

**GAO**

Report to the Subcommittee on  
Oversight and Investigations,  
Committee on Veterans' Affairs, House  
of Representatives

---

July 2008

# VETERANS AFFAIRS

## Continued Action Needed to Reduce IT Equipment Losses and Correct Control Weaknesses





Highlights of [GAO-08-918](#), a report to the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

## VETERANS AFFAIRS

### Continued Action Needed to Reduce IT Equipment Losses and Correct Control Weaknesses

#### Why GAO Did This Study

In July 2004, GAO reported that the six Department of Veterans Affairs (VA) medical centers it audited lacked a reliable property control database and effective inventory policies and procedures. In July 2007, GAO reported that continuing internal control weaknesses over IT equipment at four case study locations at VA resulted in an increased risk of theft, loss, and misappropriation of IT equipment assets. GAO's two reports included 18 recommendations to improve internal control over IT equipment. GAO was asked to perform a follow-up audit to determine (1) whether VA has made progress in implementing GAO's prior recommendations for improving internal control over IT equipment and (2) the effectiveness of VA's current internal controls to prevent theft, loss, or misappropriation of IT equipment. GAO reviewed policies and other pertinent documentation, statistically tested IT equipment inventory controls at four geographically disparate locations, and interviewed VA officials.

#### What GAO Recommends

GAO makes five recommendations to VA for additional actions to strengthen the overall control environment and improve specific internal control activities and safeguard IT equipment. VA's initial response stated that it generally agreed with four of GAO's five recommendations. After further clarification, VA officials stated that they agreed with the intent of all of GAO's recommendations and were taking steps to address them.

To view the full product, including the scope and methodology, click on [GAO-08-918](#). For more information, contact Kay L. Daly at (202) 512-9095 or [dalykl@gao.gov](mailto:dalykl@gao.gov).

#### What GAO Found

VA has made significant progress in addressing prior GAO recommendations to improve controls over IT equipment. Of the 18 recommendations GAO made in its two earlier reports, VA completed action on 14 recommendations, partially implemented action on 2 recommendations, and is working to address the 2 remaining open recommendations. These recommendations focused on strengthening policies and procedures to establish a framework for accountability and control of IT equipment. If effectively implemented, VA's July 2008 policy changes would address many of the control weaknesses GAO identified. Mandated early implementation of this new policy addresses user-level accountability and requirements for strengthening physical security. In addition, to determine the extent of inventory control weaknesses over its IT equipment, VA performed a departmentwide physical inventory in 2007. However, as of May 15, 2008, VA reported that it could not locate about 62,800 IT equipment items, of which 9,800 could have stored sensitive information. Because VA does not know what, if any, sensitive information resided on the equipment, potentially affected individuals could not be notified.

GAO's statistical tests of IT equipment inventory controls from February through May 2008 at four locations identified continuing control weaknesses, including missing items, lack of accountability, and errors in IT equipment inventory records. Although these control weaknesses may be addressed through early implementation of the July 2008 policies, the fact that GAO identified missing items only a few months after these locations had completed their physical inventories is an indication that underlying weaknesses in accountability over IT equipment have not yet been corrected.

#### IT Inventory Control Test Results at Four Case Study Locations

	North Texas	Boston	Puget Sound	VA
Control failures	HCS	HCS	HCS	headquarters
Missing items	6%	3%	1%	12%
Incorrect user organization	91%	60%	76%	12%
Incorrect location	46%	17%	14%	33%
Recordkeeping errors	9%	41%	9%	4%

Source: GAO analysis.

Note: Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 10 percent or less.

GAO's tests identified 50 missing items, of which 34 could have stored sensitive data, but again, notifications to individuals could not be made. Further, the lack of user-level accountability and inaccurate records on status, location, and item description of IT equipment items at the four case study locations make it difficult to determine the extent to which actual theft, loss, or misappropriation of IT equipment may have occurred. In addition, the four locations had weaknesses in controls over hard drives in the property disposal process as well as physical security weaknesses at IT storage facilities. These control weaknesses present a risk that VA could lose control over new, used, and excess IT equipment and that any sensitive personal and medical information residing on hard drives in this equipment could be compromised.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	4
	Background	7
	VA Has Made Significant Progress in Addressing GAO Recommendations and Completing a VA-Wide IT Equipment Inventory	10
	Tests of IT Inventory Controls at Case Study Locations Identified Continuing Weaknesses	15
	Conclusions	28
	Recommendations for Executive Action	29
	Agency Comments and Our Evaluation	30
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>32</b>
<b>Appendix II</b>	<b>Status of VA Actions on Recommendations in GAO's July 2007 and 2004 Reports</b>	<b>37</b>
<b>Appendix III</b>	<b>Comments from the Department of Veterans Affairs</b>	<b>41</b>
<b>Appendix IV</b>	<b>Reports of Survey on Missing IT Equipment for VA Case Study Locations</b>	<b>45</b>
<b>Appendix V</b>	<b>GAO Contact and Staff Acknowledgments</b>	<b>46</b>
<b>Tables</b>		
	Table 1: Overview of Key Controls in VA's IT Property Management Process	8
	Table 2: Status of VA's Actions on Prior Recommendations	12
	Table 3: Summary of VA-Wide Fiscal Year 2007 IT Equipment Physical Inventory Results as of May 15, 2008	14
	Table 4: Numbers of Missing IT Equipment Items at Four Test Locations That Were Identified during the 2007 VA-Wide IT Physical Inventory	16

---

Table 5: Estimated IT Equipment Inventory Control Failure Rates at Four Test Locations	17
Table 6: Number of Missing IT Equipment Items by Headquarters Organization and Missing Items That Could Have Stored Sensitive Personal Data	20
Table 7: Estimated IT Inventory Control Failure Rates Related to Correct User and Location at the Four Test Locations	21
Table 8: Estimated Percentages of Other IT Inventory Recordkeeping Failures at Four Test Locations	23
Table 9: Population of VA IT Equipment at Locations Selected for Testing	33
Table 10: GAO's 2007 Report Recommendations and Status of VA Actions as of July 2008	37
Table 11: GAO's 2004 Report Recommendations and Status of VA Actions as of July 2008	39
Table 12: Summary of Reports of Survey as of May 15, 2008, for Case Study Locations Covered in GAO Audits	45

---

---

## Abbreviations

AEMS/MERS	Automated Engineering Management System/Medical Equipment Repair Service
CFR	Code of Federal Regulations
CIO	Chief Information Officer
EIL	equipment inventory listing
ELF	Equipment Loan Form
FMFIA	Federal Managers' Financial Integrity Act of 1982
HCS	health care system
HHS	Department of Health and Human Services
HIPAA	Health Information Portability and Accountability Act of 1996
IT	information technology
NARA	National Archives and Records Administration
NCA	National Cemetery Administration
OAL	Office of Acquisitions and Logistics
OIT	Office of Information and Technology
OMB	Office of Management and Budget
SMC	Security Management Committee
USC	United States Code
VA	Department of Veterans Affairs
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VISN	Veterans Integrated Service Network

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

July 31, 2008

The Honorable Harry E. Mitchell  
Chairman  
The Honorable Ginny Brown-Waite  
Ranking Member  
Subcommittee on Oversight and Investigations  
Committee on Veterans' Affairs  
House of Representatives

This report responds to your request that we perform a follow-up audit to assess the Department of Veterans Affairs (VA) progress in strengthening controls over information technology (IT) equipment. Past reports of thefts of laptop computers and data breaches raised concerns about the adequacy of controls over VA IT equipment. In July 2004, we reported<sup>1</sup> that the six VA medical centers we audited lacked a reliable property control database and had problems with implementation of VA inventory policies and procedures. In July 2007, we reported<sup>2</sup> that a weak overall control environment and pervasive weaknesses in inventory control and accountability at four locations we audited put IT equipment at risk of theft, loss, and misappropriation, including sensitive personal and medical information maintained on this equipment. For example, our statistical tests of IT equipment inventory controls at the four VA case study locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive information. Our 2004 and 2007 audits found that some medical centers did not account for IT equipment valued under \$5,000 during physical inventories. Our 2004 report made 6 recommendations and our 2007 report made 12 recommendations for VA actions to improve accountability of IT equipment inventory and reduce the risk of disclosure of sensitive personal and medical information.

VA's mission is to promote the health, welfare, and dignity of all veterans in recognition of their service to the nation by ensuring they receive

---

<sup>1</sup>GAO, *VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement*, [GAO-04-755](#) (Washington, D.C.: July 21, 2004).

<sup>2</sup>GAO, *Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*, [GAO-07-505](#) (Washington, D.C.: July 16, 2007).

---

medical care, benefits, social support, and lasting memorials. The department's three major components are the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA). During 2007, VA employed over 230,000 individuals and relied on an undetermined number of contractors, volunteers, and students in carrying out its operations. VA provided these individuals with a wide range of IT equipment, including desktop and laptop computers, monitors and printers, personal digital assistants, unit-level workstations, local area networking equipment, and medical equipment capable of storing sensitive personal and medical information.<sup>3</sup> By the start of fiscal year 2008, VA had centralized its IT function at all locations within its Office of Information and Technology (OIT). OIT staff share responsibility for management of IT equipment inventory with property management personnel. Accordingly, it is crucial for the department's Assistant Secretary for Information and Technology, who serves as the Chief Information Officer (CIO), to have the cooperation of property managers to ensure that well-established integrated processes exist for controlling IT inventory. Given the continuing nature of IT equipment inventory control problems and their significance, you asked us to perform additional follow-up work to determine (1) whether VA has made progress in implementing our prior recommendations for improving internal control over IT equipment and (2) the effectiveness of VA's current internal controls to prevent theft, loss, or misappropriation of IT equipment.

To achieve our first objective, we conducted interviews and obtained documentation from VA property management and OIT officials on the actions taken to address the 12 recommendations in our July 2007 report and the 6 property-related recommendations in our July 2004 report. As you requested, we also reviewed the process and results of VA's 2007 departmentwide physical inventory of IT equipment and actions taken to resolve discrepancies, including VA inventory results for locations tested in our current and prior audits.<sup>4</sup> In addition, we reviewed policy revisions

---

<sup>3</sup>For the purpose of this audit, we included in our definition of IT equipment any equipment capable of storing or processing data, regardless of how VA classifies it. Therefore, medical devices that would typically not be classified as IT equipment, but may capture, process, or store patient data, were considered IT equipment for this audit. For example, we included electrocardiograph, anesthesiology, and ultrasound equipment in our tests.

<sup>4</sup>Our 2007 audit covered medical centers in Washington, D.C.; Indianapolis, Ind.; San Diego, Calif.; and VA headquarters organizations. Our 2004 audit covered medical centers in Atlanta, Ga.; Houston, Tex.; Los Angeles, Calif.; San Francisco, Calif.; Tampa, Fla.; and Washington, D.C.

---

related to IT equipment controls based on our prior recommendations. To achieve our second objective and determine the effectiveness of current internal controls for preventing theft, loss, or misappropriation of IT equipment, we used a case study approach, selecting three geographically disparate VA health care systems<sup>5</sup> (HCS) located in Dallas, Texas; Seattle, Washington; and Boston, Massachusetts. We also selected VA headquarters organizations<sup>6</sup> as a means of assessing the overall control environment, or “tone at the top,” as we did in our 2007 audit. At each of the four case study locations, we statistically tested IT equipment inventory control attributes for existence (meaning IT equipment items listed in inventory records exist and can be located), user-level accountability, and inventory record accuracy. As in our 2007 audit, at each of our case study locations we also evaluated (1) VA’s Reports of Survey<sup>7</sup> on lost and stolen items, (2) controls over computer hard drives in the excess property disposal process,<sup>8</sup> and (3) physical security controls for IT storage facilities. We performed sufficient procedures to determine that inventory data at the test locations were reliable for the purpose of our audit,<sup>9</sup> including data analysis, interviews of key officials, and review of VA procedures for assuring the reliability of data generated by key property inventory systems.

We conducted this performance audit from January 2008 through July 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

---

<sup>5</sup>Each of the three HCS locations included multiple medical facilities.

<sup>6</sup>Our tests of VA headquarters consist of separate strata for 6 organizations and a seventh strata for all other organizations.

<sup>7</sup>The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

<sup>8</sup>As used in this report, the term excess property refers to property that a federal agency leases or owns that is not required to meet either the agency’s needs or any other federal agency’s needs.

<sup>9</sup>The population of IT equipment items for the four test locations did not include the population of all IT equipment at those locations. Therefore, we can project our test results to the population of current, recorded IT equipment inventory at each location, but not the population of all IT equipment. Our tests were specific to each of the case study locations and cannot be projected to VA IT equipment inventory as a whole.



---

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We performed our investigative procedures in accordance with quality standards as set forth by the President's Council on Integrity and Efficiency. A detailed discussion of our objectives, scope, and methodology is included in appendix I.

---

## Results in Brief

VA has made significant progress in addressing our previous recommendations. These recommendations focused on strengthening policies and procedures to establish a framework for accountability and control of IT equipment. As of the end of our field work in July 2008, VA had completed action on 10 of the 12 recommendations in our July 2007 report<sup>10</sup> and partially implemented actions on 1 other recommendation. VA also has actions under way to address the remaining recommendation in our 2007 report. Further, VA completed action on 4 of 6 property-related recommendations in our 2004 report,<sup>11</sup> partially completed action on a fifth recommendation, and has plans to address the remaining 2004 recommendation. Details of VA's actions on our recommendations to strengthen controls over IT equipment are presented in appendix II. Importantly, VA's Assistant Secretary for Management and the CIO have worked together to draft a revised property management policy in a new VA Handbook 7002, *Logistics Management Procedures*, which includes requirements for user-level accountability, time frames for completing Reports of Survey<sup>12</sup> on missing and stolen property, and requirements for strengthening physical security. On July 3, 2008, VA's Assistant Secretary for Management mandated early implementation of the handbook.<sup>13</sup> If effectively implemented, the handbook changes would address many of the control weaknesses we identified. Further, in 2007 VA performed a departmentwide physical inventory of IT equipment at the Subcommittee's direction. Commensurate with the centralization of IT functions under the

---

<sup>10</sup>GAO-07-505.

<sup>11</sup>GAO-04-755.

<sup>12</sup>The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

<sup>13</sup>The Assistant Secretary for Management's July 3, 2008, information letter states that although the draft handbook was under final review within VA, the contents of the handbook "are of such importance that the policies and procedures need to be implemented as soon as possible."

---

CIO, including IT asset management, OIT monitored the inventory effort. Initially VA's physical inventory determined that approximately 79,000 IT equipment items were missing. After several months of searching and research of property records, as of May 15, 2008, OIT reported that approximately 62,800 recorded IT equipment items could not be located, of which over 9,800 could have stored sensitive information. Because VA does not know what, if any, sensitive information resided on the equipment, notifications to potentially affected individuals could not be made.<sup>14</sup> Facility personnel were continuing to search for missing items, and the CIO formed a quick response team to help ensure that Reports of Survey on lost and stolen items are completed in a timely manner.

Our tests of IT equipment inventory controls conducted from February through May 2008 at four case study locations, including three VA HCS and VA headquarters, identified continuing control weaknesses related to missing items, lack of accountability, and errors in IT equipment inventory records. Our *Standards for Internal Control in the Federal Government*<sup>15</sup> requires agencies to establish physical control to secure and safeguard vulnerable assets, such as equipment that might be vulnerable to risk of loss or unauthorized use, including periodically counting the assets and comparing the results to control records. Our statistical tests of IT inventory controls excluded thousands of IT equipment items identified as missing at the four case study locations during VA's 2007 IT equipment inventory effort. Therefore, if adequate controls were in place at our test locations, we would not have expected to identify any additional missing items, blank data fields, or inaccurate inventory records. However, our statistical tests and data analysis at the four locations found significant control failures related to (1) missing items, (2) blank serial numbers, (3) inaccurate information on user organization, (4) inaccurate information on user location, and (5) other recordkeeping errors related to item description information (e.g., model number and manufacturer). Our statistical tests identified a total of 50 missing items, of which 34 could

---

<sup>14</sup>See Office of Management and Budget (OMB), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Memorandum (Washington, D.C.: May 22, 2007). This memorandum requires agencies to develop and implement an information breach notification policy.

<sup>15</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999). This document was prepared to fulfill our statutory requirement under 31 U.S.C. 3512 (c), (d), commonly known as the Federal Managers' Financial Integrity Act of 1982, to issue standards that provide the overall framework for establishing and maintaining internal control.

---

have stored sensitive information. As with missing items identified in VA's departmentwide physical inventory of IT equipment, because VA does not know what, if any, sensitive information resided on the equipment, notifications to potentially affected individuals could not be made. We estimate the percentage of inventory control failures related to these missing items to be 1 percent at the Puget Sound HCS, 3 percent at the Boston HCS, 6 percent at the North Texas HCS, and 12 percent for VA headquarters organizations.<sup>16</sup> Although these control weaknesses may be addressed through VA's early implementation of the July 2008 policies, the fact that we identified missing items only a few months after these locations had completed their physical inventories is an indication that the locations had not yet corrected underlying control weaknesses related to accountability over their IT equipment. We also found that medical equipment with data storage and processing capabilities was not included in VA's physical inventory of IT equipment.<sup>17</sup> The lack of user-level accountability and inaccurate records on status, location, and item descriptions found at our case study locations make it difficult to determine the extent to which actual theft, loss, or misappropriation of IT equipment may have occurred. Moreover, our follow-up work at the four case study locations found weaknesses in controls over hard drives in the property disposal process as well as physical security weaknesses at IT storage facilities. These control weaknesses present a risk that VA could lose control over new, used, and excess IT equipment and that any sensitive personal and medical information residing on hard drives in this equipment could be compromised.

This report contains five recommendations to VA on additional actions needed to strengthen the overall control environment and improve key internal control activities to help ensure accountability and safeguard IT equipment. In initially commenting on our draft report, VA stated that it generally agreed with all but one of our five recommendations. VA was concerned that our recommendation to develop a list of medical equipment with data storage capabilities that should be considered as IT equipment for inventory control purposes intended that this equipment should be redefined (i.e., reclassified) as IT equipment. In a follow-up meeting with VA officials, we clarified that our recommendation was

---

<sup>16</sup>Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 10 percent or less.

<sup>17</sup>We included medical equipment with the capability to store or process data in our tests; such items were excluded from the 2007 VA-wide physical inventory of IT equipment.

---

intended to provide the CIO visibility over this equipment for purposes of assuring accountability and information security. Following our discussion and clarifications, VA officials said they agreed with the intent of all five of our recommendations and noted actions they are taking to address them. VA's comments and our analysis are discussed in the Agency Comments and Our Evaluation section of this report. VA's comments are reprinted in appendix III.

---

## Background

VA's mission is to serve America's veterans and their families and to be their principal advocate in ensuring that they receive medical care, benefits, and social support in recognition of their service to our nation. VA, headquartered in Washington, D.C., is the second largest federal department and reported it had over 230,000 employees as of September 30, 2007, including physicians, nurses, counselors, statisticians, computer specialists, architects, and attorneys. VA has three major line organizations—VHA, VBA, and NCA—and field facilities throughout the United States. VHA has 21 Veterans Integrated Service Networks (VISN) that oversee medical center activities within their areas, which may cover one or more states. VA provides employees, contractors, volunteers, and students with a wide range of IT equipment,<sup>18</sup> including desktop and laptop computers, monitors and printers, personal digital assistants, unit-level workstations, local area networking equipment, and medical equipment with memory and data processing/communication capabilities. By the start of fiscal year 2008, VA had centralized its IT function at all locations within the realigned OIT.

---

## VA's IT Property Management Process

The Assistant Secretary for Information and Technology heads VA's OIT, serves as the CIO for the department, and is the principal advisor to the Secretary on matters relating to IT management in the department. OIT staff share responsibility for management of IT equipment inventory with property management personnel. Accordingly, it is crucial for the department's CIO to have the cooperation of property managers to ensure that well-established integrated processes exist for controlling IT inventory.

---

<sup>18</sup>For the purpose of this audit, we include in our definition of IT equipment any equipment capable of storing or processing data, regardless of how VA classifies it. Therefore, medical devices that would typically not be classified as IT equipment, but may capture, process, or store patient data, were considered IT equipment for this audit. For example, we included electrocardiograph, anesthesiology, and ultrasound equipment in our tests.

The steps in the IT property management process are key events, which should be documented by an inventory transaction, a financial transaction, or both, as appropriate. Federal records management law, as codified in Title 44 of the U.S. Code and implemented through National Archives and Records Administration (NARA) guidance, requires federal agencies to adequately document and maintain proper records of essential transactions and have effective controls for creating, maintaining, and using records of these transactions.<sup>19</sup> Table 1 provides an overview of VA's IT property management process.

**Table 1: Overview of Key Controls in VA's IT Property Management Process**

<b>Receipt, deployment, and inventory control of items in service</b>	
Document receipt of new IT equipment items and update financial and property records	Upon receipt of IT equipment, property management personnel record receipt and acceptance for financial reporting and payment. Property personnel also affix bar code labels and create property records <sup>a</sup> for new IT equipment by entering in the automated property systems serial number, description, model number, manufacturer, and original acquisition value, among other elements. Timely recording of new IT equipment in the central property records reduces the risk of misappropriation and lessens the opportunity for undetected loss or theft.
Deploy IT equipment and record user and location information	Upon deployment of new IT equipment or deployment of existing equipment for reuse, OIT personnel record the property location. OIT personnel also record organization and user information. Recording organization and user-level information creates an environment of accountability and helps ensure that individuals take responsibility for the IT equipment items assigned to them.
Perform physical inventory of IT equipment	VA personnel confirm IT equipment existence during annual physical inventories. Personnel use handheld scanners to capture IT item bar code information and to update location information which helps achieve segregation of duties. In addition, VA Handbook 7127/4 requires that all completed inventories have a 5 percent verification inventory conducted by an accountable officer or designee, a disinterested party, and the custodial officer or designee. Comparing those items physically identified to the inventory records presents an opportunity to identify missing items and to update inventory records for changes in user, location, and status, as appropriate.
Update property records	Once personnel have completed physical inventories they update the central property records to reflect current information. Missing items are reported to VA Police or security officers, as appropriate, and to a Board of Survey <sup>b</sup> for further investigation and write-off, if necessary. Updating information on a timely basis provides an organization with accurate information on the location, quantity, and status of its IT equipment for management accountability and decision making.

<sup>19</sup> 44 U.S.C. §§ 3101 and 3102, and implementing NARA regulations at 36 C.F.R. § 1222.38. This is consistent with the more general requirement for agencies to establish internal controls under 31 U.S.C. § 3512 (c), (d), commonly known as the Federal Managers' Financial Integrity Act of 1982 (FMFIA), and [GAO/AIMD-00-21.3.1](#).

---

---

**Turn-in, hard drive cleansing, and disposal of excess IT equipment**

---

Document turn-ins of excess IT equipment items	Once an IT item has been identified for turn-in or disposal, the user or OIT will complete VA Form 2237, "Request, Turn-In, and Receipt for Property or Services" or use an electronic turn-in process. Property management personnel are responsible for updating the status of the item in the inventory records. Accurate status information provides asset visibility over items that are in service (in use) and those that have been removed from service.
Secure and remove data from hard drives in the property disposal process	OIT personnel are responsible for the physical security of computer hard drives during the disposal process. Physical security of hard drives during the disposal process mitigates the risk of theft or loss or compromise of sensitive information. As part of the disposal process, OIT personnel either cleanse the hard drives using VA-approved software or ship the hard drives to a vendor for physical destruction. Recording hard drive serial numbers and the corresponding item bar code and serial numbers of the host computers creates an audit trail that can be used to determine the system from which a hard drive originated. Since hard drives have the capability to store sensitive information, control of computer hard drives during the property disposal process is essential to safeguarding personal information that may be stored on the hard drives. <sup>5</sup>
Redeploy or dispose excess IT equipment items and update inventory status	OIT personnel may redeploy IT equipment that is determined to be excess to the turn-in user's needs. Ultimately, VA will dispose of items excess to its needs by donating them to schools, transferring them to the General Services Administration for reuse within the federal government or resale, or transferring them to disposal (or scrap) vendors. Timely recording of turn-ins and disposal of excess IT equipment helps ensure that VA maintains accountability for IT equipment throughout its life cycle as well as the accuracy of its IT equipment inventory records.

---

Source: GAO analysis of VA policies and procedures.

<sup>a</sup>Medical center personnel use the Automated Equipment Management System/Medical Equipment Repair Service (AEMS/MERS) for new IT equipment acquisitions. AEMS/MERS is a general inventory management system that is local to each VA medical center. Headquarters personnel enter records of new IT equipment in the Inte-Great™ Property Manager system.

<sup>b</sup>VA Handbook 7125, *Materiel Management Procedures*, mandates that a Board of Survey be appointed when there is a possibility that a VA employee may be assessed a pecuniary (financial) liability or disciplinary action as a result of loss, damage, or destruction of property valued at \$5,000 or more. The Board of Survey reviews the Report of Survey, which identifies IT equipment that is unaccounted for and explains efforts to account for missing items. The Board of Survey approves final Reports of Survey, including write-offs of missing items and determines if disciplinary action is warranted.

<sup>c</sup>Federal agencies, such as VA, are required to protect sensitive data stored on their IT equipment against the risk of data breaches and thus the improper disclosure of personal identification information, such as names and social security numbers. Such information is regulated by privacy protections under the Privacy Act of 1974, codified, as amended, at 5 U.S.C. § 552a and, when information concerns an individual's health, the Health Insurance Portability and Accountability Act of 1996 (HIPAA). See Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (Aug. 21, 1996), and implementing regulations at 45 C.F.R. pt. 164.

---

## VA Has Made Significant Progress in Addressing GAO Recommendations and Completing a VA-Wide IT Equipment Inventory

VA has made significant progress in addressing our previous recommendations directed at improving policies and procedures for control of IT equipment and reducing the risk of disclosure of sensitive personal and medical information. As of the end of our field work in July 2008, VA had completed action on 10 of our 12 recommendations from our July 2007 report.<sup>20</sup> VA's Assistant Secretary for Management and the CIO worked together to draft a revised property management policy in a new VA Handbook 7002, *Logistics Management Procedures*, which addresses 7 of our 2007 recommendations. This revised policy is an important step in establishing a framework for control of IT equipment. On July 3, 2008, the Assistant Secretary for Management mandated early implementation of this policy, which includes requirements for user-level accountability, time frames for completing Reports of Survey on missing and stolen property, and requirements for strengthening physical security. VA also partially implemented action on one other recommendation and has actions under way to address the remaining recommendation from our 2007 report. Successful implementation of these efforts will be key to improving controls over VA's IT equipment. VA also made progress implementing recommendations from our 2004 report<sup>21</sup> related to personal property and equipment management. VA completed action on four of six property-related recommendations in our 2004 report and partially completed action on a fifth recommendation. VA has plans to address the remaining 2004 recommendation. In addition, in response to your concerns about VA-wide controls based on our previous audits, VA required departmentwide physical inventories of IT equipment to be completed by December 31, 2007. OIT monitored the 2007 physical inventory effort for IT equipment and reported that as of May 15, 2008, VA was unable to locate approximately 62,800 recorded IT equipment items, of which over 9,800 could have stored sensitive information. The CIO formed a "tiger team"<sup>22</sup> to monitor efforts under the Report of Survey<sup>23</sup> system and to help ensure that Reports of Survey are completed in a timely manner.

---

<sup>20</sup> [GAO-07-505](#).

<sup>21</sup> [GAO-04-755](#).

<sup>22</sup> A tiger team is a quick response team formed to determine causes of identified problems and develop corrective action plans.

<sup>23</sup> The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

---

## VA Has Made Significant Progress in Addressing GAO Recommendations

To address recommendations in our July 2007 report, VA completed action on 10 of our 12 recommendations, partially implemented actions on one other recommendation, and has actions under way to address the remaining recommendation. VA actions on our 2007 report recommendations included the establishment of specific time frames for finalizing Reports of Survey, granting OIT personnel access to the central property database, and holding employees financially liable for lost IT equipment. In addition, VA completed action on four of the six recommendations in our July 2004 report, partially completed action on a fifth recommendation, and has plans to address the remaining recommendation. For example, VA revised its policy through VA Handbook 7127/4, *Materiel Management Procedures*, to state that sensitive items include IT equipment and named several types of IT equipment items. VA's revised policy also stated that IT equipment items valued under \$5,000 are to be included in physical inventories. Further, VA has drafted policies that provide a framework for strengthening controls over IT equipment, including VA Handbook 7002, *Logistics Management Procedures*.<sup>24</sup> On July 3, 2008, VA's Assistant Secretary for Management mandated early implementation of this handbook. Effective implementation of this new policy will be essential to ensuring adequate control and accountability of VA's IT equipment and any sensitive information residing on that equipment. Table 2 provides a summary of our 2007 and 2004 recommendations and the current status of VA actions. For a more detailed explanation of VA's actions taken and planned on our recommendations, see appendix II.

---

<sup>24</sup>This policy combines information originally contained in VA Handbooks 7125, *General Procedures*, and 7127, *Materiel Management Procedures*, and would rescind these policies when approved in final form.



**Table 2: Status of VA's Actions on Prior Recommendations**

<b>2007 GAO recommendations</b>	<b>Status</b>
<b>VA-wide recommendations:</b>	
1. Revise VA property management policy and procedures to include detailed requirements for what transactions must be recorded to document inventory events and to clearly establish individual responsibility for recording all essential transactions in the property management process.	Fully implemented
2. Revise VA purchase card policy to require purchase card holders to notify property management officials of IT equipment and other property items acquired with government purchase cards at the time the items are received so that they can be recorded in property management systems.	Fully implemented
3. Establish procedures to require specific, individual user-level accountability for IT equipment. In implementing this recommendation, consideration should be given to making the unit head, or a designee, accountable for shared IT equipment.	Fully implemented
4. Enforce user-level accountability and IT coordinator responsibility by taking appropriate disciplinary action, including holding employees financially liable, as appropriate, for lost or missing IT equipment.	Fully implemented
5. Establish specific time frames for finalizing a Report of Survey once an inventory has been completed so that research on missing items is completed expeditiously and does not continue indefinitely without meeting formal reporting requirements.	Fully implemented
6. Establish a mechanism to monitor adherence by the San Diego and Houston medical centers and other VA organizations, as appropriate, to VA policy for performing annual inventories of sensitive items under \$5,000, including IT equipment.	Fully implemented
7. Require that information resource management and IT Services personnel at the various medical centers be given access to the central property database and be furnished with hand scanners so they can electronically update the property control records, as appropriate, during installation, repair, replacement, and relocation or disposal of IT equipment.	Partially implemented
8. Require physical security personnel to perform inspections of buildings and storage facilities to identify informal and undesignated IT storage locations so that security assessments are performed and corrective actions are implemented, where appropriate.	Fully implemented
<b>Recommendations for the CIO:</b>	
9. Establish a formal policy requiring a review of the results of annual inventories to ensure that IT equipment inventory records are properly updated and no blank fields remain.	Fully implemented
10. Establish a process for reviewing Reports of Survey for lost, missing, and stolen IT equipment items to identify systemic weaknesses for appropriate corrective action.	Open
11. Establish and implement a policy requiring information resource management personnel and IT coordinators to inform physical security officers of the site of all IT equipment storage locations so that these store rooms can be subjected to required inspections.	Fully implemented
12. Establish and implement a policy for reviewing the results of physical security inspections of IT equipment storerooms and ensure that needed corrective actions are completed.	Fully implemented
<b>2004 GAO recommendations related to personal property and equipment</b>	
<b>Status</b>	
1. Clarify existing guidance and establish consistent parameters for personal property that is required to be accounted for in the property control records and that is subject to physical inventory to include sensitive property.	Fully implemented
2. Provide a more comprehensive list of the type of personal property assets that are considered sensitive for accountability purposes.	Fully implemented
3. Direct that physical inventories of personal property be performed by the Acquisition and Materiel Management staff or other parties who are independent of those with property custodian responsibilities.	Partially implemented

4. Reinforce VA's requirement to attach bar code labels to agency personal property.	Fully implemented
5. At the six VA medical centers we visited, determine the location or disposition of personal property items not found during our site visits.	Fully implemented
6. At the six VA medical centers we visited, review property records to identify and correct erroneous or incomplete data fields.	Open

Source: GAO interviews of agency officials and analysis of VA documentation.

### VA's 2007 Physical Inventory Effort Demonstrated Continuing Problems with Controls over IT Equipment

VA's 2007 departmentwide inventory initially identified approximately 79,000 missing IT equipment items, underscoring the need to effectively implement the new policies and procedures mandated on July 3, 2008. In the 6 months following completion of the physical inventory, VA facilities undertook efforts to locate or determine reasons for missing items. VA was able to locate several thousand of the missing equipment items. However, as summarized in table 3, on May 15, 2008, OIT reported that VA was unable to locate approximately 62,800 recorded IT equipment items, of which over 9,800 could have stored sensitive information. Because VA does not know what, if any, sensitive information resided on the equipment and when the equipment was lost, notifications to potentially affected individuals could not be made in accordance with OMB guidance.<sup>25</sup> We interviewed VA officials and obtained documentation on the VA-wide inventory; however, we did not validate the results. According to VA, many of the missing items were old equipment and may have been disposed of through VA's excess property program. However, because VA facilities had not always documented IT equipment disposal for many years, there was no way to determine whether any of the missing items were lost or stolen. Further, during our work, we discovered that not all IT equipment items were included in the departmentwide inventory. Consequently, the numbers of missing items could be higher. For example, VA's 2007 physical inventory did not include medical equipment with data storage or processing capabilities. In addition, IT equipment items not accounted for in the OIT equipment inventory listing (EIL) were not subject to the 2007 physical inventory at some VA facilities. Further, limited completeness tests we performed as part of our data reliability procedures at case study locations identified some IT equipment items recorded to EILs for organizations other than OIT. Prior to the establishment of OIT, EILs were aligned organizationally and some IT equipment assigned to other EILs had not yet been reassigned to the OIT

<sup>25</sup>See OMB, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Memorandum (Washington, D.C: May 22, 2007). This memorandum requires agencies to develop and implement an information breach notification policy.

EIL and, therefore, were omitted from the 2007 physical inventory. We discussed our finding with OIT officials, and they told us that they had met in June 2008 to develop strategies for moving all IT equipment items assigned to other EILs to the OIT EIL.

**Table 3: Summary of VA-Wide Fiscal Year 2007 IT Equipment Physical Inventory Results as of May 15, 2008**

VA location	Total missing items	Open Reports of Survey items that could have stored sensitive data	Types of missing items on open Reports of Survey that could have stored sensitive data				
			Desktop computers	Main frame systems	Laptop computers	Personal digital assistants	Other
Region 1 (VISNs 18 – 22)	10,004	1,429	1,207	0	153	4	65
Region 2 (VISNs 12, 15- 17, and 23)	18,966	3,089	2,899	20	140	3	27
Region 3 (VISNs 6 – 11)	18,623	2,736	2,038	72	593	22	11
Region 4 (VISNs 1 – 5)	13,475	2,037	1,688	12	281	22	43
Veterans Benefits Administration	8	4	4	0	0	0	0
Field Program Offices	490	1	0	0	0	0	1
VA Headquarters Organizations	1,314	570	157	0	197	119	97
<b>Total</b>	<b>62,880</b>	<b>9,866</b>	<b>7,993</b>	<b>104</b>	<b>1,364</b>	<b>170</b>	<b>244</b>

Source: VA OIT data.

Notes: According to VA officials, the “main frame systems” category refers to mini computers (a largely obsolete term for a class of multi user, middle range computers). The “other” category includes thumb drives (small, lightweight, removable data storage devices) and servers.

VA officials also stated that the mathematical differences for Region 4 data may be due to minor reporting variations.

In compliance with VA Handbook 7125, *General Procedures*, VA personnel submitted Reports of Survey for IT equipment items that were not located during the departmentwide physical inventory and subsequent follow-up investigation. A CIO tiger team was responsible for monitoring the Report of Survey process and helping to ensure that it was completed in a timely manner. Local Boards of Survey were responsible for investigating missing items and approving write-offs of IT equipment items that could not be located during the departmentwide physical inventory. However, as of May 15, 2008, VA had over 43,000 items that were listed on open Reports of

---

Survey and facility personnel were continuing to search for missing items. The 2007 physical inventories were a massive undertaking and required significant effort over several months to resolve discrepancies. Although we would have expected the VA locations that we previously tested to have few, if any, missing items, as of May 15, 2008, 6 of the 12 locations reported from 1,269 to 6,427 missing IT items; 4 locations had from 115 to 863 missing IT items; and only 2 locations had fewer than 100 missing items. A summary of Reports of Survey data on missing IT equipment and the reported original acquisition cost identified in VA's 2007 physical inventory related to sites we tested in our 2004, 2007, and 2008 audits are presented in appendix IV.

---

## Tests of IT Inventory Controls at Case Study Locations Identified Continuing Weaknesses

Our tests of IT equipment inventory controls at four case study locations, including three VA HCS and VA headquarters, identified continuing control weaknesses related to missing items, lack of accountability, and errors in IT equipment inventory records. VA's 2007 departmentwide physical inventory effort was intended to establish a reliable IT equipment inventory baseline going forward. Accordingly, our tests excluded from the population of IT equipment thousands of items identified as missing during VA's 2007 IT physical inventory effort. Given the new baseline, if adequate controls had been in place by the end of this inventory process, we would not have expected to identify missing items, blank data fields, or inaccurate inventory records at our test locations. As previously noted, in July 2008 VA mandated early implementation of revised policy related to control of IT equipment. Although the early implementation of July 2008 policy changes may address IT equipment control weaknesses, this policy was not in effect at the time of our tests. Our *Standards for Internal Control in the Federal Government*<sup>26</sup> states that a positive control environment provides discipline and structure as well as the climate that influences the quality of internal control. Further, these standards require agencies to establish physical control to secure and safeguard vulnerable assets, such as equipment that might be vulnerable to risk of loss or unauthorized use, including periodically counting the assets and comparing the results to control records. However, our tests of IT equipment inventory controls at the four case study locations, including three VA HCS and VA headquarters, identified continuing problems with (1) inventory control and accountability, (2) control over computer hard drives in the excess property disposal process, and (3) physical security of

---

<sup>26</sup> [GAO/AIMD-00-21.3.1](#).

IT equipment storage locations. For example, our statistical tests at the four locations from February through May of 2008 identified significant numbers of missing items, several of which could have stored sensitive personal and medical information. Overall, our statistical tests and data analysis at the four locations found significant failures related to IT inventory control and accountability including (1) missing items, (2) blank serial numbers, (3) inaccurate information on user organization, (4) inaccurate information on user location, and (5) other recordkeeping errors. We also identified weaknesses in the controls over computer hard drives in the property disposal process at the four test locations, involving (1) lack of timely sanitization and disposal, (2) inadequate recordkeeping, and (3) physical security. In addition, we found physical security weaknesses at IT storage facilities at all four locations. These weaknesses increase the risk that sensitive personal and medical information could be compromised.

**GAO’s IT Inventory Control Tests Found Continuing Problems**

Our 2008 statistical tests of key IT equipment inventory controls and data analysis found significant inventory control failures related to (1) missing items, (2) blank serial numbers, (3) inaccurate information on user organization, (4) inaccurate information on user location, and (5) other recordkeeping errors. As noted previously, VA performed a 2007 physical inventory of IT equipment. We excluded from our populations the missing items identified during VA’s physical inventory at the four case study locations. Table 4 shows the 2007 VA-wide inventory results related to missing items at our four case study locations.

**Table 4: Numbers of Missing IT Equipment Items at Four Test Locations That Were Identified during the 2007 VA-Wide IT Physical Inventory**

<b>Inventory results</b>	<b>North Texas HCS</b>	<b>Puget Sound HCS</b>	<b>Boston HCS</b>	<b>VA headquarters</b>
Date of VA inventory <sup>a</sup>	December 2007	December 2007	December 2007	January 2008
Missing items as of December 31, 2007	5,309	1,383	3,663	1,595
Missing items located as of May 15, 2008	1	114	437	281
Missing items not located as of May 15, 2008	5,308	1,269	3,226	1,314

<b>Inventory results</b>	<b>North Texas HCS</b>	<b>Puget Sound HCS</b>	<b>Boston HCS</b>	<b>VA headquarters</b>
Missing items as of May 15, 2008, that could have stored sensitive information	3,351	443	725	608

Source: GAO analysis of VA 2007 inventory results at four case study locations.

<sup>a</sup>The dates of the VA inventories are completion dates.

Given our exclusions of missing items from the VA inventories, if adequate controls had been in place by the end of this inventory process, we would not have expected to identify missing items, blank data fields, or inaccurate inventory records at our test locations. Table 5 shows the results of our statistical tests at the four case study locations. We present our results as point estimates of control failure rates. Each point estimate has a margin of error, based on a two-sided, 95 percent confidence interval, of plus or minus 10 percent or less.

**Table 5: Estimated IT Equipment Inventory Control Failure Rates at Four Test Locations**

<b>Control failures</b>	<b>North Texas HCS</b>	<b>Boston HCS</b>	<b>Puget Sound HCS</b>	<b>VA headquarters</b>
Missing items in sample	6%	3%	1%	12%
Blank serial numbers (actual)	59%	17%	1%	1%
Incorrect user organization	91%	60%	76%	12%
Incorrect user location	46%	17%	14%	33%
Recordkeeping errors	9%	41%	9%	4%

Source: GAO analysis of statistical test results.

Notes: The blank serial number failure rate represents the actual blank data field in the population of recorded IT equipment items in each location's property system.

Each of the other estimates is based on our statistical tests, which have a margin of error based on a two-sided, 95 percent confidence interval of +/- 10 percent or less. The details of our statistical testing are explained in appendix I. Because the four test locations did not record all IT equipment items in their inventory records, our estimated failure rates relate to current (recorded) inventory in the OIT EIL and not the population of all IT equipment at those locations.

Serial number control is essential to accountability for sensitive items, such as IT equipment, because it identifies unique items. The property bar code label alone is not a sufficient identifier for sensitive items because these labels are removable and can be replaced, if lost or damaged. In addition, because VA has not yet put in place a control for user-level

---

accountability, accurate information on user organization and user location is key to maintaining accountability for IT equipment items. Further, recordkeeping errors impair the reliability of IT inventory information for management decision making. For example, inaccurate inventory records on item name, model number, and manufacturer impair asset visibility and affect decision making on timing of IT equipment upgrades.

As discussed previously, limited completeness testing performed as part of our data reliability procedures identified IT equipment that was not included in the populations of recorded IT equipment used for our control tests. For example, our completeness tests at two of the four locations we tested identified three IT equipment items that were recorded to EILs for Psychology, Radiology, and Acquisition and Material Management rather than the OIT EIL. Our completeness tests also identified one item not recorded to an EIL. VA officials could not tell us the quantity of IT equipment items that were not included in the four case study IT equipment populations from which we selected our samples for testing.

GAO Tests Identified  
Significant Numbers of Missing  
IT Equipment Items

Our tests of physical inventory controls from February through May of 2008 identified 50 missing IT equipment items, including 9 medical equipment items. Of the 50 missing items, 34 items could have stored sensitive personal and medical information. Because VA does not know what, if any, sensitive information resided on the equipment, notifications to potentially affected individuals could not be made. Following the recent completion of VA inventories of IT equipment and adjustment of inventory records at the four test locations, we would not have expected to identify any additional missing items. The continuing occurrences of missing items indicate that underlying control weaknesses have not yet been corrected. Lost and missing IT equipment pose both a financial risk as well as a security risk associated with sensitive information maintained on computer hard drives. The scope of our IT equipment inventory tests was broader than VA's IT inventory because we included medical items with data storage capability. Medical equipment with data storage capability is not currently included in VA's definition of IT equipment. VA CIO officials told us they are aware of the need to control medical equipment with data storage capability and plan to address control of IT components of this equipment. The following discussion summarizes the results of our inventory control tests at the four case study locations.

- **North Texas HCS.** As noted in table 5, our physical inventory testing of the North Texas HCS—which covered the Dallas VA Medical Center and Fort Worth Outpatient Clinic components—found high control failure

---

rates for all of our inventory control tests. Our existence test identified seven missing items, including two that had the capability to store sensitive information. One of the missing items was a piece of medical equipment. As noted in table 5, we estimated a 6 percent failure rate related to the missing items in the recorded population of 12,172 IT equipment items from which we selected our sample. In addition, our analysis of the population of recorded IT equipment found that 7,164, or about 59 percent, did not have their serial numbers recorded in the physical inventory records. Serial numbers are essential to proper identification of sensitive computer equipment.

- **Boston HCS.** Our physical inventory testing of the Boston HCS—which covered the Brockton, Jamaica Plain, and West Roxbury Campuses—identified 10 missing items, including 7 that had the capability to store sensitive information. The 7 missing items included four medical analyzers, two microcomputers, and a radiology equipment item. As noted in table 5, we estimated a 3 percent failure rate related to the missing items in the recorded population of 15,706 IT equipment items from which we selected our sample.
- **Puget Sound HCS.** The Puget Sound HCS had an estimated failure rate of 1 percent related to missing items in the recorded population of 11,474 IT equipment items, allowing us to conclude that the HCS's controls over existence of IT equipment inventory are effective. Further, the one item we determined to be missing related to a computer monitor which did not have the capability to store data. However, the Puget Sound HCS had high failure rates for the user information and recordkeeping tests.
- **VA Headquarters Organizations.** Our physical inventory testing of VA headquarters organizations IT equipment items identified an estimated failure rate of 12 percent related to missing items in the recorded population of 34,735 items. Our population included strata for VHA, VBA, OIT, Acquisition and Materiel Management, General Counsel, Policy and Planning, and a seventh strata with all other headquarters organizations. Table 6 identifies missing IT equipment items in our stratified sample by VA headquarters organization.



**Table 6: Number of Missing IT Equipment Items by Headquarters Organization and Missing Items That Could Have Stored Sensitive Personal Data**

Test location	Number of missing IT items in stratified sample	Missing items with data storage capability
Acquisition and Material Management	0 of 10	0
General Counsel	0 of 10	0
Information and Technology	21 of 96	17 of 21
Policy and Planning	0 of 10	0
Veterans Health Administration	6 of 95	5 of 6
Veterans Benefits Administration	2 of 94	1 of 2
All other <sup>a</sup>	3 of 34	2 of 3

Source: GAO analysis of statistical test results.

<sup>a</sup>All other includes 13 additional VA headquarters organizations. The missing items are from the Construction & Facilities Management Office, the Human Resource Management Office, and the Resolution Management Office. The missing items with data storage capability are from the Human Resource Management Office and the Resolution Management Office.

**Lack of User-Level Accountability for IT Equipment at Case Study Locations**

As was the case with our 2007 audit of VA IT equipment inventory controls, we found a lack of user-level accountability at the four case study locations in our current tests. As shown in table 7, VA has not yet assured accurate IT inventory records with regard to user organization and location. Information on organization and location are key to maintaining visibility and accountability for IT equipment items. VA property management policy<sup>27</sup> and VA Handbook 7002 include guidelines for holding employees and supervisors pecuniarily (financially) liable for loss, damage, or destruction because of negligence or misuse of government property. Several VA facilities have provided us with current examples where VA employees have been held liable for lost and missing IT equipment. Since the completion of our tests, VA has mandated early implementation of Handbook 7002 which also requires assignment of user-level accountability for most IT equipment items. To be effective, the new policy will need to be adequately implemented and enforced.

<sup>27</sup>VA Handbook 7125, *Material Management General Procedures*, § 5003 (Oct. 11, 2005).

**Table 7: Estimated IT Inventory Control Failure Rates Related to Correct User and Location at the Four Test Locations**

Test location	Incorrect user organization	Incorrect user location
North Texas HCS	91% (85% to 95%)	46% (36% to 56%)
Boston HCS	60% (50% to 70%)	17% (10% to 25%)
Puget Sound HCS	76% (66% to 84%)	14% (8% to 22%)
VA headquarters organizations	12% (8% to 17%)	33% (26% to 40%)

Source: GAO analysis of statistical test results.

Note: The percentages represent point estimates and the two-sided, 95 percent confidence intervals.

The following discussion summarizes the results of our tests for user-level accountability.

- North Texas HCS.** The North Texas HCS components we tested had very high failure rates related to accountability—an estimated 91 percent for correct user organization and an estimated 46 percent for correct user location. North Texas HCS staff provided us with evidence of sign-out sheets and hand receipts for some IT equipment items such as pagers, cellular telephones, and personal digital assistants. However, for a majority of IT equipment items, the North Texas HCS did not assign user-level accountability through hand receipts or record user information in the inventory system. For medical IT equipment items, the inventory system included user organizations (e.g., radiology or anesthesiology), but did not assign the items to unit heads.
- Boston HCS.** The Boston HCS campuses we tested also had high failure rates related to accountability—an estimated 60 percent for correct user organization and an estimated 17 percent for correct user location. At our exit briefing in May 2008, Boston HCS staff reported that they are working with engineering personnel to better identify physical locations to aid in the tracking of mobile IT equipment items. For traditional IT equipment items, the Boston HCS generally did not record user organization in its IT equipment inventory records. Further, the Boston HCS generally did not assign user-level accountability through recorded user information or hand-receipts with the exception of pagers, cell phones, and laptops that have been assigned to specific users. For medical IT equipment items, the inventory system included user organizations (e.g., radiology or

---

anesthesiology). However, the inventory records for some of the equipment listed the user as “Medical” or “Nursing” and did not specify what unit in the hospital was accountable for the equipment.

- **Puget Sound HCS.** The Puget Sound HCS components we tested also had high failure rates related to accountability—an estimated 76 percent for correct user organization and an estimated 14 percent for correct user location. The Puget Sound HCS staff provided us with evidence of a locally developed supplemental application for AEMS/MERS, known as the Equipment Loan Form (ELF). Puget Sound HCS staff use the ELF to record user-level information for mobile IT equipment items (e.g., laptop computers) or IT equipment items taken off-site (e.g., a desktop computer at an employee’s home). However, for traditional IT equipment items (e.g., desktop computers, printers, and monitors at HCS facilities), the HCS did not assign user-level accountability with recorded user information or hand-receipts. For traditional IT equipment items, the inventory records generally did not identify the user organizations. For medical IT equipment items, the inventory system included user organizations (e.g., radiology or anesthesiology), but did not assign accountability for shared items to unit heads.
- **VA Headquarters Organizations.** Our statistical tests for accurate user organization information identified an estimated 12 percent error rate for VA headquarters organizations. In addition, our statistical tests for correct user information identified an estimated 52 percent error rate. Our tests included IT equipment coordinators—who are responsible for control of equipment shared by multiple users—and individual user employees. In situations where equipment, such as a printer, was shared by multiple employees, we based our tests on whether the inventory records correctly listed the equipment coordinator. In other situations where equipment was in possession and use by an individual employee, we tested to see if that employee was listed in the property record. Overall, we found 147 errors out of a sample of 349 records tested. Regarding user location, our statistical tests found an estimated 33 percent error rate related to situations where inventory records were not updated to reflect the transfer or relocation of IT equipment.

We also identified inconsistencies in the use of hand receipts for assigning user-level accountability of mobile IT equipment that can be removed from VA offices for use by employees who are on travel or are working at home. For example, we requested hand receipts for 38 mobile IT equipment items in our statistical sample that were being used by VA headquarters employees. These items either could be or were taken off-site. We received

Recordkeeping Errors in IT Equipment Inventory Status and Item Description Information

20 hand receipts—4 that were dated after the date of our request and 16 that were valid. We did not receive hand receipts for the other 18 devices.

As shown in table 8, we found some problems with the accuracy of IT equipment inventory records, ranging from an estimated 4 percent at VA headquarters to an estimated 41 percent at the Boston HCS. Recordkeeping errors included inaccurate information on the status (in use, turned-in, disposal), serial numbers, and item descriptions. Although the estimated overall failure rates for these tests were lower than the failure rates for the other control attributes we tested, they were significant for the various recordkeeping attributes we tested at the four locations.

**Table 8: Estimated Percentages of Other IT Inventory Recordkeeping Failures at Four Test Locations**

Test location	Inventory status	Serial number	Item description	Total recordkeeping failures
North Texas HCS	2% (0% to 7%)	1% (0% to 6%)	6% (3% to 12%)	9% (5% to 16%)
Boston HCS	8% (4% to 16%)	15% (8% to 24%)	26% (17% to 36%)	41% (32% to 51%)
Puget Sound HCS	1% (0% to 6%)	3% (1% to 9%)	5% (2% to 12%)	9% (4% to 16%)
VA headquarters organizations	0% (0% to 2%)	1% (0% to 3%)	3% (1% to 7%)	4% (1% to 7%)

Source: GAO analysis of statistical test results.

Notes: The percentages represent point estimates and the two-sided, 95 percent confidence intervals.

Inventory status includes items in use, turned-in, and disposed. The item description includes name, model number, and manufacturer.

Accurate IT equipment inventory records are important to management decision making because these records are used to determine the types, quantities, and age of equipment as well as life cycle and replacement time frames. Inaccurate information on the status of items—in service, sent for repair, turned in for disposal—masks visibility of items that are not available for use and may need to be replaced. Serial number errors, such as typographical errors, can impair accountability. Further, inaccurate inventory information can cause significant waste and inefficiency during

---

physical inventories because it may require additional time to locate and verify the status of the items.

Our review of the data submissions from all four test locations we visited identified data consistency and standardization issues with recorded names, models, and manufacturers of IT equipment. As a result, management at facilities we tested could not tell how many items of a certain model they had in service. Because property system data fields for item description are free-form and do not provide for data standardization, accurate data entry is critical to the identification of like items. For example, North Texas HCS inventory data showed one Solar 8000 physiological monitor listed as model “soalr 8000,” one listed as “Solar 800,” 26 listed as “Solar 8000,” and 70 listed as “Solar8000.” Although some of these differences appear to be typographical errors, when searching for Solar 8000 equipment in the database, there is no assurance that other variations of the item name would appear in the search results. Further, this situation hindered the North Texas HCS staff’s identification of medical IT equipment items that store or process patient data, requiring us to select a second sample and make an additional site visit. At the Boston HCS, we found that Samsung monitor model number 150N was referred to inconsistently as a “Monitor” 4 times, “Neoware” 3 times, “Samsung 15 Inch” 33 times, and a “Samsung Monitor” 58 times. VA’s policy does not address data consistency and standardization. Our *Internal Control Management and Evaluation Tool*<sup>28</sup> states that an agency should

- establish a variety of control activities suited to information processing systems to ensure accuracy and completeness,
- consider whether edit checks are used in controlling data entry, and
- consider accuracy control in relation to data entry design features.

Although this tool is not required to be used, it is intended to provide a systematic, organized, and structured approach for federal agency use in assessing internal control structure. The failure to maintain consistent information on identical items or classes of items impairs visibility over IT

---

<sup>28</sup>GAO, *Internal Control Management and Evaluation Tool*, [GAO-01-1008G](#) (Washington, D.C.: August 2001). This document was prepared to assist agencies in maintaining or implementing effective internal control and, when needed, to help determine what, where, and how improvements can be implemented.

---

assets as well as analysis and management decision making on existing IT equipment and replacements.

---

## Weaknesses in Controls over Hard Drives in the Disposal Process

Although VA requires that hard drives of IT equipment and medical equipment be sanitized prior to disposal to prevent unauthorized release of sensitive personal and medical information, we found weaknesses in the disposal process at each of our test locations that pose a risk that sensitive personal and medical information could be compromised.<sup>29</sup> Specifically, we found weaknesses related to (1) timeliness of data sanitization, (2) adequacy of inventory recordkeeping for hard drives removed from their host computers, and (3) physical security controls. Currently, VA OIT personnel are not cleansing all hard drives in the property disposal process because of the guidance from VA's Office of General Counsel to preserve electronic information relevant to a class action lawsuit filed against VA in 2007 (the litigation hold),<sup>30</sup> which heightens the need to maintain control over the hard drives in the property disposal process. However, two case study locations had not performed timely sanitization and disposal of hard drives prior to the effective date of the litigation hold. Specifically, one of our HCS test locations had stored excess hard drives for 3 to 4 years and another HCS test location indicated some of its excess hard drives dated back to the 1980s. Two HCS locations did not record dates that all hard drives were received. VA headquarters organizations did not keep records on hard drives in the disposal process prior to February 2008. In addition, adequate control over computer hard drives in the property disposal process requires accurate and complete recordkeeping, such as recording the hard drive serial number along with property identification and serial numbers of the original host computer. The ability to identify hard drives with the host computer inventory records also provides a means to determine the type of data that may have been stored on the hard drives. However, two of our four test locations did not record sufficient information to identify hard drives with host computers, and VA did not have a standard procedure to address this

---

<sup>29</sup>VA OIT personnel and contractors follow National Institute of Standards and Technology Special Publication 800-88 guidelines, which require performing three separate erasures for media sanitization.

<sup>30</sup>On August 21, 2007, VA distributed a "litigation hold" memorandum that explained issues in *Veterans for Common Sense v. Peake*, a class action lawsuit filed in July 2007 against VA, and VA's ongoing obligation to identify and preserve electronic information relevant to those issues. VA directed employees not to preserve all information, only information relevant to the lawsuit.

---

issue. Moreover, although storage locations used for excess hard drives are subject to access controls in VA Handbook 0730/1, *Security and Law Enforcement*, including motion detection intrusion alarm systems and special key (access) controls, three of our four case study locations did not comply with these requirements. Weaknesses in the controls over hard drives in the property disposal process create an unnecessary risk that sensitive personal information protected under the Privacy Act of 1974<sup>31</sup> and health information accorded additional protections under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)<sup>32</sup> could be compromised. The following discussion summarizes our findings at the four case study locations.

- **North Texas HCS.** We found that the North Texas HCS had weaknesses in controls over hard drives in the property disposal process related to timely sanitization, inadequate recordkeeping, and lack of access controls. According to North Texas HCS staff, they were not sanitizing data from any hard drives in the property disposal process at the time of our site visit because of the litigation hold related to the class action lawsuit. The North Texas HCS also indicated that not all hard drives received for sanitization and disposal had been logged in their tracking system. However, for those drives that were recorded, we found that the hard drive disposal records contained sufficient information for identifying hard drives with their original host computers. In addition, the disposal records contained the dates on which the hard drives were removed from their original host computers. The North Texas HCS also maintained a file on certifications of drives that had been cleansed. Further, we observed that one of the two storage locations storing hard drives had inadequate physical security because of the absence of an access control system and intrusion detection alarm system, as required by VA Handbook 0730/1.
- **Boston HCS.** Our work identified recordkeeping weaknesses in the hard drive disposal process at the Boston HCS. Specifically, we found that the hard drive disposal records did not contain sufficient information for identifying hard drives with their original host computers. Further, these records did not indicate the dates on which OIT personnel removed hard drives from their original host computers, which would impede an assessment of timely sanitization or disposal. The Boston HCS also had a

---

<sup>31</sup>Privacy Act of 1974, *codified, as amended*, at 5 U.S.C. § 552a.

<sup>32</sup>HIPAA, Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (Aug. 21, 1996). The HHS Secretary has prescribed standards for safeguarding health information in the HIPAA Medical Privacy Rule. *See* 45 C.F.R. pt. 164.

---

practice of storing used hard drives in unsecured locations, such as closets and cabinets, and indicated that it had hard drives dating back to the 1980's. The Boston HCS Information Security Officer is in the process of establishing a centralized storage facility for computer hard drives.

- **Puget Sound HCS.** We identified control weaknesses in the hard drive disposal process at the Puget Sound HCS related to a lack of timely sanitization and disposal and inadequate recordkeeping. Although Puget Sound HCS officials are holding drives because of the litigation hold related to the class action lawsuit, they told us that approximately 100 of the hard drives we observed had been in storage for approximately 3 or 4 years, and therefore are not related to the litigation hold. In addition, the hard drive disposal records at the Puget Sound HCS did not contain sufficient information for identifying hard drives with their original host computers. After our site visit, Puget Sound HCS staff provided us with revised hard drive records that include property identification numbers and hard drive serial numbers and identify hard drives with their original host computers. The Puget Sound HCS stored hard drives in a location that was in full compliance with physical security requirements in VA Handbook 0730/1.
- **VA Headquarters Organizations.** Weaknesses we identified in controls involved the lack of recordkeeping prior to February 2008 and the lack of access controls of hard drive storage facilities. We found that the current hard drive disposal records at VA headquarters contain sufficient information for identifying hard drives with their original host computers. Specifically, OIT records hard drive information in a log that requires, among other elements, the bar code and serial numbers of the original host computer from which OIT personnel removed the hard drive and the serial number of the hard drive. OIT also records the dates on which hard drives are removed from original host computers. However, according to OIT officials and our review of the hard drive records, VA headquarters did not maintain a central record of hard drives prior to February 2008. Further, one of the two hard drive storage locations that we observed at VA headquarters had inadequate physical security because of the absence of an access control system and intrusion detection alarm system, as required by VA Handbook 0730/1.

---

Physical Security Weaknesses Increase Risk of Loss, Theft, and Misappropriation

VA Handbook 0730/1, *Security and Law Enforcement*, prescribes physical security requirements for storage of new and used IT equipment. Specifically, the handbook requires warehouse-type storerooms to have walls to ceiling height with either masonry or gypsum wall board reaching the underside of the slab (floor) above. OIT storerooms are required to



---

have overhead barricades that prevent “up and over” access from adjacent rooms. Warehouse, OIT, and medical equipment storerooms are all required to have motion intrusion detection alarm systems that detect entry and broadcast an alarm of sufficient volume to cause an illegal entrant to abandon a burglary attempt. Finally, OIT storerooms also are required to have special key control, meaning room door lock keys and day lock combinations that are not master keyed for use by others.

Our investigator’s inspection of physical security at officially designated IT warehouses and storerooms that held new and used IT equipment at the four case study locations found that most of these storage facilities met the requirements in VA Handbook 0730/1. However, we identified some deficiencies. For example, our investigator found at least one room at all four case study locations that did not have an electronic access control system or an intrusion detection system. Designated IT equipment storage locations at the Seattle Division of the Puget Sound HCS met the physical security requirements in VA Handbook 0730/1. However, IT workrooms and other informal, undesignated storage facilities did not.

Despite the established physical security requirements, we found numerous informal, undesignated IT equipment storage locations that did not meet VA physical security requirements. For example, we observed an excess property storage room at the North Texas HCS that contained boxes of 86 hard drives that needed to be disposed of or sanitized. This room lacked a motion detection alarm system and the type of locking system prescribed in VA policy. North Texas HCS staff believed this room was not subject to the security provisions of VA Handbook 0730/1 because it was not formally designated as a storeroom or warehouse. Our investigator also identified an IT equipment work room at the North Texas HCS that lacked adequate physical security measures and was considered temporary in nature. In addition, at the Boston HCS, our investigator found that security personnel were unaware of several temporary storage rooms that contained IT equipment. Some of these rooms were initially established by OIT personnel as temporary storage areas, but had been in use for several years. Because these storerooms had not been formally designated as IT storage facilities, they were not subjected to required physical security inspections. Weaknesses in physical security heighten the risk that sensitive information contained on IT equipment stored in unsecured warehouses and storerooms could be compromised.

---

## Conclusions

Our audits and VA’s departmentwide physical inventory of IT equipment identified pervasive control weaknesses that resulted in tens of thousands

---

of missing IT equipment items that were purchased with taxpayer dollars. About 9,800 of these items have data storage capabilities and therefore pose a risk of improper disclosure of veterans' personal and medical information. Further, VA's lack of user-level accountability and its failure to maintain accurate and complete IT inventory records have hindered efforts to locate missing items. In the past year, VA has made significant progress in implementing its realigned OIT organization and strengthening policies for control over IT equipment. However, ensuring that IT inventory records are complete and that they are updated as changes in status occur will be key to maintaining accuracy and accountability over IT equipment items. VA's continued efforts to establish and maintain control over IT assets will be essential if VA is to adequately safeguard those assets from theft, loss, and misappropriation and protect sensitive personal and medical information of the nation's veterans.

---

## Recommendations for Executive Action

We recommend that the Secretary of Veterans Affairs require the CIO, with the support of medical centers and VA headquarters organizations we tested and other VA organizations, as appropriate, to take the following five actions to improve accountability of IT equipment inventory and reduce the risk of disclosure or compromise of sensitive personal and medical information:

- Review property inventory records and confirm that all IT equipment, regardless of the organizational equipment inventory listing, is identified in the property system.
- Establish and implement a policy requiring development of standardized naming classifications for IT equipment—including item name, manufacturer, and model—for recording IT equipment into local property inventory systems.
- Develop a list of medical equipment with data storage capability that should be considered as IT equipment for inventory control purposes.
- Develop a procedure for identifying hard drive serial numbers with both the property identification numbers and serial numbers of host computers.
- Revise the definition of IT storage locations in VA's Handbook 0730/1, *Security and Law Enforcement*, to include informal IT storage locations, such as OIT work rooms, and require these locations to be included in physical security inspections.

---

---

## Agency Comments and Our Evaluation

In its July 28, 2008, written comments on our report, which are reprinted in appendix III, VA generally agreed with four of our five recommendations. VA initially disagreed with our recommendation concerning inventory control over medical equipment because it interpreted our recommendation as requiring them to redefine (i.e., reclassify) medical equipment with data storage capability as IT equipment. Instead, our recommendation was directed at developing a list of medical equipment with data storage capability and including this equipment in physical inventories of IT equipment to provide for CIO oversight of these items. We followed up with VA officials to clarify the intent of our recommendation. We also made appropriate changes to our report to clarify the intent of our recommendation.

In addition, while agreeing with the intent of our recommendation concerning the development of standard naming classifications for its IT equipment, VA initially commented that it differed with part of our recommendation concerning who should be responsible for the development of standardized naming classifications. However, VA's comments indicate that it interpreted this recommendation as requiring classification action to occur on a decentralized basis at each VA facility. This was not our intent. In follow-up discussions with VA officials, we explained that our recommendation was directed at taking action to establish VA-wide naming conventions that would be used by all VA facilities in recording property information in their local inventory systems. We clarified the wording in our recommendation accordingly.

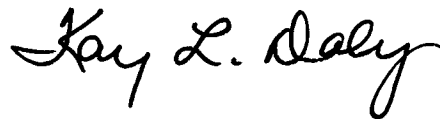
Based on our follow-up meeting, VA officials said they agreed with all five of our recommendations. They reiterated actions noted in VA's comment letter on steps taken as well as planned actions to improve the accuracy and consistency of information in VA's property inventory systems.

---

We are sending copies of this report to interested congressional committees; the Secretary of Veterans Affairs; the Veterans Affairs Chief Information Officer; the Under Secretary of Health, Veterans Health Administration; and the Director of the Office of Management and Budget. We will make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

---

Please contact me at (202) 512-9095 or [dalykl@gao.gov](mailto:dalykl@gao.gov), if you or your staff have any questions concerning this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report are acknowledged in appendix V.

A handwritten signature in black ink that reads "Kay L. Daly". The signature is written in a cursive, flowing style.

Kay L. Daly  
Acting Director  
Financial Management and Assurance

---

# Appendix I: Objectives, Scope, and Methodology

---

Given the continuing nature of information technology (IT) equipment inventory control problems and their significance, the Chairman and Ranking Member of the House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations asked us to perform additional follow-up work to determine (1) whether the Department of Veterans Affairs (VA) has made progress in implementing our prior recommendations for improving internal control over IT equipment and (2) the effectiveness of VA's current internal controls to prevent theft, loss, or misappropriation of IT equipment.

We evaluated VA's progress in implementing our previously reported recommendations by reviewing agency documentation and interviewing property management and Office of Information Technology (OIT) officials on actions taken in response to recommendations in our 2007 and 2004 reports.<sup>1</sup> In concert with the Subcommittee request that VA perform a departmentwide physical inventory of IT assets, we reviewed the results of VA's 2007 physical inventory of IT equipment items and VA's process for completing Reports of Survey<sup>2</sup> on lost and stolen items. We also evaluated policies that include guidance for improving accountability of IT equipment and accuracy of inventory records, related memorandums, and other documentation, such as action summaries. In addition, we interviewed cognizant VA officials about specific actions under way or completed, the component organizations responsible for those actions, and the status and targeted completion dates of those actions.

Our assessment of the effectiveness of current VA IT equipment inventory controls included statistical tests of key control attributes at four case study locations, including the health care systems (HCS) in North Texas, Boston, and Puget Sound, and VA headquarters organizations. We also assessed controls over hard drives in the excess property disposal process, and our investigators made physical security inspections of IT storage locations at our four case study locations.

---

<sup>1</sup>GAO, *Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*, [GAO-07-505](#) (Washington, D.C.: July 16, 2007) and GAO, *VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement*, [GAO-04-755](#) (Washington, D.C.: July 21, 2004).

<sup>2</sup>The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

---

We used as our criteria applicable law and VA policy, as well as our *Standards for Internal Control in the Federal Government*<sup>3</sup> and our *Internal Control Management and Evaluation Tool*.<sup>4</sup> We reviewed applicable program guidance provided by the test locations and interviewed officials about their IT inventory processes and controls.

In selecting our case study locations, we chose three geographically disparate VA HCS. We also tested inventory at VA headquarters organizations as a means of assessing the overall control environment, or “tone at the top,” as we did in our 2007 audit. Table 9 shows the VA locations selected for IT equipment inventory control testing, the sample size, and the reported number and value of IT equipment items at each location.

**Table 9: Population of VA IT Equipment at Locations Selected for Testing**

VA location	Sample size and number of VA IT equipment items	Value of VA IT equipment inventory
North Texas HCS	167 of 12,172	\$49,097,365
Boston HCS	148 of 15,706	48,972,306
Puget Sound HCS	147 of 11,474	33,969,881
VA headquarters	349 of 34,735	48,996,332

Source: GAO analysis of VA facility IT equipment inventory data.

Note: The data represent current inventory at the time we selected our samples. The reported value is the original acquisition cost, though not all items in VA’s property management systems included original acquisition values.

We performed appropriate data reliability procedures, including an assessment of each VA test location’s procedures for assuring data reliability, reasonableness checks on electronic data, and tests to assure

---

<sup>3</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999). This document was prepared to fulfill our statutory requirement under 31 U.S.C. 3512 (c), (d), commonly known as the Federal Managers’ Financial Integrity Act of 1982, to issue standards that provide the overall framework for establishing and maintaining internal control.

<sup>4</sup>GAO, *Internal Control Management and Evaluation Tool*, [GAO-01-1008G](#) (Washington, D.C.: August 2001). This document was prepared to assist agencies in maintaining or implementing effective internal control and, when needed, to help determine what, where, and how improvements can be implemented. Although this tool is not required to be used, it is intended to provide a systematic, organized, and structured approach to assessing the internal control structure.

that IT equipment inventory was sufficiently complete for the purposes of our work. As in our 2007 work, we relied on biomedical engineers to provide lists of medical equipment with the ability to store or process electronic data. We performed analytical procedures to confirm reasonableness of the medical equipment listings provided by the three HCS. Our analysis determined that the original listing submitted by the North Texas HCS staff was incomplete regarding medical equipment meeting our definition as IT equipment. We revisited our criteria for identifying medical equipment with data storage and processing capability with North Texas HCS officials and asked them to provide us a new medical equipment listing to support our sampling and control tests. Our procedures and test work also identified a limitation related to the completeness of IT equipment inventory at our four test locations. The VA North Texas and Boston HCS maintained some IT equipment records outside of their central listings of IT equipment. We also identified evidence that the VA Puget Sound and VA headquarters did not record all IT equipment items in the official property records. Further, our statistical tests determined that some IT equipment was recorded in inventory categories other than IT. We disclosed this limitation in the discussion of our test results. As a result of these limitations, the population of IT equipment is not known for VA overall or by location and we were not able to project our test results to the population of IT equipment inventory at each of our four test locations. However, we determined that these data were sufficiently reliable for us to project our test results to the population of current, recorded IT equipment inventory at each of the four locations.

From the population of current, recorded IT equipment inventory at the time of our tests,<sup>5</sup> we selected stratified random probability samples of IT equipment, including medical equipment with data storage capability, at each of the three HCS locations. For the 19 VA headquarters organizations, we stratified our sample by 6 major offices and used a seventh stratum for the remaining 13 organizations. With these statistically valid samples, each item in the population for the four case study locations had a nonzero probability of being included, and that probability could be computed for any item. Each sample item for a test location was subsequently weighted in our analysis to account statistically for all items in the population for that location, including those that were not selected.

---

<sup>5</sup>The population of IT equipment from which we selected our samples excluded IT equipment items identified as missing at the time of each of our tests.

We performed tests on statistical samples of IT equipment inventory transactions at each of the four case study locations to assess whether the system of internal control over physical IT equipment inventory was effective (i.e., provided reasonable assurance of the reliability of inventory information and accountability of the individual items). For each IT equipment item in our statistical sample, we assessed whether (1) the item existed (meaning that the item recorded in the inventory records could be located), (2) inventory records and processes provided adequate accountability, and (3) identifying information (property number, serial number, model number, and location) was accurate. We explain the results of our existence tests in terms of control failures related to missing items and recordkeeping errors. The results of our statistical samples are specific to each of the four test locations and cannot be projected to the population of VA IT inventory as a whole. We present the results of our statistical samples for each population as point estimates representing (1) our projection of the estimated error overall for each control attribute and (2) the two-sided, 95 percent confidence intervals for the failure rates.

To assess VA's controls over computer hard drives in the property disposal process, at each HCS and VA headquarters we interviewed OIT officials, observed hard drive storage locations, and obtained copies of VA documentation related to hard drives in the disposal process at the time of our site visits.

Our investigators supported our tests of IT physical inventory controls by assessing the physical security of various IT equipment storage facilities at each of our four case study locations. As part of our assessment, one of our investigators interviewed VA Police at the three HCS locations and federal agency law enforcement officers at VA headquarters and met with physical security specialists at each of the test locations to discuss the results of our physical security inspections and the status of VA actions on identified weaknesses.

We briefed VA managers at our three HCS test locations and VA headquarters, including VA HCS directors and OIT and property management officials, on the details of our audit, our findings, and their implications. On July 15, 2008, we requested comments on a draft of this report. We received comments from the Secretary of Veterans Affairs on July 28, 2008, and we had follow-up discussions with cognizant VA officials. We have summarized VA's comments and our follow-up discussions in the Agency Comments and Our Evaluation section of this report. We conducted this performance audit from January 2008 through July 2008 in accordance with generally accepted government auditing



---

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We performed our investigative work in accordance with standards prescribed by the President's Council on Integrity and Efficiency.

# Appendix II: Status of VA Actions on Recommendations in GAO's July 2007 and 2004 Reports

Table 10 lists the 12 recommendations from our 2007 report, summarizes VA's actions, and presents the status of each recommendation. VA property officials from the Office of Acquisition and Logistics (OAL) and officials in the Office of Information and Technology (OIT) worked together to create a new VA Handbook 7002, *Logistics Management Procedures*, which updates VA policy for property management, including specific policy pertaining to information technology (IT) equipment. The Assistant Secretary for Management mandated early implementation of VA Handbook 7002 on July 3, 2008.

**Table 10: GAO's 2007 Report Recommendations and Status of VA Actions as of July 2008**

GAO recommendation	VA action on the recommendation	Status of GAO recommendation
<b>2007 VA-wide recommendations:</b>		
1. Revise VA property management policy and procedures to include detailed requirements for what transactions must be recorded to document inventory events and to clearly establish individual responsibility for recording all essential transactions in the property management process.	VA mandated early implementation of Handbook 7002, <i>Logistics Management Procedures</i> , which requires the recording of key inventory events, including the recording of IT equipment information upon receipt, changes in item status, and turn-in and disposal.	Fully implemented
2. Revise VA purchase card policy to require purchase card holders to notify property management officials of IT equipment and other property items acquired with government purchase cards at the time the items are received so that they can be recorded in property management systems.	VA mandated early implementation of VA Handbook 4080, <i>Government Purchase Card Procedures</i> , which requires purchase cardholders to notify the property officer of IT equipment acquired with the purchase card so that these items may be recorded in the property management system. Handbook 7002 includes the same requirement.	Fully implemented
3. Establish procedures to require specific, individual user-level accountability for IT equipment. In implementing this recommendation, consideration should be given to making the unit head, or a designee, accountable for shared IT equipment.	Handbook 7002 requires employees to sign for IT equipment assigned exclusively for individual use and department heads or service chiefs to sign for shared IT equipment.	Fully implemented
4. Enforce user-level accountability and IT coordinator responsibility by taking appropriate disciplinary action, including holding employees financially liable, as appropriate, for lost or missing IT equipment.	VA facilities provided several fiscal year 2008 examples of bills sent to VA personnel for lost and damaged IT equipment items.	Fully implemented

**Appendix II: Status of VA Actions on  
Recommendations in GAO's July 2007 and  
2004 Reports**

GAO recommendation	VA action on the recommendation	Status of GAO recommendation
5. Establish specific time frames for finalizing a Report of Survey once an inventory has been completed so that research on missing items is completed expeditiously and does not continue indefinitely without meeting formal reporting requirements.	In May 2008, OAL issued an information letter implementing immediately an overall Report of Survey timeline of 60 days. In addition, Handbook 7002 requires the Report of Survey process to be completed within 60 days.	Fully implemented
6. Establish a mechanism to monitor adherence by the San Diego and Houston medical centers and other VA organizations, as appropriate, to VA policy for performing annual inventories of sensitive items under \$5,000, including IT equipment.	VA established the Office of Information Technology Oversight and Compliance in February 2007, which reviewed compliance with established VA policy. VA also established a tiger team in May 2007, which reviewed the results of the VA-wide 2007 physical inventory of IT equipment.	Fully implemented
7. Require that information resource management and IT Services personnel at the various medical centers be given access to the central property database and be furnished with scanners so they can electronically update the property control records, as appropriate, during installation, repair, replacement, and relocation or disposal of IT equipment.	VA has granted OIT personnel access to the central property database (AEMS/MERS). Furthermore, VA has begun to furnish OIT employees with hand scanners that may be used to scan equipment during routine maintenance. VA reports that it is currently assessing how many hand scanners various VA facilities need.	Partially implemented
8. Require physical security personnel to perform inspections of buildings and storage facilities to identify informal and undesignated IT storage locations so that security assessments are performed and corrective actions are implemented, as appropriate.	In September 2007, VA established Handbook 6500, <i>Information Security Program</i> , requiring that the Information Security Officer conduct and document physical security reviews as part of the annual review of the system security plan to help analyze any new or existing physical security vulnerabilities.	Fully implemented
<b>2007 Recommendations for the CIO:</b>		
9. Establish a formal policy requiring a review of the results of annual inventories to ensure that IT equipment inventory records are properly updated and no blank fields remain.	VA Handbook 7002 requires the accountable officer to ensure that property records have been updated correctly at the completion of each physical inventory and that no blank fields remain.	Fully implemented
10. Establish a process for reviewing Reports of Survey for lost, missing, and stolen IT equipment items to identify systemic weaknesses for appropriate corrective action.	VA's OIT is working with OAL and the Office of Prosthetics and Clinical Logistics to develop an integrated approach for Report of Survey monitoring. OIT's tiger team also is reviewing VA facilities' internal controls for IT equipment and the results of the 2007 physical inventory, which included IT equipment items submitted for Report of Survey processing. However, VA has not yet established a formalized process for reviewing Reports of Survey.	Open

**Appendix II: Status of VA Actions on  
Recommendations in GAO's July 2007 and  
2004 Reports**

<b>GAO recommendation</b>	<b>VA action on the recommendation</b>	<b>Status of GAO recommendation</b>
11. Establish and implement a policy requiring information resource management personnel and IT coordinators to inform physical security officers of the site of all IT equipment storage locations so that these store rooms can be subjected to required inspections.	VA Handbook 7002 requires that facilities' Security Management Committees (SMC) develop local strategic security plans as guides to identify physical and procedural security needs. Handbook 7002 requires the IT custodial officer to provide the facility information security officer a list of all IT storage areas and that access to IT equipment storage areas be provided to facility security personnel for use in performing regular inspections.	Fully implemented
12. Establish and implement a policy for reviewing the results of physical security inspections of IT equipment storerooms and ensure that needed corrective actions are completed.	VA Handbook 7002 states that the IT custodial officer will coordinate with the SMC to develop a plan to address IT-related security requirements identified in the strategic security plan. The handbook also requires the IT custodial officer to develop a plan to address all corrective actions identified in the Report of Physical Security Inspection of IT Equipment Store Rooms within 10 days of receipt of the report from security personnel.	Fully implemented

Source: GAO interviews of agency officials and analysis of VA documentation.

Table 11 lists the 6 property-related recommendations from our 2004 report, summarizes VA's actions, and presents the status of each recommendation.

**Table 11: GAO's 2004 Report Recommendations and Status of VA Actions as of July 2008**

<b>GAO recommendation</b>	<b>VA action on the recommendation</b>	<b>Status of GAO recommendation</b>
<b>2004 Property-related recommendations:</b>		
1. Clarify existing guidance and establish consistent parameters for personal property that is required to be accounted for in the property control records and that is subject to physical inventory to include sensitive property.	In October 2005, VA issued a modification to VA Handbook 7127/4, <i>Materiel Management Procedures</i> , which stated that sensitive items, regardless of cost, should be included in annual equipment inventories. In addition, the guidance provided an expanded list of eight categories of sensitive items.	Fully implemented
2. Provide a more comprehensive list of the type of personal property assets that are considered sensitive for accountability purposes.	In October 2005, VA issued a modification to VA Handbook 7127/4, <i>Materiel Management Procedures</i> , which provided an expanded list of eight categories of sensitive items, including handheld and portable communication devices, printers, desktop and laptop computers, and video imaging equipment.	Fully implemented

**Appendix II: Status of VA Actions on  
Recommendations in GAO's July 2007 and  
2004 Reports**

GAO recommendation	VA action on the recommendation	Status of GAO recommendation
3. Direct that physical inventories of personal property be performed by the Acquisition and Materiel Management staff or other parties who are independent of those with property custodian responsibilities.	In October 2005, VA issued a modification to Handbook 7127/4, <i>Materiel Management Procedures</i> , which required that all completed inventories have a 5 percent verification inventory conducted by an accountable officer or designee, a disinterested party, and the custodial officer or designee. However, the handbook did not direct that the independent party should perform the physical inventories, and 5 percent verifications do not suffice for independent inventories. In addition, VA has begun to furnish OIT employees with hand scanners that may be used to scan equipment. VA reports that it is currently assessing how many hand scanners its facilities need. The use of hand scanners for capturing IT equipment bar code label and serial number information during physical inventories would help achieve necessary independence.	Partially implemented
4. Reinforce VA's requirement to attach bar code labels to agency personal property.	During a June 2008 property conference call with property management personnel from VA field locations across the nation, OAL personnel reinforced VA's requirement to attach bar code labels to agency personal property.	Fully implemented
5. For the six sites we visited in 2004, determine the location or disposition of personal property items not found during our site visits.	VA reported in its Fiscal Year 2006 Budget Submission that the six identified medical centers were directed to conduct inventories of equipment inventory listings by March 31, 2005. VA further reported that upon completion of the inventories, the network director must submit certification that inventories were accomplished, any discrepancies were identified, and required Reports of Survey were prepared on items that could not be found.	Fully implemented
6. For the six sites we visited in 2004, review property records to identify and correct erroneous or incomplete data fields.	In June 2008, VA's Office of Information and Technology Oversight and Compliance planned to review the erroneous and blank data fields at the six medical centers we visited. In addition, VA officials indicated that they plan to review the data fields at a national level using a data warehouse and provide reports to the six sites by September 1, 2008. However, VA has not yet reviewed or corrected these erroneous and blank data fields.	Open

Source: GAO interviews of agency officials and analysis of VA documentation.

# Appendix III: Comments from the Department of Veterans Affairs



THE SECRETARY OF VETERANS AFFAIRS  
WASHINGTON

July 28, 2008

Ms. Kay L. Daly  
Acting Director  
Financial Management and Assurance  
U. S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Ms. Daly:

The Department of Veterans Affairs (VA) has reviewed your draft report, **VETERANS AFFAIRS: Continued Action Needed to Reduce IT Equipment Losses and Correct Control Weaknesses** (GAO-08-918), and generally agrees with all but one of the recommendations. VA does not agree with the recommendation that medical devices with data storage capability be considered information technology (IT) equipment for the purpose of inventory control. Not only is this counter to the Joint Commission accreditation requirements, a separate inventory of medical equipment is a necessity to address the Food and Drug Administration's recalls and other hazard notifications related to patient safety. VA does agree that sensitive information must be protected, and VA has established policy to deal with this issue. VA agrees with GAO's recommendation regarding the development of a standardized naming classification for IT equipment, but differs on the responsibility for implementing the recommendation.

The enclosure specifically addresses GAO's recommendations and provides additional discussion and comments to the draft report. VA appreciates the opportunity to comment on your draft report.

Sincerely yours,

A handwritten signature in black ink, appearing to read "James B. Peake".

James B. Peake, M.D.

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comments to  
Government Accountability Office (GAO) Draft Report  
**CONTINUED ACTION NEEDED TO REDUCE IT EQUIPMENT LOSSES AND  
CORRECT CONTROL WEAKNESSES**  
(GAO-08-918)

**GAO recommends that the Department of Veterans Affairs take the following five actions:**

- **Review property inventory records and confirm that all IT equipment, regardless of the organizational equipment inventory listing, is identified in the property system.**

**Concur-** VA Handbook 7002 requires the senior information technology (IT) official at each facility to review property inventory records and ensure that all IT equipment is identified in the VA property system. The senior IT official is responsible for establishing and implementing a process to identify, account for, track, monitor, inventory, and dispose of IT items that are capable of storing information electronically but are not assigned catalog stock numbers (CSN). The senior IT official will coordinate perpetual inventory activities as well as schedule and conduct an annual physical inventory of expendable IT items to verify the accuracy of the data contained in the sensitive expendable IT item listing (SEILL). The senior IT official will document and report any discrepancies identified during inventory activities.

The senior IT official will also coordinate perpetual inventory activities and conduct an annual physical inventory of IT equipment items assigned a CSN in accordance with the schedule established by Logistic Services to verify the accuracy of the data contained in the equipment inventory listing (EIL). The senior IT official is responsible for documenting and reporting any discrepancies identified during inventory activities. The annual EIL/SEILL inventories include an audit to ensure accurate documentation in the inventory tracking systems. Following an inventory of IT items, or whenever an IT equipment item is identified as 'not accounted for', the senior IT official will review the documentation for discrepancies and coordinate with Logistic Services regarding a determination as to the need for report of survey (ROS) action. IT items on ROS must be resolved within 60 days of initiation. Any exceptions will be documented in a plan of action and approved by the facility director. The facility director is accountable for all equipment in their facility and is responsible for ensuring adherence to all applicable policies. Performance measures are being established for Office of Information and Technology (OI&T) regional directors and Veterans Health Administration (VHA) facility directors related to the accountability of IT equipment under their cognizance.

- **Establish and implement a policy requiring facility CIOs to develop standardized naming classifications for IT equipment, including item**

Enclosure

Department of Veterans Affairs (VA) Comments to  
Government Accountability Office (GAO) Draft Report  
**CONTINUED ACTION NEEDED TO REDUCE IT EQUIPMENT LOSSES AND  
CORRECT CONTROL WEAKNESSES**  
(GAO-08-918)  
(continued)

**name, manufacturer, and model, for recording IT equipment into  
local property inventory systems.**

**Partially Concur-** VA concurs that standardized naming classifications are required to support tracking of IT equipment. However, VA does not concur that the standardized naming classifications should be established at the facility level. VA employs a cataloging process to categorize equipment using CSNs. The CSNs are assigned according to the schema established in VA Catalog No. 3, Section V, which provides a description for each CSN. This provides for a standardized naming classification system that applies across the Department.

In the Fall of 2006 a group of subject matter experts assembled to develop standard operating procedures (SOP) for Veterans Health Administration (VHA) on asset management. These SOPs were issued March 8, 2007. One of the SOPs (AM 1 SOP) specifically addresses the data elements required to be included in the local property inventory system maintained in the Automated Engineering Management System/Medical Equipment Repair Service (AEMS/MERS) system. These data elements include item name, manufacturer, and model number/designation for each item of IT equipment.

Prosthetics and Clinical Logistics Office (P&CLO) will be assessing compliance with this requirement by September 2008. Monthly reports will be generated and analyzed to identify facilities with incomplete data. P&CLO will send notifications to OI&T regional directors and VHA facility directors of non-compliant sites. Copies of reports will also be provided to the IT Asset Advisory Group (ITAAG) for trend analysis and to support the identification of systemic issues requiring corrective action.

- **Develop a list of medical equipment with data storage capability that should be considered as IT equipment for inventory control purposes.**

**Partially Concur -** VA does concur with maintaining an inventory of all equipment, including medical for inventory control purposes. In accordance with VA Handbook 7002, the facility director is responsible for ensuring that all nonexpendable equipment items, and sensitive equipment items regardless of cost, are entered into the VA property system for inventory control purposes. The Joint Commission verifies that medical devices are subjected to inspection before deployment; this inspection process includes the entry of these items into the property system. VA Handbook 6500



Enclosure

Department of Veterans Affairs (VA) Comments to  
Government Accountability Office (GAO) Draft Report  
**CONTINUED ACTION NEEDED TO REDUCE IT EQUIPMENT LOSSES AND  
CORRECT CONTROL WEAKNESSES**  
(GAO-08-918)  
(continued)

addresses the requirements associated with the management and protection of sensitive information and applies to all organizational components of the Department.

VA does not concur with redefining medical equipment as IT equipment. Joint Commission accreditation requirements include maintenance of a separate and distinct medical equipment inventory to manage and document quality assurance activities. Medical devices are highly regulated by the Food and Drug Administration and a separate and accurate inventory is a necessity to address recall and other hazard notifications to minimize potential impact on patient safety.

- **Develop a procedure for identifying hard drive serial numbers with both the property identification numbers and serial numbers of host computers.**

**Concur-** VA agrees that hard drives need to be tracked and matched to host computers. OI&T and P&CLO will develop a procedure for identifying hard drive serial numbers with both the property identification numbers and serial numbers of host computers by the end of fiscal year 2008. This procedure will delineate organizational responsibilities and the process for ensuring appropriate mapping of hard drives to host computers.

- **Revise the definition of IT storage locations in VA's Handbook 0730/1, *Security and Law Enforcement*, to include informal IT storage locations, such as OIT work rooms and require these locations to be included in physical security inspections.**

**Concur-** OI&T will work with Security and Law Enforcement to revise the definition of IT storage locations to include informal IT storage locations. Meanwhile, IT custodial officers are responsible for identifying all IT storage areas for security personnel. The following requirements are included in VA Handbook 7002:

*The IT Custodial Officer will provide a list of all IT storage areas to the Facility IT Security Officer (FISO). This list will be updated as necessary to ensure it is maintained current....*

*Access to IT equipment storage locations will be provided to facility security personnel to perform regular inspections. Security personnel will provide a Report of Physical Security Inspection of IT Equipment Store Rooms to the IT Custodial Officer at the facility within 10 days of completing a physical security inspection. The report will document*

# Appendix IV: Reports of Survey on Missing IT Equipment for VA Case Study Locations

Table 12 summarizes Report of Survey<sup>1</sup> information related to VA's 2007 physical inventories of IT equipment for the 12 case study locations covered in our 2004, 2007, and 2008 audits. We used the original acquisition value as the best available data for the cost of IT equipment items that could not be located during VA's 2007 physical inventory.

**Table 12: Summary of Reports of Survey as of May 15, 2008, for Case Study Locations Covered in GAO Audits**

Location	Date physical inventory completed	Dates VA closed Reports of Survey	Items missing as of 12/31/07	Items missing as of 5/15/08	Reported original acquisition value of missing items as of 5/15/08
Atlanta medical center	Aug. 2007	Apr. 2008	198	129	\$ 220,115
Boston healthcare system	Dec. 2007	Ongoing	3,663	3,226	5,026,271
North Texas healthcare system	Dec. 2007	Ongoing	5,309	5,308	5,615,070
Washington D.C. medical center	Sept. 2007	May 2008	139	115	120,048
Houston medical center	Dec. 2007	Ongoing	6,485	6,427	7,737,917
Indianapolis medical center	Dec. 2007	May 2008	113	82	29,986
Los Angeles medical center	Dec. 2007	Ongoing	1,767	1,648	1,273,144
VA headquarters	Jan. 2008	Ongoing	1,595	1,314	3,316,951
San Diego healthcare system	Dec. 2007	Feb. 2008	930	863	717,805
San Francisco medical center	Dec. 2007	May 2008	39	39	105,298
Puget Sound healthcare system	Dec. 2007	Ongoing	1,383	1,269	1,536,840
Tampa medical center	Dec. 2007	Ongoing	815	690	638,946

Source: GAO analysis of VA-reported 2007 inventory results and related Reports of Survey data.

<sup>1</sup>The Report of Survey system is the method used by VA to obtain an explanation of the circumstances surrounding loss, damage, or destruction of government property other than through normal wear and tear.

---

# Appendix V: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Kay L. Daly, (202) 512-9095 or dalykl@gao.gov

---

## Acknowledgments

In addition to the contact named above, Gayle L. Fischer, Assistant Director; Andrew O'Connell, Assistant Director and Supervisory Special Agent; F. Abe Dymond, Assistant General Counsel; Doreen S. Eng, Assistant Director; Bamidele A. Adesina; James D. Ashley; Deyanna J. Beeler; Francine M. DeVecchio; Lauren S. Fassler; Steven M. Koons; Kelly A. Richburg; Ramon J. Rodriguez, Special Agent; Daniel E. Silva; Chevalier C. Strong; Danietta S. Williams; and Matthew L. Wood made key contributions to this report.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548