Audit Report

MANAGEMENT OF INFORMATION TECHNOLOGY EQUIPMENT, OFFICE OF THE SECRETARY OF DEFENSE

Report No. D-2001-096 April 9, 2001

Office of the Inspector General
Department of Defense

Form SF298 Citation Data

Report Date ("DD MON YYYY")	Report Type	Dates Covered (from... to) ("DD MON YYYY")
09Apr2001	N/A	

Title and Subtitle Management of Information Technology Equipment, Office of the Secretary of Defense	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Number(s)** D-2001-096
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
An Inspector General, DoD, Report of Investigation issued on August 28, 2000, indicated that the investigation was complicated by incomplete Office of the Secretary of Defense (OSD) inventory records for information technology equipment, such as personal computers. In addition, the investigation identified security issues concerning the disposal of personal computer hard drives. As a result, we initiated an audit of information technology equipment management at the OSD. The Director, Washington Headquarters Services (WHS) is responsible for managing the information technology equipment program for the OSD, the WHS, and other assigned DoD activities. The Director, Information Operations and Reports, WHS, is responsible for reviewing automated information systems requirements for those organizations and ensuring that DoD standardization, interoperability, security, and information-sharing requirements are met. Also, the Director, Information Operations and Reports, has the responsibility to maintain and operate an automated centralized inventory control system that is compatible with other DoD-wide inventory systems. The WHS system included records for about 34,000 items of information technology equipment with a total value of $99.8 million. The inventory of information technology equipment included central processing units, hard drives, personal computers, and computer monitors.

Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 33	

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AIRM	Automated Information Resource Management
ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
CIO	Chief Information Officer
ITE	Information Technology Equipment
OSD	Office of the Secretary of Defense
WHS	Washington Headquarters Services

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2885

April 9, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES

SUBJECT: Audit Report on Management of Information Technology Equipment, Office of the Secretary of Defense (Report No. D-2001-096)

We are providing this report for your information and use. We considered management comments on a draft of this report when preparing the final report.

The Deputy Secretary of Defense had previously concurred with the finding and directed responsive actions. Comments from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) were responsive. However, we request additional comments by June 8, 2001, on when the time-phased implementation plan for the recommendations will be completed and whether any alternative actions have been approved.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Charles J. Richardson at (703) 604-9582 (DSN 664-9582) (crichardson@dodig.osd.mil) or Mr. Walter R. Loder at (703) 604-9534 (DSN 664-9534) (wrloder@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-096 **April 9, 2001**
(Project No. D2001FA-0040)

Management of Information Technology Equipment, Office of the Secretary of Defense

Executive Summary

Introduction. An Inspector General, DoD, Report of Investigation issued on August 28, 2000, indicated that the investigation was complicated by incomplete Office of the Secretary of Defense (OSD) inventory records for information technology equipment, such as personal computers. In addition, the investigation identified security issues concerning the disposal of personal computer hard drives. As a result, we initiated an audit of information technology equipment management at the OSD.

The Director, Washington Headquarters Services (WHS) is responsible for managing the information technology equipment program for the OSD, the WHS, and other assigned DoD activities. The Director, Information Operations and Reports, WHS, is responsible for reviewing automated information systems requirements for those organizations and ensuring that DoD standardization, interoperability, security, and information-sharing requirements are met. Also, the Director, Information Operations and Reports, has the responsibility to maintain and operate an automated centralized inventory control system that is compatible with other DoD-wide inventory systems. The WHS system included records for about 34,000 items of information technology equipment with a total value of $99.8 million. The inventory of information technology equipment included central processing units, hard drives, personal computers, and computer monitors.

Objectives. Our objective was to evaluate the management of information technology equipment in the possession of the OSD. Specifically, we tested the existence and completeness of information technology equipment databases and other records used to control equipment within the OSD. Existence tests measure the ability to physically locate the equipment recorded on the information technology inventory databases. Completeness tests ascertained whether equipment located in OSD work spaces was recorded on the information technology inventory databases. We also assessed the management control program as it relates to the overall objective.

Results. The Office of the Secretary of Defense information technology equipment management practices and controls needed improvement. Although WHS has reported progress over the last several years in improving inventory records, more needs to be done. Based on a physical inventory test of sample items, we statistically estimated that of about 34,000 items of information technology equipment, 2,790, or 8 percent, of the items would not be found after a reasonable search was performed, and that an

estimated 7,859, or 23 percent, of the inventory records would contain inaccurate information. Also, to test the completeness of the inventory records, we selected 635 pieces of equipment from the OSD work spaces and determined that 51 items were not included on any inventory record. We also identified security vulnerabilities related to the disposal of OSD computers containing sensitive information and the inappropriate use of personal digital devices in secure classified areas. As a result, the OSD risked the loss of computer equipment and the disclosure of sensitive and classified information. See Appendix A for details on the review of the management control program.

Management Actions. During the audit, we provided two memorandums to the Deputy Secretary of Defense to advise of weaknesses in computer disposal operations and problems with the inventory management of information technology equipment. We also made six recommendations to improve inventory management. The Deputy Secretary of Defense responded to each memorandum and directed the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to implement the audit recommendations and to take immediate action to correct the problems. Subsequently, the DoD Chief Information Officer Executive Board established a working group to review issues and refine the policy related to the Deputy Secretary of Defense direction to destroy DoD computers hard drives prior to disposal. See Appendix B for copies of the Deputy Secretary of Defense guidance.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) establish a time-phased plan to implement the corrective actions directed by the Deputy Secretary of Defense during the audit, and to develop policy regarding the proper use of current technology items, such as personal digital devices, with secured classified computers.

Management Comments. The Deputy Assistant Secretary of Defense, Command, Control, Communications, and Intelligence acknowledged the concurrence of the Deputy Secretary of Defense to the audit report findings and recommendations. The Deputy Assistant Secretary stated that actions were underway to develop a time-phased implementation plan for the recommendations and to provide for the DoD Chief Information Officer to serve as the OSD Chief Information Officer. The Deputy Assistant Secretary stated that further analysis might lead to alternative actions, as did the Director, Washington Headquarters Services. The Director, Policy Automation, Office of the Deputy Under Secretary of Defense Policy Support, expressed concerns with the accuracy of the data in the report. See the Finding section for a discussion of the management comments and the Management Comments section for the complete text of the comments.

Audit Response. Management comments were generally responsive. We agree that there could be cost effective alternatives to some recommendations. However, the Deputy Secretary of Defense clearly committed DoD to seeking further inventory management improvement and reducing security risks associated with the loss of computers and hard drives containing sensitive data. We met with a representative of the Director, Policy Automation, and demonstrated that there was no basis for concern regarding the accuracy of the data in the report. We request that the Assistant

Secretary of Defense (Command, Control, Communications, and Intelligence) inform us by June 8, 2001, on when the implementation plan will be complete and what alternative actions, if any, have been approved.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 1

Finding

Management of Information Technology Equipment 2

Appendixes

A. Audit Process
Scope 10
Methodology 10
Statistical Sampling Methodology 11
Management Control Program Review 12
Prior Coverage 12
B. Deputy Secretary of Defense Responses to the Inspector General, DoD, Preliminary Findings and Recommendations 13
C. Component Organizations of the Office of the Secretary of Defense Visited During the Audit 16
D. Report Distribution 18

Management Comments

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) 21
Washington Headquarters Services 22
Under Secretary of Defense for Policy 24

Background

Office of the Secretary of Defense (OSD). The OSD is the principal staff element of the Secretary of Defense in the exercise of policy development, planning, resource management, and fiscal and program evaluation responsibilities. The OSD includes four Under Secretaries of Defense, five Assistant Secretaries of Defense, and other organizations. (See Appendix C for a list of OSD components visited during the audit.) As of November 30, 2000, OSD included 1,815 civilian personnel, 755 military personnel, and 1,638 contractor manyears. Overall administrative support is provided by the Washington Headquarters Service (WHS) under the Director for Administration and Management. WHS provides broad support for OSD organizations to include maintaining centralized information technology equipment (ITE) inventory records. WHS issues administrative instructions providing guidance to other organizations for ITE functions. The individual OSD organizations periodically update the WHS ITE inventory database while also maintaining their own inventory records.

Administrative Instruction No. 56. Administrative Instruction No. 56, "Automated Information Resource Management (AIRM) in the Office of the Secretary of Defense and Washington Headquarters Services," August 20, 1991, provides guidance for AIRM support to OSD and the WHS. The instruction generally covers the AIRM program. The instruction assigns WHS responsibility for maintaining and operating an automated centralized inventory control system that is compatible with the DoD-wide inventory system and meets the needs of Defense Information Systems Agency in accomplishing its ITE mission.

Automated Data Processing Resources Management. DoD Directive 7950.1, "Automated Data Processing Resources Management," September 29, 1980, provides policy guidance on the management and reporting of automatic data processing resources within the OSD and DoD Components. That directive was implemented by DoD 7950.1-M, "Defense Automation Resources Management Manual," September 1988, which provides consistent procedures, standards, policies, definitions, and requirements governing the redistribution, sharing, and inventorying of automation assets. The manual applies to all DoD Components.

Objectives

Our objective was to determine whether information technology equipment in the possession of the OSD was adequately managed. Work on this project included verifying existence and completeness of information technology equipment databases and other records used to control equipment within the OSD. We also assessed the management control program as it relates to the overall objective. See Appendix A for a discussion of the audit scope and methodology, our review of the management control program, and prior audit coverage, related to the audit objectives.

Management of Information Technology Equipment

The OSD practices and controls for managing ITE needed improvement. Based on a statistical test for existence and a nonstatistical test for completeness, ITE inventory records were incomplete and inaccurate. The existence test consisted of a physical inventory of statistically selected ITE items from a universe of about 34,000 items. The results of the existence test projected that an estimated 2,790 (8 percent) ITE items would not be located if a full inventory were conducted. The completeness test showed that of 635 ITE items judgmentally selected from OSD work spaces, 51 (8 percent) ITE items were not included on any OSD inventory records. In addition, we estimated that the records for 7,859 (23 percent) ITE items contained critical inventory data errors. In addition, security problems were identified when computers containing sensitive information were marked for reutilization outside of the DoD, and personal digital devices were used inappropriately in secure classified areas. The problems occurred because there was no single authority, such as a Chief Information Officer (CIO), managing the information technology equipment within the OSD. A CIO would have had the responsibility for ensuring that the OSD developed and implemented management controls related to an integrated, consistent process for receiving, recording, and disposing of information technology equipment. As a result, the OSD was at risk for the loss of computer equipment and the loss of sensitive and classified information.

Inventory Tests

The WHS maintains a centralized database of ITE owned by OSD. The database included about 34,000 ITE items such as central processing units, hard drives, personal computers, and computer monitors and was updated every 6 months by OSD component organizations. Our audit included two tests to measure the existence and completeness of overall inventory database accuracy. Existence tests measured the ability to physically locate the equipment recorded on the information technology inventory databases. Completeness tests ascertained whether equipment located in OSD work spaces was recorded on the information technology inventory databases.

Existence Test Results. We statistically sampled items from the 34,000 pieces of information technology equipment listed in the WHS active property database as of October 2, 2000. We conducted a physical inventory to determine whether OSD components could locate 635 selected items. The projected results of the existence test are provided in Table 1.

Table 1. Projected Existence Test Results

ITE Database Universe	Estimated Number of Items Not Found	Estimated Number of Significant ITE Data Errors
33,889	2,790	7,859

Based on the results of our statistical sampling, we estimated that about 2,790 (8 percent) ITE items would not be located if a complete wall-to-wall inventory was taken. Among the specific items in our sample not located were personal computers, laptops, and hard drives. For those items that were located, we verified that database information such as the location, serial number, bar code, and other identifying information of ITE were reported correctly in the WHS databases. We estimated that data errors would exist in the inventory records for 7,859 (23 percent) of the items. The data errors we noted, such as incorrect locations, would make it difficult for the OSD to effectively manage the large quantity of ITE in the database. (See Appendix A for the statistical sampling methodology and other information related to the existence test.)

Completeness Test Results. We selected 635 items of ITE on a nonstatistical basis located in the work spaces visited and determined whether the items were included on the WHS and component databases. The results are included in Table 2.

Table 2. Completeness Test Results

Total Work Spaces ITE Reviewed	Work Spaces ITE not on any OSD Database	Work Spaces ITE with Data Errors
635	51	319

The results showed that 51 (8 percent) of the 635 work space selections, which included personal computers and laptops, were not recorded on any OSD database. In addition, 319 (50 percent) of the supporting inventory records for 635 ITE items contained significant data errors on the OSD database. As noted in the existence test, data errors such as incorrect locations make it difficult to effectively manage ITE.

Single ITE Manager

The OSD did not have a single, centralized manager for information technology equipment within the OSD. A manager, such as a CIO, could have ensured that the OSD developed and implemented management controls related to an integrated, consistent process for receiving, recording, and disposing of information technology equipment. This manager could have also ensured that OSD policy and management control procedures for ITE were current and implemented by the OSD. At the time of the audit, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)] was only responsible for overall DoD policy related to automated data processing equipment and WHS had only limited responsibility for managing ITE within the OSD.

Information Technology Equipment Policies. The ASD(C^3I) had not issued updated ITE policies for the OSD. The most recent comprehensive policy document, DoD Directive 7950.1, was prepared more than 20 years ago, and does not reflect the state of information technology in existence at the time of this audit. The policy does not cover issues such as the use of personal digital devices and the ability of software to recover data on hard drives. The ASD(C^3I) recognized that the document was outdated and in early FY 2000, a draft policy document was prepared but was never issued. We were unable to determine the reason for not issuing the policy. As a result of the outdated policies, we observed poor security practices within the OSD. For instance, during the physical inventory, a personal digital device similar to a palm pilot was attached inappropriately to a computer processing unit designated to handle classified material. Such a practice can compromise national security because of the risk that classified information could be recorded on the personal digital device and taken out of the secure area on a nonrestricted device. We reported the incident as a potential security violation. Further, an additional 15 personal digital devices were observed in restricted classified areas in the OSD.

Washington Headquarters Services. A single ITE manager with clear authority would be able to issue and implement mandatory operating procedures and practices. The WHS issued administrative instructions and inventory bulletins covering the centralized database records, aspects of excessing equipment, and some disposal practices. The bulletins, however, were limited in scope, provided guidance that was not often followed and was not mandatory. WHS did not believe it had the authority to make its instruction mandatory. Each OSD component was expected to create its own policies and procedures within the overall guidance issued by WHS.

Chief Information Officer. The Clinger-Cohen Act of 1996, P.L. (104-106), Division E, Sec. 5002(3)(A), (B), and (C) requires all Government agencies to appoint a CIO responsible for overall management of automated systems. The ASD(C^3I) implemented this policy in DoD by requiring DoD Components to appoint CIOs; however, implementing instructions were never issued for OSD. Like the rest of the DoD, OSD would benefit from having a CIO.

Management Control Processes

The OSD lacked an integrated, consistent management control process for receiving ITE and maintaining an ITE inventory database. WHS Administrative Instructions generally did not mandate specific procedures for an ITE management control process. Each OSD organization was allowed to establish specific procedures for controlling ITE.

Control Process. The practices followed by OSD component organizations were not based on centralized or consistent procedures. For example, some OSD component organizations used bar coding for controlling inventory and others did not. An effective control process should include standard procedures for recording equipment in accountability records upon receipt. Such procedures would establish a clear record of who is using the equipment, for what purpose, and how it is disposed at the end of its useful life. We believe that the most effective accountability systems use a single record system and uniform policies and procedures for an entire organization.

Procedures for Receiving Equipment. ITE was being brought into OSD locations from multiple entry points. Equipment was delivered to multiple storage facilities and sent directly to work spaces. For example, two organizations maintained central warehouses for equipment, and one of these organizations generally ensured that all equipment was delivered to the warehouse. However, the same organization purchased ITE using Government credit cards and the ITE was delivered directly to work stations without accountability at the central warehouse. Several items from this organization could not be located during our audit, and the records for several other items contained errors. The use of a single entry point for all equipment would greatly increase the ability of the OSD to ensure that equipment was appropriately recorded in inventory records, marked, and controlled.

WHS Inventory Records. Administrative Instruction No. 56 designates WHS as the office responsible for maintaining ITE inventory records. WHS maintains a database intended to provide a central record of ITE for use in meeting information needs of the Defense Information Systems Agency. However, the WHS database did not include location and user information, a complete history of all equipment, and other information needed to effectively manage ITE. WHS updated the centralized database every 6 months using information provided by the OSD component organizations. As a result, the WHS centralized database did not include current information, especially for those organizations that failed to provide updated information. WHS relied on each OSD office to maintain separate records with more detailed information. There were 14 separate sets of automated inventory records in the OSD.

OSD Component Inventory Records. The individual OSD component inventory records we reviewed generally did not include information showing whether the equipment was used to process classified information, the reason for removing an item from inventory, and a history of an item from acquisition to disposition. Organizations also used different database formats and data elements. For example, one OSD organization deleted more than 500 items of

equipment, valued at more than $1 million, from its records in December 1999. We were unable to trace any of the equipment in the inventory records to determine the reasons recorded for the deletions and history for each item. A Defense Protective Service Investigation report covering the matter indicated that the items were either lost or removed from OSD locations as a result of poor accountability. The actual disposition of the 500 items will never be known because the entire record for the deleted items was removed by the OSD organization instead of modifying the record to show the reason for the loss. The lack of adequate detail, inaccurate and incomplete records, and inconsistent database layouts all contributed to poor inventory records.

WHS Accountability. Although WHS had overall inventory responsibility, it had delegated the detailed accountability functions to each OSD component. During the period from 1995 to 1999, WHS performed periodic inventory spot checks to check the accuracy of OSD records. The results of the spot checks showed that most OSD components were improving but ITE accountability problems still remained. The WHS spot checks for 2000 were not conducted because of our audit. In view of the large numbers of missing items, unrecorded items and inaccurate records, a wall-to-wall inventory is needed to establish a complete database, with physical inventories taken annually to ensure the accuracy of inventory records. The physical inventories could be part of the annual management control assessments already required by DoD.

OSD Computer Disposal Practices

OSD disposal practices were not adequate for safeguarding the sensitive information residing in DoD computers. OSD did not have current guidance for OSD components to follow. The most recent guidance was issued more than 20 years ago, before many of the technologies commonly in use today were available.

Reutilization of DoD Computers. Until November 2000, the OSD participated in a computer reutilization program. The procedures for excessing OSD computers call for swiping clean or sanitizing the hard drives of computers that do not contain classified information. Our initial visit to the WHS warehouse used to store excess OSD computers in the reutilization program resulted in the identification of four computers that contained either sensitive or classified information on the hard drives. In accordance with existing procedures, the owning organizations were supposed to have “swiped” the hard drives clean and a WHS official was supposed to have certified that the computers no longer contained sensitive or classified information. However, these procedures were not followed. In addition, we were also able to use software to reconstruct information that was supposedly removed from the hard drives. As a result, the disposal of any OSD computer that processes sensitive or classified information represents a potential risk.

Deputy Secretary of Defense Actions

On October 31, 2000, we advised the Secretary of Defense of weaknesses in OSD computer disposal operations. On November 7, 2000, the Deputy Secretary of Defense directed immediate action to correct the weaknesses within the OSD and then on January 8, 2001, he directed the destruction of all DoD computer hard drives prior to disposal of computers outside of DoD. Subsequently, the DoD Chief Information Officer Executive Board established a working group to review issues and refine the policy related to the Deputy Secretary of Defense direction to destroy DoD computers hard drives prior to disposal.

On December 4, 2000, we advised the Secretary of Defense of weaknesses in the inventory management of OSD computer equipment, and provided proposed recommendations for corrective action. On December 15, 2000, the Deputy Secretary of Defense stated that he wanted to implement the Inspector General's recommendations and directed the ASD(C^3I) to take immediate action to correct the inventory management problem. (See Appendix B for the three Deputy Secretary of Defense Memorandums.) We believe an action plan with milestones should be prepared to ensure prompt implementation of the recommendations.

Recommendations, Management Comments, Audit Response

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence):

1. Establish a time-phased plan to implement the recommendations directed by the Deputy Secretary of Defense during the audit. The recommendations include:

a. Establish a Chief Information Officer for the Office of the Secretary of Defense with responsibility for developing an integrated, consistent management control process for managing information technology equipment within the Office of the Secretary of Defense;

b. Rely on a single inventory database and standard process for controlling information technology equipment. Replace all existing databases with a single database designed to meet the needs of multiple users;

c. Perform a wall-to-wall physical inventory of information technology equipment within the Office of the Secretary of Defense and establish quality control procedures to ensure that the master database inventory is maintained on a real-time basis;

d. Require comprehensive information technology equipment inventory reviews at least annually, preferably as part of each office's management control self-assessments;

e. Establish a clear chain of custody for equipment, including using hand receipts signed by the end user of the equipment;

f. Establish a single entry and exit point for all information technology equipment, ensuring that all equipment is recorded on inventory records before release to the user and then is appropriately excessed; and

g. Implement a policy (as directed by the Deputy Secretary of Defense memorandum of December 15, 2000) that requires all hard drives of OSD computers being disposed of outside the DoD be destroyed.

2. Develop policy regarding the proper use of current technology items, such as personal digital devices, with secure classified computers.

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments. The Deputy Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, and Deputy Chief Information Officer of DoD acknowledged the concurrence of the Deputy Secretary of Defense to the audit report findings and recommendations. The Deputy Assistant Secretary stated that actions were underway to provide for the DoD CIO to serve as the OSD CIO through updates to DoD Directive 8000.1, "Management of Department of Defense Information Resources and Information Technology" and WHS issued updated guidance on January 22, 2001, for removal of all hard drives prior to surplus turn-ins of excess ITE. The Deputy Assistant Secretary stated he had concern about the cost to implement several of the inventory management recommendations, and that his office would follow investment management guidance while considering the cost benefit of each recommendation, the potential return on investment, and the affordability to include the impact on the full life-cycle requirements for acquiring, managing, and disposing of ITE. Further, as they develop their time-phased implementation plan, they will evaluate alternatives for satisfying the recommendations.

As part of these alternatives, on March 6, 2001, the Director of the Washington Headquarters Services issued policy prohibiting digital devices in Pentagon Sensitive Compartmented Information Facilities unless digital devices were modified to prevent data transmission.

Audit Response. The ongoing and proposed actions will benefit the effectiveness of the ITE management program in the OSD. We request the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) provide additional comments describing when the time-phase implementation plan will be completed.

Washington Headquarters Services Comments. The Director, Washington Headquarters Services, provided comments for clarification purposes, and emphasized inventory management improvements achieved since 1991. The

Director stated that the draft report was misleading in stating that the results of inventory spot checks performed between FY 1995 and FY 1999 showed that most of the OSD components had accountability problems. Through hard work, OSD has improved its accountability of ITE based on the results of equipment existence spot checks from 54 percent in 1995 to 94 percent in 1999. The results in 1999 were compromised by two OSD components that scored only 78 and 50 percent on the existence spot checks. The Director also commented that further analysis of alternatives was advisable before commitment to a single inventory system is made and more resources are applied to achieve marginal improvement.

Audit Response. We agree that the spot checks indicate improvement in ITE accountability practices since 1995. However, the value of the pre-announced spot check as a management tool is limited. Unannounced statistical samples are more appropriate for measuring the implementation of internal controls. More importantly, we believe that the OSD should set a strong example within the DoD for emphasis on inventory control and security. The Director's concerns regarding the need for further analysis are noted, but the Deputy Secretary of Defense and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) have already concurred with the recommendation and with the need to improve inventory control.

Under Secretary of Defense for Policy Comments. The Director, Policy Automation, Office of the Deputy Under Secretary of Defense Policy Support, expressed concerns regarding problems with the conduct of the audit that may have contributed to erroneous conclusions, raising a question about the credibility of the audit. The Director offered to have us review worksheets that detailed the errors. Further, the Director had concerns with several of the recommendations in the report. Specifically, the Director stated that a single system to control all OSD equipment is not reasonable and that it is impossible to physically inventory everything at one snapshot in time in a "wall-to-wall" inventory. The Director further stated that hand receipting all users may result in a loss of control and establishment of a single point of entry for the OSD would compound the problems of tracking procurement actions to delivery orders.

Audit Response. We accepted the Director's offer to review the worksheets of his staff. The worksheets and associated analysis did not refute the facts and conclusions as presented in our report. The recommendations with which the Director disagrees were made to another OSD component and the Deputy Secretary of Defense has previously directed implementation of the recommendations.

Appendix A. Audit Process

Scope

Work Performed. This audit focused on whether information technology equipment in the possession of the Office of the Secretary of Defense is adequately managed. The WHS provided a copy of the ITE inventory database that contained 33,889 inventory records as of October 2, 2000. We statistically selected 635 items from the database for review. In addition, we judgmentally selected 635 items from the locations visited for review. We reviewed the procedures for recording and reporting ITE inventory data. We conducted our review at the offices of the Secretary of Defense within the Washington Metropolitan area. See Appendix C for a list of the offices visited.

DoD-Wide Corporate-Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following objectives and goal, subordinate performance goal, and performance measure.

- **FY 2001 DoD Corporate-Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the Revolution in Military Affairs, and reengineer the Department to achieve a 21st century infrastructure. **(01-DoD-02)**

- **FY 2001 Subordinate Performance Goal 2.3:** Streamline the DoD infrastructure by redesigning the Department's support structure and pursuing business practice reforms.

- **FY 2001 Subordinate Performance Goal 2.5:** Improve DoD financial and information management. **(01-DoD-2.5)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Use of Computer-Processed Data. To achieve the audit objective, we extensively relied on computer-processed data from WHS inventory database and databases from various OSD components when available. The results of our data testing showed an error rate that casts doubt on the data accuracy. However, when the data are reviewed in context with other available evidence, we believe that the opinions and conclusions in this report are valid.

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from October 2000 through January 2001 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We included tests of management controls considered necessary.

Potential Security Violations. We referred two potential security violations to the cognizant security offices for action.

Contacts During the Audit. The organizations contacted during the audit are listed in Appendix C.

Statistical Sampling Methodology

Sampling Purpose. The purpose of the statistical sampling plan was to estimate the number of items missing from or not properly recorded in the information technology equipment database.

Universe Represented. WHS provided a database of information technology equipment as of October 2, 2000. The database consisted of 33,889 items with a total value of $99.8 million.

Sampling Design. The sampling design used to determine whether or not items were missing from or whether or not items were properly recorded in the information technology equipment database was a stratified attribute design. We divided the population into two strata: a census strata, which consisted of the five largest data processing installation identifier codes, and an all other strata. The census strata contained 72 percent of the items. A random sample of 105 items was selected for review from each of the five data processing installation identifier codes that made-up the census strata. From all other strata, 110 items were randomly selected for review.

Sample Results. We derived the following statistical estimates from the information technology equipment database:

Missing Items and Data Errors Statistical Bound (95 Percent Confidence Intervals)			
	Lower Bound	Point Estimate	Upper Bound
Items Missing	2,049	2,790	3,531
Data Errors	6,714	7,859	9,004

Management Control Program Review

DoD Directive 5010.38, "Management Control Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of Review of Management Control Programs. We reviewed the adequacy of management controls over procedures to ensure that ITE is accurately recorded and reported. We did not assess management's self-evaluation of those controls.

Adequacy of Management Controls. We identified material management control weaknesses at the OSD as defined by DoD Instruction 5010.40. Weak management controls at OSD components were exhibited by the lack of a centralized process for receiving, controlling, and disposing of ITE. No single official was responsible for control and management of ITE. Responsibilities for ITE policies and procedures were divided among many offices, and individuals were not made clearly responsible for the security and control of equipment assigned to them. A copy of the report will be provided to the Director, Administration and Management, who is responsible for management controls in the OSD.

Prior Coverage

The Inspector General, DoD, issued one investigation report relating to OSD ITE issues, "Allegations of Breaches of Secretary of Defense, Dr. John M. Deutch, Former Deputy Secretary of Defense and Former Under Secretary of Defense for Acquisition and Technology," August 28, 2000

Appendix B. Deputy Secretary of Defense Responses to the Inspector General, DoD, Preliminary Findings and Recommendations

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JAN 0 8 2001

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Destruction of DoD Computer Hard Drives Prior to Disposal

Historically, the Department's policies regarding sanitization and destruction of computer hard drives have been applied only to equipment that processed classified information. More recently, the proliferation of networked unclassified desktop computers, with their ability to retain vast amounts of information, and the resultant possibility of increased sensitivity of the aggregated data, dictated that we properly sanitize unclassified computer equipment before it is turned in for disposal or reutilization. Notwithstanding these precautions, preliminary results of a recent Inspector General audit have revealed instances of sensitive information remaining on computer hard drives that had been certified as having been "wiped" clean (i.e., they contain no sensitive information) prior to disposal or reutilization outside DoD.

Accordingly, I direct that you take immediate steps to ensure that all hard drives of unclassified computer equipment being disposed of outside DoD are removed and destroyed. Guidance for destruction may be found at ***http://www.c3i.osd.mil/org/sio/ia/diap/***.

The Assistant Secretary of Defense (C3I) will assess this implementation and determine, within 12 months, if further adjustments are warranted. Questions concerning this memorandum may be directed to Mr. Donald Jones, OASD(C3I)/IA, at 703-614-6640.

Rudy de Leon

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

15 DEC 2000

MEMORANDUM FOR THE ASSISTANT SECRETARY (COMMAND, CONTROL, COMMUNICATIONS & INTELLIGENCE)

As you know, Pentagon Security is one of my top priorities. I have reviewed the attached memo from the Department of Defense Inspector General regarding weaknesses in the management of OSD computer equipment. I want to implement their recommendations. I direct you to take immediate action to correct these problems.

cc: Secretary of Defense
DoD IG

Attachment

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

- 7 NOV 2000

MEMORANDUM FOR ART MONEY
LINN WELLS

SUBJECT: OSD Computer Disposal

As you know, Pentagon Security is one of the Secretary's and my top priorities. I have reviewed the attached memo from the DoD IG regarding OSD computer disposal practices. I want to implement their recommendations. I direct you take immediate action.

Rudy DeLeon

cc: Sec Def
DOD IG

Appendix C. Component Organizations of the Office of the Secretary of Defense Visited During the Audit

We conducted our review at the following offices of the Secretary of Defense within the Washington Metropolitan area:

Under Secretary of Defense

- Under Secretary of Defense for Policy
- Under Secretary of Defense for Acquisition, Technology, and Logistics
- Under Secretary of Defense (Comptroller)
- Under Secretary of Defense for Personnel and Readiness

Assistant Secretary of Defense

- Assistant Secretary of Defense (Legislative Affairs)
- Assistant Secretary of Defense (Health Affairs)
- Assistant Secretary of Defense (Public Affairs)
- Assistant Secretary of Defense (Reserve Affairs)
- Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

Other OSD Organizations

- Assistant to the Secretary of Defense (Intelligence Oversight)
- Assistant to the Secretary of Defense (Executive Secretariat)
- Defense Acquisition University
- DoD Joint Defense Total Asset Visibility Office
- Office of Economic Adjustment
- Strategic Environmental Research and Development Program
- Space Architecture
- Test Systems Engineering and Evaluation

- Information Technology Directorate
- Director, Program Analysis and Evaluation
- General Counsel
- Director, Operations Test and Evaluation
- Office of the Special Assistant for Gulf War Illnesses
- Director, Administration and Management
- Enterprise Support Organization
- Air Force Pentagon Communication Agency (OSD Support)
- Defense Supply Service – Washington (OSD Support)

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Under Secretary of Defense for Personnel and Readiness
  Assistant Secretary of Defense (Health Affairs)
  Assistant Secretary of Defense (Reserve Affairs)
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Public Affairs)
Assistant to the Secretary of Defense (Intelligence Oversight)
General Counsel
Director, Administration and Management
Director, Operational Test and Evaluation

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Washington Headquarters Services

Non-Defense Federal Organizations and Individuals

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

March 1, 2001

MEMORANDUM FOR OFFICE OF DOD INSPECTOR GENERAL,
DIRECTOR OF FINANCE & ACCOUNTING

Subject: Audit Report on Management of Information Technology Equipment, Office of the Secretary of Defense (Project No. D2001FA-0040)

As requested in your memorandum dated January 30, 2001, same subject, we reviewed the draft report and provide the following comments.

We recognize the concurrence of the Deputy Secretary of Defense in the report's finding and recommendations. We have concerns that several of the inventory management recommendations would be of considerable cost to implement. As we develop our time-phased implementation plan, we will evaluate alternatives for satisfying the recommendations. We will follow investment management guidance while considering the cost benefit of each recommendation, the potential return on investment, and affordability, including the process implementation costs. We will also consider the impact on the full life cycle management requirement for acquiring, managing, and disposing of information technology assets.

These are actions completed or underway in support of the recommendations.

a. DoD 8000.1, Management of Department of Defense (DoD) Information Resources and Technology, is out for formal DoD-wide coordination. A provision of this updated issuance is for the DoD CIO to serve as the CIO for OSD.

b. WHS issued updated OSD guidance for excessing information technology equipment on January 22, 2001. The updated guidance calls for the removal of all hard drives prior to surplus turn-in.

If you have additional questions, Connie Leonard, 703-602-2536, is my point of contact.

Paul R. Brubaker
Deputy Assistant Secretary of Defense
Deputy Chief Information Officer

Washington Headquarters Services Comments

Final Report Reference

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

FEB 27 2001

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL, DOD
ATTENTION: DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE

SUBJECT: Draft Audit Report on Management of Information Technology Equipment, Office of the Secretary of Defense (Project No. D2001FA-0040)

As requested in your memorandum of January 30, 2001, we have reviewed the subject report and acknowledge that the Deputy Secretary of Defense has already concurred with the report's recommendations. Accordingly, the following comments and recommendations are provided for clarification purposes regarding implementation issues as opposed to accepting or rejecting recommendations contained in the report.

In several places, the report correctly states that the OSD current inventory database contained 33,889 items. However, the value of the current inventory is actually $99.8 million, not $631.5 million as stated in other parts of the report. Revised

On page 6, under WHS Accountability, the report states that WHS performed inventory spot checks from 1995 through 1999 and the results showed that most of the OSD Components had accountability problems. We believe this is misleading, needs to be clarified, and could have led to different recommendations as a result of the study.

When WHS took over the OSD inventory reporting function in 1991, only three inventory records had been reported to DISA since 1988 via a centralized system. WHS and the OSD Components have worked hard to improve the OSD inventory accountability since that time. Specifically, WHS took the initiative to start floor-to-book and book-to-floor spot checks of the OSD Components that showed steady improvement as follows:

FY 1995	54%
FY 1996	74%
FY 1997	81%
FY 1998	89%
FY 1999	94%
FY 2000	92% (Subject IG Audit)

In the FY 1999 spot check, most of the OSD Components actually returned results of 100% and did not have accountability problems. A few were above 90%, one was at

78%, and one was at 50%. We believe the root causes of the problems with the lower scoring organizations are a lack of management focus on the inventory function, inadequately trained personnel, failure to record equipment moves, and high turnover of personnel in the inventory management area, not the lack of a centralized system.

The Clinger-Cohen Act of 1996 establishes the requirement to evaluate the business case and conduct cost benefit and risk-adjusted return on investment analyses before investing in information technology. The acquisition regulations require that analyses of alternatives be performed as well. We believe that the business case to achieve the marginal improvement in inventory accountability from 92% to some higher level needs to be conducted before proceeding to the design of a new system as recommended. For example, the simple addition of two data elements (person and location) to the existing system is a very low cost change that would significantly enhance accountability.

Similarly, a business case and attendant analyses need to be conducted on a centralized delivery and disposal activity. Of major concern are the additional costs associated with multiple deliveries and handling of the same equipment and the contribution of such an undertaking to the marginal improvement in the inventory accountability.

My point of contact on this matter is Mr. Robert S. Drake, (703) 604-4569 or drakeb@dior.whs.mil.

D. O. Cooke
Director

cc: Mr. Drake

Under Secretary of Defense for Policy Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

POLICY

February 28, 2001

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL (DIRECTOR, FINANCE AND ACCOUNTING DIRECTORATE)

SUBJECT: Audit Report on Management of Information Technology Equipment, Office of the Secretary of Defense (Project No. D2001FA-0040)

Thanks you for the opportunity to coordinate on this draft report.

Our analysis of the draft audit report indicates problems in the conduct of the inspection that may have contributed to some erroneous conclusions raising a question about the credibility of the audit. Our analysis of the missing items is that auditors transposed numbers or read the wrong numbers on over 80% of the equipment reported as having a problem in Policy. In reality, the problems in Policy are not nearly as serious as the audit report reflects and we suspect that the same is true in other OSD components. We recommend that the IG return and evaluate again the produced data to ensure an accurate picture is presented. To assist, we have worksheets that specifically identify the errors made which are available from our POC identified below.

With respect to the draft findings, we do not concur or have serious problems with a number of the audit recommendations as commented on below:

- We have no objection to the establishment of an OSD CIO. We do contend it would not fix the problems identified in the report. Problems that are identified and verified must be corrected by management action within the organizations affected.

- Establishing a single system to control all OSD equipment is not reasonable. Policy has requirements for additional data elements such as highest classification level processed on equipment. This information in aggregate is classified. We also need control of our database to make it available to Helpdesk personnel on our classified system to assist in problem resolution. We currently pass unclassified information to the centralized WHS database and feel strongly we need to maintain control of that portion containing Policy assets.

- We concur with a requirement for a full and accurate inventory. Within Policy our inventory custodial managers are tasked to accomplish this on an annual basis. You do need to recognize with over 800 items of portable equipment, it is impossible to physically inventory everything at one snapshot in time in a "wall-to-wall" inventory.

- We non-concur with the proposal that all equipment be hand receipted to users. Policy desktop equipment is office oriented and not controlled by the individual user. Much of the equipment is shared in kiosk fashion. The chain of custody system established within Policy meets our needs. Each user signs hand receipts for portable IT equipment and is responsible to the custodian for it. Each custodian is responsible for all items in the account. Requiring hand receipts for all IT equipment would result in significant additional workload and probably decrease control.

- We non-concur with the establishment of a single OSD entry point for IT purchases. We have a difficult time now tracking our procurement actions to delivery orders. Expanding this volume five fold would only exacerbate these problems. Policy would also be forced to abandon our initiative to mask from vendors that a procurement is destined for our classified environment. This would be detrimental to the mission and security of this organization.

With respect to the overall recommendations of the Audit, they seem to violate the intent of the Clinger Cohen Act unless we accomplish the requisite cost benefit analysis requirements before proceeding with system changes. Recommend that OSD organizations be given the opportunity to improve IT equipment management, with a follow-up audit within nine months. After an accurate follow-up audit, if major problems persist, procedural changes may be warranted.

My point of contact for inventory activity is Mr Robert Smolinski, (703) 697-5149.

Ronnie R. Larson
Director, Policy Automation
Office of the Deputy
USD Policy Support

Audit Team Members

The Finance and Accounting Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

F. Jay Lane
Salvatore D. Guli
Charles J. Richardson
Walter R. Loder
Adrienne B. Brown
Michael L. Davitt
Bryan K. Kitchens
Linh Truong
Barry D. Gay
Walter J. Gaich
John W. Wright
Charles A. Mordecai
Alejandra Rodriguez
Lusk Penn