had already been taken. The SRO Manager stated:

> The Report implies that there was no basis for the destruction of surplus computer equipment on hand, and that the practice of shredding all surplus computer scrap is unwarranted. DOE has been advised by WSRC [Westinghouse] that the initial decision to destroy all computer equipment has subsequently been rescinded and currently, no equipment is being shredded pending a re-evaluation of the site policy. In all likelihood, surplus computer equipment such as monitors, keyboards, cables and printers will be sold in an "as is" condition or as scrap depending on condition. Central Processing Units (CPU's) and media will likely be destroyed. The decision to destroy the equipment that was recovered from Allied was based on an economic analysis performed at that time that supported destruction as the most cost beneficial disposition. Property Management procedures related to the disposition of surplus

> computer equipment are being revised to address the lesson's learned from this incident.

In respect to the shredding of computer equipment, the SRO Chief Financial Officer stated:

> …it should be noted that this action is not a common practice at Savannah River Site and that it was in fact weighed to be the most feasible and cost effective means at the time in order to eliminate any further risk. In the two main shredding incidents, a High-Risk reevaluation of said commodities would cause action to have each unit be considered for review. In addition, component sorting and reprocessing through the disposal system could have been very labor intensive. It was concluded that the cost incurred to provide for the safe handling and resource needs to perform this intensive task would not be prudent when considering the low resale value for non-Y2K compliance computers and their components.

SRO also provided general comments on the draft report that conveyed several distinct concerns. SRO requested that our report include a statement that the OIG inspection did not disclose any situation where classified information had been sent off-site or inadvertently transported overseas in the process of computer equipment disposal at SRS.

SRO also stated that classified information is protected differently than unclassified information reducing the chance of inadvertent disclosure of classified information. SRO requested that the OIG recognize in the report "differences in the levels of controls over classified information from those of unclassified, sensitive information."

INSPECTOR COMMENTS

We consider management's comments to our recommendations to be responsive. Where appropriate, we have incorporated management's comments into the final report.

With respect to SRO's concerns regarding classified information, the OIG recognizes there are differences in the levels of control over classified information and unclassified sensitive information. However, despite these controls, Westinghouse allowed a floppy disk labeled "Secret-Restricted Data" to be sold and transported off-site. At the time the disk was discovered it was included in a

pending shipment to the PRC. SRS officials later determined this disk did not contain classified information. Nevertheless, this situation raises concerns about the internal controls that were in place for protecting classified information. Additionally, not all of the computer equipment repurchased from Allied was examined before it was destroyed. Further, over 16,000 computers and computer related items were sold publicly by SRS during Fiscal Years 1998 and 1999. Without the examination of all computer related items sold by SRS, both publicly and through contract to Allied, we were unable to conclude whether classified information had been sent off-site or inadvertently transported overseas.

Appendix A

SCOPE AND METHODOLOGY

The inspection was initiated at the Savannah River Operations Office in Aiken, South Carolina, in November 1999.

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency. As part of our inspection, we interviewed officials at DOE's Savannah River Operations Office and Westinghouse Savannah River Company. We also reviewed pertinent records and documents pertaining to Westinghouse's Computer Security, Export Control, and Asset Management Operations.

Appendix B

SUMMARY OF PRELIMINARY INQUIRY REPORT
REPORT #PL 99-063

On November 11, 1999, Westinghouse's Computer and Information Security Section issued a preliminary report documenting a security inquiry conducted August through October 1999. This report informed Westinghouse officials that a 5-1/4 inch floppy disk labeled Secret Restricted Data was found in a disposed VAX (supermicrosystem manufactured by Digital Equipment Corporation) system which had been sold to Allied Fabricators. The VAX was formerly used at the Site's Tritium Facilities to manage the Automated Reservoir Management System (ARMS)[8] program. Later, Westinghouse officials determined that the disk was used to boot up the system from the console. The officials concluded that the disk had remained with the system for a prolonged period of time and would not have been any use to the system in its present configuration. The disk was labeled "Secret" because it was associated with a classified system and required to have been marked to the highest level available for data the system would be able to process. After further review by Westinghouse's Computer Security officials, the disk was determined not to contain any classified files because the space on the disk was used for unclassified boot-up system information.

As a result of this incident, a Westinghouse Computer Security official visited Allied to determine if there was other media that might have been considered as classified or sensitive and sold by SRS officials. The official noticed one trailer filled with computer parts, and determined that the trailer was about to be shipped from the location. Also, the official stated that although no items were found marked as classified or sensitive, several items were returned to SRS for inspection and evaluation, including hard drives and various floppy disks. The inquiry report stated that "When the installed drives were found it was not apparent, in most cases, whether or not they had been cleared/degaussed in any way until after the installed drives were returned to the site. Upon further inspection, it was discovered that very few of the drives had been cleared."

Subsequently, a meeting was held with Westinghouse's Computer Security, Export Control, Property Management, and Procurement officials. The DOE/SRO's Computer and Information Security Official also attended this meeting. Westinghouse's management personnel decided to halt pending shipments of two trailer loads of computer equipment to the PRC and required Allied's owner to delay any movement until further notice was given by Westinghouse. The computer equipment loaded on these trailers included monitors, mainframe computers, keyboards, and miscellaneous cards, and cables. Later, an agreement was reached between Westinghouse officials and the owner of Allied that allowed Westinghouse to pay the price of the negotiated sale for the two trailer loads of computer equipment.

[8] Automated Reservoir Management System (ARMS) – ARMS is an online reservoir production and data archive system that provides real-time reservoir tracking and inventory, process calculations, operator instructions, and data entry screens to capture, store, and manage reservoir-related processing information. ARMS does not provide process control but verifies data and sequence of operation.

Westinghouse officials determined that most drives had not been cleared and many of the floppy disks that had not been damaged due to weathering contained operational files, some of which revealed sensitive personnel information. As noted by Westinghouse's preliminary inquiry:

> Sensitive unclassified employee personnel information was found in the retrieved media from a desk top personal computer. Two VAX unit memory disks were found which contained sensitive unclassified SRS E3S security system data. The E3S VAX along with 32 memory disks had been excessed and sold to Allied Fabricators in the same time period as the ARMS VAXs. The E3S system is approved for up to Unclassified Controlled Nuclear Information (UCNI).

In October 1999, as a result of information found on hard drives and floppy disks, Westinghouse officials repurchased all computer equipment sold to or located at Allied Fabricators and subsequently transported the retrieved equipment to West Columbia, South Carolina, for shredding. Westinghouse officials said they witnessed the shredding of this computer equipment.

Appendix C

SELECTED OIG PERSONAL PROPERTY REPORTS

IG-0455	Inspection Report on "Inspection of the Sale of a Paragon Supercomputer by Sandia National Laboratories," December 1999
IG-0385	"Special Audit Report on the Department of Energy's Arms and Military-Type Equipment," February 1996
IG-0344	"Summary Report on Department of Energy's Management of Personal Property," March 1994
IG-0343	"Inspection of the Management of Excess Personal Property at Sandia National Laboratory, Albuquerque, New Mexico," March 1994
IG-0329	"Inspection of Management of Excess Personal Property at Rocky Flats," May 1993
ER-B-98-07	Audit Report on "Personal Property at the Oak Ridge Operations Office and the Office of Scientific and Technical Information," April 1998
WR-B-97-07	"Audit of Desktop Computer Acquisitions at the Idaho National Engineering and Environmental Laboratory," August 1997
INS-L-93-01	Inspection Report on "Controls Over Personal Computer Equipment at the Savannah River Site," January 1993

IG Report No. DOE/IG-0472

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 more clear 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 nay 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 Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

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.