

July 2007

VETERANS AFFAIRS

Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation





Highlights of [GAO-07-505](#), a report to congressional requesters

VETERANS AFFAIRS

Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation

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 had problems with implementation of VA inventory policies and procedures. Fewer than half the items GAO selected for testing could be located. Most of the missing items were information technology (IT) equipment. Given recent thefts of laptops and data breaches, the requesters were concerned about the adequacy of physical inventory controls over VA IT equipment. GAO was asked to determine (1) the risk of theft, loss, or misappropriation of IT equipment at selected locations; (2) whether selected locations have adequate procedures in place to assure accountability and physical security of IT equipment in the excess property disposal process; and (3) what actions VA management has taken to address identified IT inventory control weaknesses. GAO statistically tested inventory controls at four case study locations.

What GAO Recommends

GAO makes 12 recommendations to improve VA-wide policies and procedures with respect to controls over IT equipment, including recordkeeping requirements, physical inventories, user-level accountability, and physical security. VA agreed with GAO's findings, noted significant actions under way, and concurred on the 12 recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-505.

To view the full product, including the scope and methodology, click on the link above. For more information, contact McCoy Williams at (202) 512-9095 or williams1@gao.gov.

What GAO Found

A weak overall control environment for VA IT equipment at the four locations GAO audited poses a significant security vulnerability to the nation's veterans with regard to sensitive data maintained on this equipment. GAO's *Standards for Internal Control in the Federal Government* requires agencies to establish physical controls to safeguard vulnerable assets, such as IT equipment, which might be vulnerable to risk of loss, and federal records management law requires federal agencies to record essential transactions. However, GAO found that current VA property management policy does not provide guidance for creating records of inventory transactions as changes occur. GAO also found that policies requiring annual inventories of sensitive items, such as IT equipment; adequate physical security; and immediate reporting of lost and missing items have not been enforced. GAO's statistical tests of physical inventory controls at four VA locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive data. The lack of user-level accountability and inaccurate records on status, location, and item descriptions make it difficult to determine the extent to which actual theft, loss, or misappropriation may have occurred without detection. The table below summarizes the results of GAO's statistical tests at each location.

Current IT Inventory Control Failures at Four Test Locations

| Control failures | Washington, D.C. | Indianapolis | San Diego | VA HQ offices |
|-----------------------------|------------------|--------------|-----------|---------------|
| Missing items | 28% | 6% | 10% | 11% |
| Incorrect user organization | 80% | 69% | 70% | 11% |
| Incorrect location | 57% | 23% | 53% | 44% |
| Recordkeeping errors | 5% | 0% | 5% | 3% |

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 also found that the four VA locations reported over 2,400 missing IT equipment items, valued at about \$6.4 million, identified during physical inventories performed during fiscal years 2005 and 2006. Missing items were often not reported for several months and, in some cases, several years. It is very difficult to investigate these losses because information on specific events and circumstances at the time of the losses is not known. GAO's limited tests of computer hard drives in the excess property disposal process found hard drives at two of the four case study locations that contained personal information, including veterans' names and Social Security numbers. GAO's tests did not find any remaining data after sanitization procedures were performed. However, weaknesses in physical security at IT storage locations and delays in completing the data sanitization process heighten the risk of data breach. Although VA management has taken some actions to improve controls over IT equipment, including strengthening policies and procedures, improving the overall control environment for sensitive IT equipment will require a renewed focus, oversight, and continued commitment throughout the organization.

Contents

| | | |
|---------------|--|----|
| Letter | | 1 |
| | Results in Brief | 4 |
| | Background | 7 |
| | Inadequate IT Inventory Control and Accountability Pose Risk of Loss, Theft, and Misappropriation | 13 |
| | Physical Security Weaknesses Increase Risk of Loss, Theft, and Misappropriation of IT Equipment and Sensitive Data | 29 |
| | VA Actions to Improve IT Management and Controls Have Been Limited | 34 |
| | Conclusions | 35 |
| | Recommendations for Executive Action | 36 |
| | Agency Comments and Our Evaluation | 37 |

| | | |
|-------------------|---|----|
| Appendix I | Objectives, Scope, and Methodology | 39 |
|-------------------|---|----|

| | | |
|--------------------|---|----|
| Appendix II | Comments from the Department of Veterans Affairs | 44 |
|--------------------|---|----|

| | | |
|---------------------|--|----|
| Appendix III | GAO Contact and Staff Acknowledgments | 53 |
|---------------------|--|----|

| | | |
|---------------|---|----|
| Tables | | |
| | Table 1: Current IT Equipment Inventory Control Failure Rates at Four Test Locations | 14 |
| | Table 2: Number of Missing IT Equipment Items at Four Test Locations, Including Items That Could Have Stored Sensitive Information | 15 |
| | Table 3: Number of Missing IT Equipment Items by Headquarters Office and Missing Items That Could Have Stored Sensitive Personal Data and Information | 20 |
| | Table 4: Estimated Percentage of IT Inventory Control Failures Related to Correct User and Location at the Four Test Locations | 22 |
| | Table 5: Estimated Percentage of Other IT Inventory Recordkeeping Failures at Four Test Locations | 24 |
| | Table 6: Summary of Physical Inventories and Missing IT Equipment Identified by the Four Current Case Study Locations as of February 28, 2007 | 27 |

| | |
|--|----|
| Table 7: Summary of Physical Inventories and Missing IT Equipment Identified by Five Case Study Locations Previously Audited as of March 2, 2007 | 29 |
| Table 8: Population of VA IT Equipment at Locations Selected for Testing | 40 |
| Table 9: Number of Computer Hard Drives in the Property Disposal Process Selected for Testing at Four Locations | 42 |

Figures

| | |
|--|----|
| Figure 1: VA's IT Property Management Process | 8 |
| Figure 2: Photograph of Unsecured IT Equipment Storeroom in the VA Headquarters Building | 33 |

Abbreviations

| | |
|-----------|--|
| AEMS/MERS | Automated Engineering Management System/Medical Equipment Repair Service |
| CFR | Code of Federal Regulations |
| CIO | Chief Information Officer |
| CMR | consolidated memorandum receipt |
| DOD | Department of Defense |
| EIL | equipment inventory listing |
| FMFIA | Financial Managers' Financial Integrity Act of 1982 |
| HHS | Department of Health and Human Services |
| HIPAA | Health Information Portability and Accountability Act of 1996 |
| IFCAPS | Integrated Funds Distribution Control Point Activity, Accounting, and Procurement System |
| IRM | information resource management |
| IT | information technology |
| MRI | magnetic resonance imaging |
| NARA | National Archives and Records Administration |
| NIST | National Institute of Standards and Technology |
| USB | universal serial bus |
| USC | United States Code |
| VA | Department of Veterans Affairs |
| 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 16, 2007

The Honorable Bob Filner
Chairman
The Honorable Steve Buyer
Ranking Member
Committee on Veterans' Affairs
House of Representatives

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

In light of reported weaknesses in Department of Veterans Affairs (VA) inventory controls and reported thefts of laptop computers and data breaches, you were concerned about the adequacy of controls over VA information technology (IT) equipment. In July 2004, we reported¹ that the six VA medical centers we audited lacked a reliable property control database, which did not produce a complete and accurate record of current inventory and compromised effective management and security of agency assets. We found that key policies and procedures established by VA to control personal property provided facilities with substantial latitude in conducting physical inventories² and maintaining their property management systems, which resulted in reduced property accountability. For example, VA's Handbook 7127/3, *Materiel Management Procedures*³ allowed the person responsible for custody of VA property to attest to the existence of that property rather than requiring independent verification. Also, personnel at some locations interpreted a policy that established a \$5,000 threshold for property that must be inventoried as a license to

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

² Physical inventory is the process of reconciling personal property records with the property actually on hand.

³ Department of Veterans Affairs, VA Handbook 7127/3, *Materiel Management Procedures*.

ignore VA requirements to account for sensitive, lower cost items that are susceptible to theft or loss, such as personal computers and peripheral equipment. Personnel at the VA medical centers, which are part of the Veterans Health Administration (VHA), located fewer than half of the 100 items we selected for testing at each of five medical centers and 62 of 100 items at the sixth medical center. Most of the items that could not be located were computer equipment. Based on our work, we concluded in our July 2004 report that these weak practices, combined with lax implementation, resulted in low levels of accountability and heightened risk of loss.

During 2006, VA employed nearly 235,000 employees and relied on an undetermined number of contractors, volunteers, and students to support its operations. VA provided these individuals a wide range of IT equipment,⁴ including desktop and laptop computers, monitors and printers, personal digital assistants, unit-level workstations, local area networks, and medical equipment with memory and data processing/communication capabilities. VA information resource management (IRM) and property management personnel share responsibility for management of IT equipment inventory.

This report responds to your request that we perform follow-up work to determine (1) the risk of theft, loss, or misappropriation⁵ of IT equipment at selected VA locations; (2) whether selected VA locations have adequate procedures in place to assure physical security and accountability over IT equipment in the excess property disposal process;⁶ and (3) what actions VA management has taken to address identified IT equipment inventory control weaknesses. In assessing the risk of theft, loss, or misappropriation of IT equipment, you also asked that we consider the

⁴ For the purpose of this audit, we defined IT equipment as any equipment capable of processing or storing 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.

⁵ As used in this report, theft and misappropriation both refer to the unlawful taking or stealing of personal property, with misappropriation occurring when the wrongdoer is an employee or other authorized user.

⁶ 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.

results of physical inventories performed by the four case study locations covered in this audit and the six medical centers we previously audited.⁷

To achieve our first two objectives, we used a case study approach, selecting VA medical centers located in Washington, D.C., Indianapolis, Indiana, and San Diego, California; associated clinics; and VA headquarters organizations for our test work. To determine the risk of theft, loss, or misappropriation of IT equipment at these locations, we statistically tested IT equipment inventory to determine the effectiveness of controls relied on for accurate recording of inventory transactions, including existence (meaning IT equipment items listed in inventory records exist and can be located), user-level accountability, and inventory record accuracy. As requested, we also obtained and analyzed the results of physical inventories performed by the case study locations covered in our current and our previous audits. In addition, our investigator assessed physical security of IT equipment storerooms and procedures for reporting lost and missing items to VA law enforcement officials at our four current case study locations. To determine if the four case study locations had adequate procedures in place for proper disposal of excess IT equipment, we assessed procedures for security and accountability of excess IT equipment and independently tested a limited selection of computer hard drives for proper removal of data and compliance with VA property management policies. We performed sufficient procedures to determine that inventory data at the test locations were reliable for the purpose of our audit.⁸ We conducted our audit and investigation from September 2006 through March 2007. We performed our audit procedures in accordance with generally accepted government auditing standards, and we performed our investigative procedures in accordance with quality standards for investigators as set forth by the President's Council on Integrity and Efficiency. We obtained agency comments on a draft of this report. A detailed discussion of our objectives, scope, and methodology is included in appendix I.

⁷ The Washington, D.C., medical center was also covered in our 2004 report.

⁸ The universe 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 universe 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.

Results in Brief

A weak overall control environment and pervasive weaknesses in inventory control and accountability at the four locations we audited put IT equipment at risk of theft, loss, and misappropriation and pose a continuing security vulnerability to our nation's veterans with regard to sensitive data maintained on this equipment. Our *Standards for Internal Control in the Federal Government*⁹ 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. Further, federal records management law and regulations require agencies to create and maintain records of essential transactions, including property records, as part of an effective internal control structure. However, we found that current VA property management policy does not provide guidance for recording IT equipment inventory transactions as events occur. We also found that certain other VA policies have not been enforced, including policies requiring (1) user-level accountability; (2) annual inventories of sensitive items, including IT equipment; (3) adequate physical security; and (4) immediate reporting of lost and missing items. Our statistical tests of IT equipment inventory controls at our four VA case study locations identified a total of 123 missing IT equipment items, including 53 computers that could have stored sensitive data. We estimate the percentage of inventory control failures related to these missing items to be 6 percent at the Indianapolis medical center, 10 percent at the San Diego medical center, 28 percent at the Washington, D.C., medical center, and 11 percent for VA headquarters organizations.¹⁰ In addition, although VA property management policy establishes guidelines for user-level accountability, we found a pervasive lack of user-level accountability across the four case study locations, and significant errors in recorded IT inventory information concerning user organization and location. As a result, for the four case study locations, we concluded that under the lax control environment, essentially no one was accountable for IT equipment. The lack of user-level accountability and inaccurate records on status, location, and item descriptions make it difficult to determine the extent to which actual theft, loss, or misappropriation may have occurred without detection at the case study locations.

⁹ GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

¹⁰ Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of +/- 7 percent or less.

Our follow-up on the results of physical inventories performed by the four case study locations included in our current audit and the five other case study locations from our previous audit found that the case study locations identified thousands of missing IT equipment items valued at tens of millions of dollars. For example, the four case study locations included in our current audit reported over 2,400 missing IT equipment items, with a combined original acquisition value of about \$6.4 million. Information we obtained as of March 2, 2007, showed that the five other locations we previously audited had identified over 8,600 missing IT equipment items with a combined original acquisition value of over \$13.2 million. One of the four case study locations in our current audit and three of the five other case study locations covered in our previous audit had not yet completed Reports of Survey¹¹ on losses identified in their physical inventories. Because none of the nine case study locations consistently recorded transactions as changes in IT equipment inventory status and location occurred, it is not possible to determine the disposition of IT equipment items that cannot be located. When attempts to locate missing IT equipment items were unfruitful, the losses were administratively reported for recordkeeping purposes, including the authorization to write them off in the property records. According to VA Police and security specialists,¹² when losses are not immediately identified and reported, it is very difficult to conduct an investigation because information about the specific events and circumstances of the losses is no longer available.

Our limited tests of computer hard drives in the excess property disposal process at the four case study locations found no data on those hard drives that were certified as sanitized.¹³ However, at two of the four test

¹¹ 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.

¹² VA medical centers and other facilities have a VA Police Service, which provides law enforcement and physical security services, including security inspections and criminal investigations. The VA headquarters building does not have a police service. VA headquarters law enforcement duties are the responsibility of the Federal Protective Service.

¹³ VA IRM personnel and contractors follow National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines as well as more stringent Department of Defense (DOD) policy in DOD 5220.22-M, *National Industrial Security Program Operating Manual*, ch. 8, § 8-301, which requires performing three separate erasures for media sanitization.

locations, we found that hard drives not yet subjected to data sanitization contained hundreds of names and Social Security numbers. Further, file dates on the hard drives we tested indicate that some of them had been in the disposal process for several years without being sanitized, creating an unnecessary risk that sensitive personal and medical information could be compromised. Excessive delays in completing data sanitization processes and noncompliance with VA physical security policy heighten the risk of data breach related to sensitive personal information residing on hard drives in the excess property disposal process. For example, we found numerous unofficial IT equipment storage locations in VA headquarters area office buildings that did not meet VA physical security requirements. One IT storeroom at the VA headquarters building did not have a door. At other VA headquarters buildings, we found IT equipment stored in open areas, closets, and filing cabinets. These storage locations did not meet VA physical security requirements for secure walls, doors, locks, special keys, and intrusion detection alarms.

Since our July 2004 report, VA management has taken some actions and has other actions under way to strengthen controls over IT equipment. For example, on October 11, 2005, VA revised its *Materiel Management Procedures*¹⁴ to emphasize that requirements for annual inventories of sensitive items valued at under \$5,000 include IT equipment. On August 4, 2006, VA issued a new directive entitled *Information Security Program*, which requires, in part, periodic evaluations and testing of the effectiveness of all management, operational, and technical controls and calls for procedures for immediately reporting and responding to security incidents. In December 2006, VA's new Chief Information Officer (CIO) centralized functional IT units across local VA organizations under the CIO organization. Despite these improvements, the department has not yet established and ensured consistent implementation of effective controls for accountability of IT equipment inventory, and IT inventory responsibilities shared by IRM and property management personnel are not well-defined. Until these shortcomings are addressed, VA will continue to face major challenges in safeguarding IT equipment and sensitive personal data on this equipment from loss, theft, and misappropriation.

This report contains 12 recommendations to VA to further improve the overall control environment and strengthen key internal control activities and to increase attention to protecting IT equipment used in VA

¹⁴ VA Handbook 7127/4 § 5302.3, "Inventory of Equipment in Use."

operations. In comments on a draft of this report, VA generally agreed with our findings, noted significant actions under way, and concurred on the 12 recommendations. VA also provided technical comments. VA's comments, including its technical comments, are discussed in the Agency Comments and Our Evaluation section of this report. VA's written comments are reprinted in appendix II.

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 has over 235,000 employees, including physicians, nurses, counselors, statisticians, computer specialists, architects, and attorneys. VA carries out its mission through three major line organizations—VHA, Veterans Benefits Administration, and National Cemetery Administration—and field facilities throughout the United States. VA provides services and benefits through a nationwide network of 156 hospitals, 877 outpatient clinics, 136 nursing homes, 43 residential rehabilitation treatment programs, 207 readjustment counseling centers, 57 veterans' benefits regional offices, and 122 national cemeteries.

Previously Reported Weaknesses in IT Inventory Controls

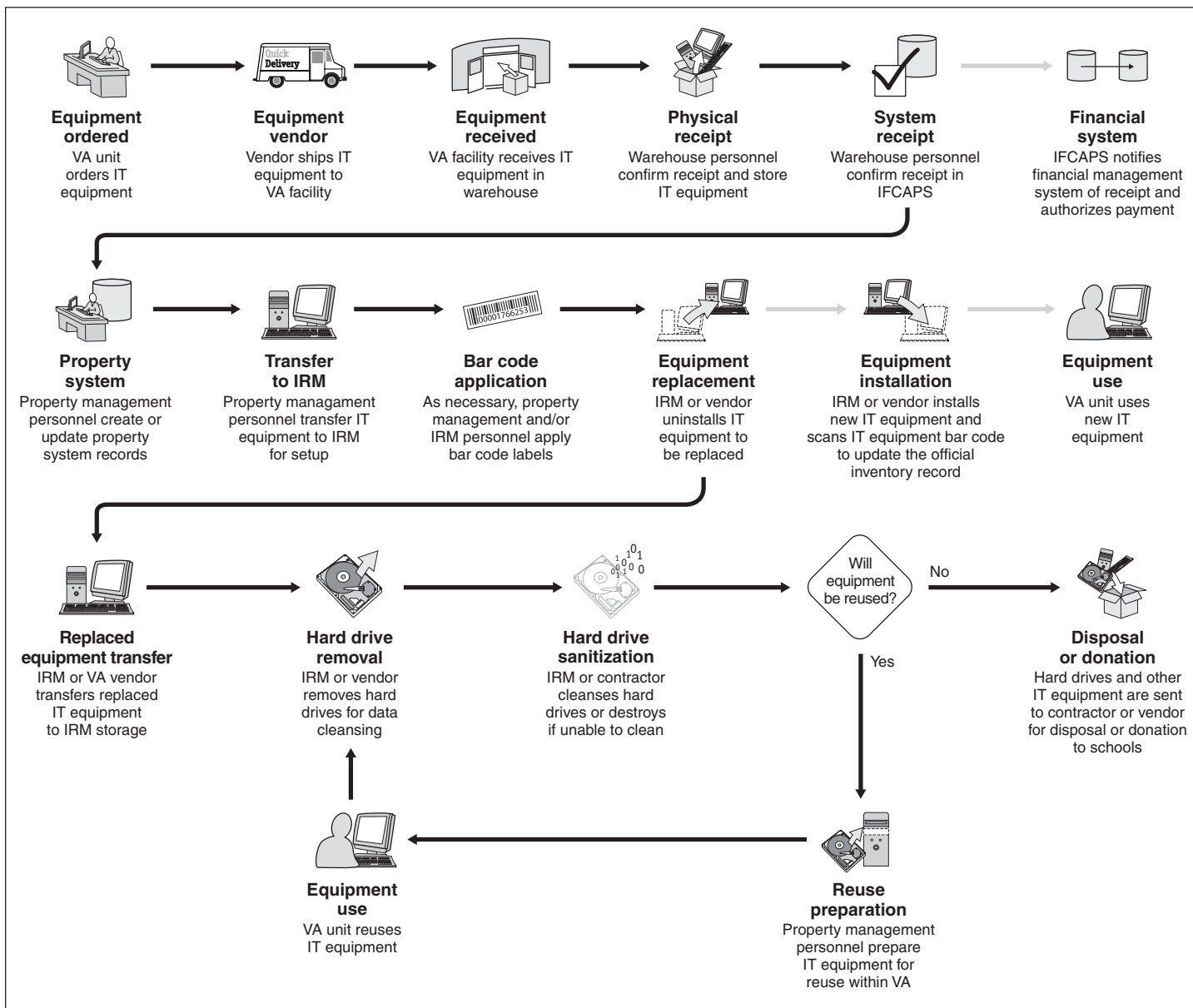
Our July 2004 report found significant property management weaknesses, including weaknesses in controls over IT equipment items valued at under \$5,000 that are required to have inventory control. In that report, we made several recommendations for improving property management, including actions to (1) clarify existing policy regarding sensitive items that are required to be accounted for in the property control records, (2) provide a more comprehensive list of the type of personal property assets that are considered sensitive for accountability purposes, and (3) reinforce VA's requirement to attach bar code labels to agency personal property.

VA's IT Property Management Process

The Assistant Secretary for Information and Technology serves as the CIO for the department and is the principal advisor to the Secretary on matters relating to IT management in the department. Key functions in VA's IT property management process are performed by IRM and property management personnel. These functions include identifying requirements; ordering, receiving, and installing IT equipment; performing periodic inventories; and identifying, removing, and disposing of obsolete and unneeded IT equipment. Figure 1 illustrates the IT property management

process. In general, this is the process we observed at the four VA locations we audited.

Figure 1: VA's IT Property Management Process



Source: GAO.

Request and Ordering of IT Equipment

The steps in the IT property management process are key events, which should be documented by an inventory transaction, 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.¹⁵

IRM personnel determine IT equipment requirements for a particular VA medical center or headquarters office based on strategic planning, medical center or office needs, specific requests, and budgetary resources. IRM personnel then submit requests to the cognizant Veterans Integrated Service Network (VISN),¹⁶ the CIO, and VA headquarters in Washington, D.C., for approval. For VA medical centers, the VISN generally purchases or leases IT equipment to realize economies of scale, but individual medical centers also may place incidental orders to meet their needs. In addition, headquarters offices may place individual orders or use purchase cards to acquire IT equipment. Medical equipment with IT capability is generally acquired through procurement contracts. When contracting personnel create a purchase order and submit it to the vendor, contracting personnel are required to send a copy of the purchase order to the appropriate property management personnel to notify them of a new order.

When the vendor delivers ordered IT equipment to the loading dock, property management warehouse personnel inspect the boxes for visible signs of damage, and after accepting delivery, store IT equipment until they can transfer it to IRM personnel. Warehouse personnel confirm receipt and acceptance in the Integrated Funds Distribution Control Point Activity, Accounting, and Procurement System (IFCAPS), which then notifies the Financial Management System so that payment can be made to the vendor. Once the receipt is confirmed within IFCAPS, warehouse personnel notify IRM personnel of the delivery and arrange a transfer of

¹⁵ 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](#).

¹⁶ VHA has 21 VISNs that oversee medical center activities within their area, which may cover one or more states.

the equipment to them. Upon transfer, an IRM official signs the receipt document, signifying acceptance of custody for the IT equipment.

Recording of IT Equipment Acquisitions in Inventory Records

VA medical center property management personnel use information from the purchase order, including item name, item description, model number, manufacturer, vendor, and acquisition cost, to create property record(s) in the Automated Equipment Management System/Medical Equipment Repair Service (AEMS/MERS) for new IT equipment acquisitions.¹⁷ AEMS/MERS is a general inventory management system that is local to each VA medical center. Headquarters personnel also use purchase order information to enter records of new IT equipment in the Inte-Great™ Property Manager system. Property management personnel also identify the department responsible for the IT equipment by recording an equipment inventory listing (EIL) code at VA medical centers and a consolidated memorandum receipt (CMR) code at headquarters. Once property records are created, property management personnel generate a bar code label for each piece of IT equipment. IRM personnel may prepare the equipment for issuance to specific users by installing VA-specific software and configurations prior to installation. In addition, VA medical center biomedical engineering personnel may test medical equipment for electrical safety before placing it in service.

Issuance and Replacement of IT Equipment

IRM personnel or, in some cases, contractor personnel deliver new IT equipment to the appropriate service or location for installation. IRM or contractor personnel also remove and replace old IT equipment that has been approved for replacement. At some VA facilities, a bar code label is affixed to a door jam or other physical element of the specific location in which the IT equipment has been installed to document item locations in the property management system. Once the new equipment is installed, IRM or contractor personnel transfer the replaced equipment to an IRM storage room pending disposal.

¹⁷ VA Handbook 7127, *Materiel Management Procedures* (Sept. 19, 1995), required that all sensitive items, including those valued under \$5,000, be inventoried regardless of cost. According to VA Handbook 7127/1 (Oct. 21, 1997), records of property costing \$5,000 or greater will be maintained in AMES/MERS. In addition to assets valued over \$5,000, VA Handbook 7124/4 (Oct. 11, 2005) added a further explanation that sensitive items include handheld and portable telecommunication devices, printers, data storage equipment (e.g., desktop and laptop computers), video imaging equipment, cell phones, radios, motor vehicles, and firearms and ammunition.

Physical Inventories of IT Equipment and Reports of Survey

VA policy¹⁸ mandates that each VA facility take physical inventory of its accountable property using one of two methods. The first method determines when the next inventory will be taken based on the accuracy rate for each EIL or CMR during the previous inventory. If an EIL or CMR was found to have an accuracy rate of 95 percent or above, the VA facility may inventory that EIL or CMR in 12 months. If the EIL or CMR has an accuracy rate of less than 95 percent, the VA facility must inventory that EIL or CMR within 6 months. The second method permits physical inventories to be performed on an exception basis. Under this method, a VA facility uses property management system data to identify the item bar codes that were scanned since the last inventory. If items have been scanned since the last inventory, they may be excluded from the current physical inventory.

When a VA facility determines that items listed in inventory cannot be located, those items are listed on a Report of Survey and facility personnel convene a Board of Survey. Reports of Survey are provided to medical center VA Police or the Federal Protective Service officers at VA headquarters, as appropriate. The Report of Survey documents the circumstances of loss, damage, or destruction of government property. VA policy¹⁹ mandates that a Board of Survey be appointed when there is a possibility that a VA employee may be assessed pecuniary liability or disciplinary action as a result of loss, damage, or destruction of property and the value of the property involved is \$5,000 or more. The Board of Survey reviews the Report of Survey, which identifies IT equipment that is unaccounted for and explains efforts made to account for the missing items. An approved Report of Survey provides necessary support for writing off lost and missing items. For items on the Report of Survey, VA personnel are supposed to update the use status in the property management system from “in-use” to “lost.” Updating the use status allows for the generation of an exception report in case any of the items unaccounted for are subsequently located.

Approval for Turn-in and Disposal

An IRM technician originates the request for turn-in of old IT equipment using VA Form 2237, “Request, Turn-In, and Receipt for Property or Services,” or users may submit an electronic form 2237. Pending final approval of VA Form 2237, electronic notification is given to property management and IRM personnel, who use this documentation to ensure

¹⁸ VA Handbook 7127/4, *Materiel Management Procedures* (Oct. 11, 2005).

¹⁹ VA Handbook 7125, *Materiel Management General Procedures*, pt. 5, § 5101-8.

that they are removing and disposing of the correct item(s). IRM or contractor personnel transfer the old IT equipment to an IRM storage room for hard drive sanitization and subsequent reuse or disposal. Medical equipment with IT capability is generally traded in to the vendor for upgraded models after medical center IRM personnel have documented that data sanitization procedures were completed.

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 1974²⁰ and, when information concerns an individual's health, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and implementing regulations.²¹

Removal of Data from Hard Drives

VA facilities have two options for removing data from hard drives of IT equipment in the excess property disposal process. Under the first option, the VA medical center removes the hard drives from the IT equipment and ships them to a vendor for sanitization (data erasing). The vendor physically destroys any hard drives it cannot successfully erase. The vendor submits certification of hard drive sanitization or destruction to IRM personnel and ships the sanitized hard drives back to the VA facility for disposal. Under the second option, VA IRM personnel perform the procedures to sanitize the hard drives using VA-approved software, such as Data EraserTM. IRM personnel complete VA Form 0751, "Information Technology Equipment Sanitization Certification," to document the erasing of the hard drives. Hard drives that Data EraserTM software cannot successfully sanitize are held at the VA facility in IRM storage for physical destruction by another contractor at various intervals throughout the year.

Final Disposition of IT Equipment

After data have been removed from the hard drives, the hard drives can be placed back into the IT equipment from which they were previously

²⁰ Privacy Act of 1974, *codified, as amended*, at 5 U.S.C. § 552a.

²¹ HIPAA required the Secretary of Health and Human Services (HHS) to submit to Congress detailed recommendations on standards related to the privacy of individually identifiable health information, including an individual's rights with respect to such information, procedures for an individual to exercise those rights, and the authorized uses and disclosures of such information by others, such as health care providers and insurers. The HHS Secretary has prescribed such standards in the HIPAA Medical Privacy Rule. *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.

removed so that the computers can be reused or shipped directly to a VA IT equipment disposal vendor. For IT equipment that is not selected for reuse within VA, IRM personnel will notify cognizant property management personnel that the IT equipment is ready for final disposal and property management personnel transfer the items to a warehouse. VA facilities use different processes to handle the final disposal of IT equipment. For example, property management personnel may contact transportation personnel at the VA Central Office, who then contact a shipper to take the IT equipment to a disposal vendor, or a disposal vendor may pick up the IT equipment from the VA facility. Disposal vendors, including Federal Prison Industries, Inc.,²² determine what IT equipment is to be donated to schools. Generally, within several days of the equipment being shipped to the disposal vendor, property management personnel change the status field of the equipment in the property management system from “in-use” to “turned-in” and designate the property record as inactive.

Inadequate IT Inventory Control and Accountability Pose Risk of Loss, Theft, and Misappropriation

Our tests of IT equipment inventory controls at four case study locations, including three VA medical centers and VA headquarters, identified a weak overall control environment and a pervasive lack of accountability for IT equipment items across the four locations we tested. Our *Standards for Internal Control in the Federal Government*²³ states that a positive control environment provides discipline and structure as well as the climate that influences the quality of internal control. However, as summarized in table 1, our statistical tests of key IT inventory controls at our four case study locations found significant control failures related to (1) missing IT equipment items in our existence tests, (2) inaccurate information on user organization, (3) inaccurate information on user location, and (4) other recordkeeping errors. None of the case study locations had effective controls to safeguard IT assets from risk of loss, theft, and misappropriation.

²² Federal Prison Industries, Inc. (also known as UNICOR) is a wholly owned U.S. government corporation, which operates factories and employs inmates in federal prisons. See 31 U.S.C. § 9101 (3)(E), 18 U.S.C. §§ 4121-4129.

²³ [GAO/AIMD-00-21.3.1](#).

Table 1: Current IT Equipment Inventory Control Failure Rates at Four Test Locations

| Control failures | Washington, D.C., medical center | Indianapolis medical center | San Diego medical center | VA headquarters |
|-----------------------------|---|--|---|----------------------------|
| Missing items in sample | 28% | 6% | 10% | 11% |
| Incorrect user organization | 80% | 69% | 70% | 11% |
| Incorrect user location | 57% | 23% | 53% | 44% |
| Recordkeeping errors | 5% | 0% | 5% | 3% |

Source: GAO analysis.

Notes: Each of these estimates has 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 app. 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 and not the population of all IT equipment at those locations.

Moreover, our statistical tests identified a total of 123 lost and missing IT equipment items across the four case locations, including 53 IT equipment items that could have stored sensitive personal information. Personal information, such as names and Social Security numbers, is regulated by privacy protections under the Privacy Act of 1974²⁴ and information concerning an individual’s health is accorded additional protections from unauthorized release under HIPAA and implementing regulations.²⁵ Although VA property management policy²⁶ establishes guidelines for holding employees and supervisors pecuniarily (financially) liable for loss, damage, or destruction because of negligence and misuse of government property, except for a few isolated instances, none of the case study locations assigned user-level accountability. Instead, these locations relied on information about user organization and user location, which was often incorrect and incomplete. In addition, although our standards for internal control require timely recording of transactions as part of an effective internal control structure and safeguarding of sensitive assets, we found

²⁴ Privacy Act of 1974, *codified, as amended*, at 5 U.S.C. § 552a.

²⁵ The HHS Secretary has prescribed standards for safeguarding medical information in the HIPAA Medical Privacy Rule. *See* 45 C.F.R. pt. 164.

²⁶ VA Handbook 7125, *Materiel Management General Procedures*, § 5003 (Oct. 11, 2005).

that VA's property management policy²⁷ neither specified what transactions were to be recorded for various changes in inventory status nor provided criteria for timely recording. Further, IRM and IT Services personnel responsible for installation, removal, and disposal of IT equipment did not record or assure that transactions were recorded by property management officials when these events occurred. Under this lax control environment, missing IT equipment items were often not reported for several months and, in some cases several years, until the problem was identified during a physical inventory.

Inventory Tests Identified Significant Numbers of Missing Items

As shown in table 2, our statistical tests of IT equipment existence at the four case study locations identified a total of 123 missing IT equipment items, including 53 items that could have stored sensitive personal data and information. Although VA headquarters had the highest number of missing items, none of the four test locations had effective controls. Missing IT equipment items pose not only a financial risk but also a security risk associated with sensitive personal data maintained on computer hard drives.

Table 2: Number of Missing IT Equipment Items at Four Test Locations, Including Items That Could Have Stored Sensitive Information

| Test results | Washington, D.C., medical center | Indianapolis medical center | San Diego medical Center | VA headquarters |
|---|-------------------------------------|-----------------------------------|--------------------------------|--------------------|
| Number of missing items in each sample | 44 | 9 | 17 | 53 |
| Total missing items that could have stored sensitive data | 19 | 3 | 8 | 23 |

Source: GAO analysis.

Note: After we completed our analysis, Washington, D.C., medical center personnel provided documentation that one of the missing items—a new computer monitor—had been located. This information is not reflected in the table.

Because of the lack of user-level accountability and the failure to consistently update inventory records for changes in inventory status and user location, VA officials at our test locations could not determine the

²⁷ VA Handbook 7127/3, *Material Management Procedures*, pt. 1 § 5002-2.3, and VA Handbook 7127/4, *Material Management Procedures*, pt. 4, § 5302.3.

Washington, D.C., Medical Center

user or type of data stored on the 53 missing IT equipment items that could have stored sensitive personal information and, therefore, the risk posed by the loss of these items. The details of our test work at each location follow.

Our physical inventory existence testing at the Washington, D.C., medical center identified an estimated 28 percent failure rate²⁸ related to missing items in the recorded universe of 8,728 IT equipment items. Our analysis determined that the primary cause of these high control failure rates was a lack of coordination and communication between medical center IRM and property management personnel to assure that documentation on IT items in physical inventory was updated in the property management system when changes occurred. VA records management policy²⁹ that implements federal records management law and NARA guidance³⁰ requires the creation and maintenance of records of essential transactions, such as creating a timely record of newly acquired IT equipment in the property management system, and recording timely updates for changes in the status of IT equipment, including transfers, turn-ins, and replacement of equipment, and disposals.

The medical center's IT equipment inventory records included 550 older IT equipment items that property management officials told us should have been removed from active inventory. Because the inventory status fields for these items were either blank or indicated the items were "in use," we included these items in the universe of current inventory for purposes of our statistical sample. Of the 44 missing IT equipment items identified in our statistical tests at the Washington, D.C., medical center, 9 items related to the 550 older IT equipment items of questionable status. Washington, D.C., medical center officials asserted that because of their age, these items would likely have been turned in for disposal. However, because the property system had not been updated to reflect a turn-in or disposal and no hard copy documentation had been retained, it was not possible to determine whether any of the 44 missing IT equipment items, including 19

²⁸ The two-sided, 95 percent confidence interval for this estimate is from 21 percent to 35 percent.

²⁹ VA Directive 6300, *Records and Information Management*, § 2 (Jan. 12, 1998).

³⁰ 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 FMFIA, and [GAO/AIMD-00-21.3.1](#).

items that could have stored sensitive personal information, had been sent to disposal or if any of them were lost or stolen.

For other IT equipment items that could not be located during our existence testing, IRM or property management officials were able to provide documentation created and saved outside the property management system that showed several of these items had been turned in for disposal without recording the corresponding inventory transaction in the property management system. In March 2006, the Washington, D.C., medical center initiated an automated process for electronic notification and documentation of property turn-ins in the property management system. If effectively implemented, the electronic process should help resolve this problem going forward.

With regard to the use and type of data stored on the 19 computers that our tests identified as missing, Washington D.C., medical center officials could not tell us the users or the types of data that would have been on these computers. This is because local medical center property management procedures call for recording the local IRM organization as the user for most IT equipment in the property management system, rather than the actual custodian or user of the IT equipment.

Indianapolis Medical Center

The Indianapolis medical center had an estimated failure rate of 6 percent³¹ related to missing items in the recorded universe of 7,614 IT equipment items. However, our test results do not allow us to conclude that the center's controls over existence of IT equipment inventory are effective. Our statistical tests identified 9 missing IT equipment items, including 3 items that could have stored sensitive personal and medical information. Of the 3 missing items that could have stored sensitive information, medical center inventory records showed that 2 of these items were medical devices assigned to the radiology unit. Although medical center officials provided us with turn-in documentation for one of these items—a magnetic resonance imaging (MRI) machine that had just been disassembled and removed from service—the documentation did not match the bar code (property identification number) or the serial number for our sample item, indicating possible recordkeeping errors. The user of the third item, a computer, was not known.

³¹ The two-sided, 95 percent confidence interval for this estimate is from 2 percent to 13 percent.

In addition, our review of Indianapolis medical center purchase card records determined that some IT equipment items that were not included in property inventory records had been acquired with a government purchase card. We found that VA purchase card policy³² does not require cardholders to notify property management officials of the receipt of property items acquired with a purchase card, including IT equipment. As a result, there is no asset visibility³³ or accountability for these items. Further, there is no assurance that sensitive personal data, medical data, or both that could be stored on these items are properly safeguarded.

San Diego Medical Center

We estimated an overall failure rate of 10 percent³⁴ related to missing items in the San Diego medical center's recorded universe of 11,604 IT equipment items. Our statistical tests at the San Diego medical center identified 17 missing IT equipment items, including 8 items that could have stored sensitive personal data and information. San Diego medical center officials could not tell us the user or type of data that would have been stored on the missing computers. San Diego medical center officials noted that some of the missing items were older IT equipment that would no longer be in use. However, without valid turn-in documentation, it is not possible to determine whether these IT equipment items were disposed of without creating the appropriate transaction record or if any of these items, including items that could have stored sensitive personal and medical information, were lost, stolen, or misappropriated without detection.

Our tests also determined that San Diego medical center officials were not following VA policy for physical inventory control and accountability of IT equipment. Consistent with a finding in our July 2004 report, we found that the San Diego medical center had not included IT equipment items valued at less than \$5,000 in annual physical inventories. Although San Diego medical center property management officials record IT equipment ordered through the formal property acquisition process in inventory records at the time it is acquired, absent an annual physical inventory, center officials have no way of knowing whether these items are still in

³² VA Handbook 1730/1, *Use and Management of the Government Purchase Card Program* (June 17, 2005).

³³ Asset visibility refers to accurate and timely information on the location, movement, status, and identifying information for property and equipment assets.

³⁴ The two-sided, 95 percent confidence interval for this estimate is from 5 percent to 17 percent.

use or if any of these items were lost, stolen, or misappropriated. VA property management policy³⁵ requires that sensitive items, including computer equipment, be subjected to annual physical inventories. At the time of our IT equipment inventory testing in January 2007, San Diego medical center officials told us that consistent with requirements in VA Handbook 7127/4, they were initiating a physical inventory of all IT equipment items, including those items valued at less than \$5,000.

In addition, our analysis of San Diego medical center purchase card records identified several purchases of IT equipment that had not been recorded in the medical center's inventory records. As a result, our statistical tests did not include these items. Because the medical center's IT Services and property management officials are not tracking IT equipment items that were acquired with government purchase cards, there is no accountability for these items. As a result, San Diego medical center management does not know how many of these items have not been recorded in the property inventory records or how many of these items could contain sensitive personal information. If San Diego medical center officials properly perform their fiscal year 2007 physical inventory, they should be able to locate and establish an accountable record for IT equipment items acquired with purchase cards that are being used within their facility. However, additional research would be required to identify all IT equipment items that were acquired with a purchase card and are being used at employees' homes or other off-site locations.

San Diego medical center IT Services personnel told us that they created and maintained informal "cuff records" outside the property management system to document installation and removal of IT equipment because property management officials did not permit them to have access to the property management system. In addition, IT Services personnel did not provide information from their informal cuff records to property management officials so that they could update the formal records maintained in property management system. As a result, the formal IT equipment inventory records saved in the property management system remained out-of-date, while more accurate records were maintained as separate IT Services files outside the formal system and were not available for management decision making. Further, San Diego IT Services personnel were not provided handheld scanners so that they could

³⁵ VA Handbook 7127/4, *Material Management Procedures*, pt. 1, § 5002.2 and pt. 4, § 5302.3 (Oct. 11, 2005).

electronically update inventory records when they installed or removed IT equipment. The San Diego medical center IT Services' informal cuff records create internal control weaknesses because they do not provide reasonable assurance of furnishing information the agency needs to conduct current business.

VA Headquarters Offices

We statistically tested a random sample of VA headquarters IT equipment items, which included IT equipment for each headquarters office. Based on our sample, we estimate an 11 percent failure rate³⁶ related to missing items in the VA headquarters recorded universe of 25,353 IT equipment items. In addition, our tests of VA headquarters IT inventory identified 53 missing IT equipment items, including 23 computers that could have stored sensitive personal information. VA headquarters officials could not tell us the use or type of information that would have been stored on the missing computers. Table 3 identifies missing IT equipment items in our stratified sample by VA headquarters office.

Table 3: Number of Missing IT Equipment Items by Headquarters Office and Missing Items That Could Have Stored Sensitive Personal Data and Information

| Test location | Number of missing IT items in stratified sample | Missing items with data storage capability |
|----------------------------------|---|--|
| Acquisition and Materiel | 0 of 10 | 0 |
| General Counsel | 2 of 10 | 0 of 2 |
| Information and Technology | 9 of 94 | 6 of 9 |
| Policy and Planning | 0 of 10 | 0 |
| Veterans Health Administration | 17 of 95 | 7 of 17 |
| Veterans Benefits Administration | 24 of 93 | 10 of 24 |
| All other ^a | 1 of 32 | 0 of 1 |

Source: GAO analysis.

^aAll other includes 17 additional VA headquarters organizations. The missing item in this category related to the Human Resource Management Office.

We found that VA headquarters property records were incomplete and out-of-date, particularly with regard to users and locations. VA headquarters officials told us that IT coordinators had access to the headquarters property system for purposes of updating records for their units. However,

³⁶ The two-sided, 95 percent confidence interval for this estimate is from 8 percent to 15 percent.

we found that the IT coordinators maintained informal spreadsheets, or cuff records, to track IT equipment assigned to their units instead of updating IT equipment records in the formal VA headquarters property system. As stated previously, the use of informal cuff records creates an internal control weakness because management does not have visibility over this information for decision making purposes.

VA headquarters officials also told us that various headquarters offices acquire IT equipment using government purchase cards and that these items are not identified and recorded in inventory unless they are observed coming through the mail room or they are identified during physical inventories. As previously discussed, VA purchase card policy does not require purchase card holders to notify property management officials at the time they receive IT equipment and other property acquired with government purchase cards.

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

VA management has not enforced VA property management policy and has generally left implementation decisions up to local organizations, creating a nonstandard, high-risk environment. Although VA property management policy establishes guidelines for user-level accountability,³⁷ the three medical centers we tested assigned accountability for most IT equipment to their IRM or IT Services organizations, and VA headquarters organizations tracked IT equipment items through their IT inventory coordinators. However, because these IT personnel and IT coordinators did not have possession (physical custody) of all IT equipment under their purview, they were not held accountable for IT equipment determined to be missing during physical inventories. This weak overall control environment at the four case study locations resulted in a pervasive lack of user-level accountability for IT equipment.

Absent user-level accountability, accurate information on the using organization and location of IT equipment is key to maintaining asset visibility and control over IT equipment items. The high failure rates in our tests for correct user organization and location of IT equipment, shown in table 4, underscore the lack of user-level accountability at the four case study locations. The lack of accountability has in turn resulted in a lax attitude about controlling IT equipment. As a result, for the four case study

³⁷ VA Handbook 7125, *Materiel Management General Procedures*, § 5003.

locations, we concluded that under the current lax control environment, essentially no one was accountable for IT equipment.

Table 4: Estimated Percentage of IT Inventory Control Failures Related to Correct User and Location at the Four Test Locations

| Test location | Incorrect user organization | Incorrect user location |
|----------------------------------|-----------------------------|-------------------------|
| Washington, DC, medical center | 80% (72% to 87%) | 57% (49% to 64%) |
| Indianapolis, IN, medical center | 69% (60% to 78%) | 23% (15% to 33%) |
| San Diego, CA, medical center | 70% (61% to 78%) | 53% (43% to 63%) |
| VA headquarters organizations | 11% (8% to 15%) | 44% (37% to 51%) |

Source: GAO analysis.

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

Our statistical tests found numerous instances where inventory records were not updated when equipment was transferred to another VA unit, moved to another location, or removed from a facility. We also found that critical inventory system data fields, such as user and location, were often blank. Completion of these data fields would have created records of essential transactions for IT inventory events. Because property management system inventory records were incomplete and out-of-date, it is not possible to determine the timing or events associated with lost IT equipment as a basis for holding individual employees accountable.

In addition to failures in our tests for accurate user organization and location, we found that the inventory system data field for identifying IT coordinators at headquarters units was often blank or incorrect. The IT coordinator role, which is unique to VA headquarters offices, is intended to provide an additional level of control for tracking and managing assignment of IT equipment within each headquarters organizational unit. Our tests for accurate and complete information on headquarters IT coordinators found 85 errors out of a sample of 344 records tested. We estimated the failure rate for the IT coordinator records at VA headquarters units to be 47 percent.³⁸ Further, although VA headquarters

³⁸ The margin of error, based on a two-sided, 95 percent confidence interval is +/- 3 percent.

officials told us they use hand receipts³⁹ for 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, we found this procedure was not used consistently. For example, we requested hand receipts for 15 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 9 hand receipts—1 that had expired, 6 that were dated after the date of our request, and 2 that were valid. Officials at the three medical centers we tested were able to provide hand receipts for IT equipment that was being used by their employees at home.

Officials at all four case study locations expressed concerns that it would be difficult and burdensome to implement user-level accountability for IT equipment, particularly in the case of shared workstations used by multiple employees. However, Washington, D.C., medical center officials initiated actions to establish user-level accountability for individual employees and unit heads who have shared workstations. In March 2007, Washington, D.C., medical center officials implemented a policy for user-level accountability and began training their employees on the new requirements. The new policy requires employees to sign personal custody receipts for IT equipment assigned to them, and it requires supervisors to be responsible for IT equipment that is shared among staff in their sections. The policy states that users of IT equipment will be held accountable for acts deemed inappropriate or negligent and that employees are personally and financially responsible for loss, theft, damage, or destruction of government property caused by negligence. VA headquarters officials told us that they are considering approaches for implementing a VA-wide policy for user-level accountability of IT equipment.

Errors in IT Equipment Inventory Status and Item Description Information

As shown in table 5, we also found some problems with the accuracy of IT equipment inventory records, including inaccurate information on status (e.g., in use, turned-in, disposal), serial numbers, model numbers, and item descriptions. The estimated overall error rates for these tests were lower than the error rates for the other control attributes we tested, and the Indianapolis medical center had no errors.

³⁹ A hand receipt is a document used to assign individual custody of a government-furnished equipment item. At VA headquarters a hand receipt includes the description and bar code number of the item, and it is signed by the employee responsible for the equipment and an authorizing official.

Table 5: Estimated Percentage of Other IT Inventory Recordkeeping Failures at Four Test Locations

| Test location | Inventory status information | Serial number | Item description | Total failures |
|----------------------------------|------------------------------|-------------------|------------------|-------------------|
| Washington, D.C., medical center | 1% (0% to 4%) | 6% (2% to 11%) | 0% (0% to 5%) | 5% (2% to 10%) |
| Indianapolis medical center | 0% (0% to 2%) | 0% (0% to 4%) | 0% (0% to 2%) | 0% (0% to 4%) |
| San Diego medical center | 2% (0% to 7%) | 1% (0% to 6%) | 2% (0% to 8%) | 5% (2% to 12%) |
| VA headquarters organizations | 0% (0% to 2%) | 2% (1% to 7%) | 1% (0% to 2%) | 3% (1% to 6%) |

Source: GAO analysis.

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

The errors we identified affect management decision making and create waste and inefficiency in operations. For example, inaccurate information on the status of IT equipment inventory items impairs management’s ability to determine what items are available or in use. Errors in item descriptions impair management decision making on the number and types of available items and timing for replacement of these items, and serial number errors impair accountability. Further, inaccurate inventory information on the IT equipment item status, as well as the location errors discussed above, caused significant waste and inefficiency during physical inventories. Many of these errors should have been detected and corrected during annual physical inventories.

Physical Inventories by
Case Study Locations
Identified Thousands of
Missing IT Equipment
Items Valued at Millions of
Dollars

To assess the effect of the lax control environment for IT equipment, we asked VA officials at the case study locations covered in both our current and previous audits to provide us with information on the results of their physical inventories performed after issuance of recommendations in our July 2004 report, including Reports of Survey⁴⁰ information on identified losses of IT equipment. VA policy⁴¹ requires that when property items are determined to be lost or missing, they are to be listed in a Report of Survey and an investigation is to be conducted into the circumstances of the loss before these items are written off in the property records. As of February 28, 2007, the four case study locations covered in our current audit reported over 2,400 missing IT equipment items with a combined original acquisition value of about \$6.4 million as a result of inventories they performed during fiscal years 2005 and 2006. Based on information obtained through March 2, 2007, the five case study locations we previously audited had identified over 8,600 missing IT equipment items with a combined original acquisition value of over \$13.2 million. Because inventory records were not consistently updated as changes in user organization or location occurred and none of the locations we audited required accountability at the user level, it is not possible to determine whether the missing IT equipment items represent recordkeeping errors or the loss, theft, or misappropriation of IT equipment. Further, missing IT equipment items were often not reported for several months and, in some cases several years, because most of the nine case study locations had not consistently performed required annual physical inventories or completed Reports of Survey promptly. Although physical inventories should be performed over a finite period, at most of the nine case study locations these inventories were not completed for several months or even several years while officials performed extensive searches in an attempt to locate missing items before preparing Reports of Survey to write them off.

⁴⁰ 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.

⁴¹ VA Handbook 7125, *Materiel Management General Procedures*, pt. 5, § 5101 and § 5101-21.

According to VA Police and security specialists,⁴² it is very difficult to conduct an investigation at this point because the details of the incidents cannot be determined. As law enforcement officers, VA Police are trained in investigative techniques that could potentially track and recover lost and missing items if promptly reported. Further, because VA Police are responsible for facility security, consistent reporting of lost and missing IT equipment to the Chief of Police at each VA medical center or federal law enforcement officers responsible for building security at VA headquarters locations could identify patterns of vulnerability that could be addressed through upgraded security plans.

Physical Inventories Performed by Four Case Study Locations Identify Significant Numbers of Missing IT Equipment Items

The timing and scope of the physical inventories performed by the four case study locations in our current audit varied. For example, the Indianapolis medical center had been performing annual physical inventories in accordance with VA policy for several years. As a result, IT equipment inventory records were more accurate and physical inventories identified fewer missing items than most locations tested. The Washington, D.C., medical center performed a wall-to-wall physical inventory in response to our July 2004 report, which found that previously performed physical inventories of IT equipment were ineffective. In this case, inventory results reflected several years of activity involving IT inventory records that had not been updated and lost and missing IT equipment items that had not previously been identified and reported. Although the San Diego medical center had performed periodic physical inventories, it had not followed VA policy for including sensitive items, such as IT equipment valued at less than \$5,000. As a result, the San Diego medical center's Reports of Survey are not a good indicator of the extent of lost and missing IT equipment at this location. The fiscal year 2006 VA headquarters physical inventory identified IT equipment items that may have been lost or missing for several years without detection or final resolution. For example, VA headquarters officials told us that during renovations of headquarters offices 10 years ago, IT equipment was relocated to office space designated as storerooms. When this space had to be vacated for renovation, the IT equipment had to be relocated, and many items were sent to disposal. According to VA headquarters officials,

⁴² VA medical centers and other facilities have a VA Police Service, which provides law enforcement and physical security services, including security inspections and criminal investigations. The VA headquarters building does not have a police service. VA headquarters law enforcement duties are the responsibility of the Federal Protective Service.

accountability for individual IT equipment items was not maintained during the renovation or disposal process. This weak overall control environment presents an opportunity for theft, loss, or misappropriation to occur without detection.

As of February 28, 2007, based on inventories they performed during fiscal years 2005 and 2006, the four case study locations covered in our current audit reported over 2,400 missing IT equipment items with a combined original acquisition value of about \$6.4 million. Table 6 provides information on the results of physical inventories performed by our four current case study locations.

Table 6: Summary of Physical Inventories and Missing IT Equipment Identified by the Four Current Case Study Locations as of February 28, 2007

| Test location | Fiscal years of inventory | Dates of Reports of Survey | Number of missing items identified | Original acquisition value of missing items |
|---------------------------------------|---------------------------|----------------------------|------------------------------------|---|
| Washington, D.C., medical center | 2005 thru 2006 | Mar. 2006 thru Oct. 2006 | 1,133 | \$1,758,096 |
| Indianapolis medical center | 2005 | Dec. 2004 | 6 | \$23,206 |
| | 2006 | Oct. 2006 | 112 | \$79,230 |
| San Diego medical center ^a | 2005 | Dec. 2004 | 42 | \$135,344 |
| | 2006 | Ongoing | 15 | \$24,418 |
| VA headquarters offices | 2006 and ongoing | Not yet finalized | 1,162 | \$4,385,444 |

Source: GAO analysis.

^aThe San Diego medical center IT Services personnel inventoried only items valued at \$5,000 or more.

In response to our test work, in January 2007, the Washington, D.C., medical center prepared an additional Report of Survey to write off 699 older IT equipment items valued at \$794,835 that had not been located or removed from current inventory. The VA headquarters physical inventory had initially identified about 2,700 missing IT equipment items, and officials told us that their research has resolved over half of the discrepancies. VA headquarters officials told us that they have not yet prepared a Report of Survey because they believe some of their missing IT equipment items may still be located.

**Physical Inventories by
Five Locations Previously
Audited Also Identify
Significant Numbers of
Missing IT Equipment
Items**

We also followed up with the five other case study locations⁴³ that we previously audited to determine the results of physical inventories performed in response to recommendations in our July 2004 report. As of the end of our fieldwork in February 2007, the Tampa, Florida, medical center had not yet completed its physical inventory. In addition, the Houston, Texas, medical center's fiscal year 2005 physical inventory procedures continued to exclude IT equipment valued under \$5,000 because the center had followed inaccurate guidance from its VISN.

Our standards for internal control require federal agencies to have policies and procedures for ensuring that the findings of audits and other reviews are promptly resolved. In accordance with these standards, managers are to (1) promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations; (2) determine proper actions in response to findings and recommendations; and (3) complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. The failure to ensure that VA organizations take appropriate, timely action to address audit findings and recommendations indicates a significant control environment weakness with regard to a "tone at the top" and does not set an example that supports performance-based management and establishes controls that serve as the first line of defense in safeguarding assets and preventing and detecting errors.

Based on information obtained through March 2, 2007, the five case study locations we previously audited had identified over 8,600 missing IT equipment items with a combined original acquisition value of over \$13.2 million. As noted in table 7, of the three medical centers that completed their physical inventories, the Los Angeles, California, medical center reported over 8,400 missing IT equipment items valued at over \$12.4 million.

⁴³ The Washington, D.C., medical center was covered in both audits.

Table 7: Summary of Physical Inventories and Missing IT Equipment Identified by Five Case Study Locations Previously Audited as of March 2, 2007

| Medical center test location | Fiscal year of inventory | Dates of Reports of Survey | Number of missing items | Original acquisition value of missing items |
|------------------------------|--------------------------|----------------------------|-------------------------|---|
| Atlanta, GA | Ongoing since 2005 | Not yet prepared | 195 | \$254,666 |
| Houston, TX ^a | 2005 | Mar. 2005 | 3 | \$79,703 |
| Los Angeles, CA | 2006 | Not yet prepared | 8,402 | \$12,424,860 |
| San Francisco, CA | 2005 | Oct. 2004 thru Dec. 2005 | 68 | \$463,373 |
| Tampa, FL | Ongoing since Jan. 2006 | Not yet prepared | Unknown | Unknown |

Source: GAO analysis.

^aThe Houston medical center inventoried only items valued at \$5,000 or more.

We found that Houston medical center property management policy did not include IT equipment within its definition of sensitive items requiring annual physical inventories. As a result, the Houston medical center inventoried items valued at \$5,000 or more and reported 3 missing IT equipment items valued at \$79,703. Houston medical center officials told us that they are now complying with VA policy to include all IT equipment in their current annual physical inventory effort. The Atlanta medical center identified 195 missing IT equipment items valued at \$254,666, and the San Francisco medical center reported a total of 68 missing IT equipment items valued at \$463,373. Three of the five medical centers—in Atlanta, Los Angeles, and Tampa—had not yet prepared Reports of Survey on the missing items identified in their physical inventories.

Physical Security Weaknesses Increase Risk of Loss, Theft, and Misappropriation of IT Equipment and Sensitive Data

Our investigator’s inspection of physical security at officially designated IT warehouses and storerooms that held new and used IT equipment found that most of these storage facilities met the requirements in VA Handbook 0730/1, *Security and Law Enforcement*. However, not all of the formally designated storage locations had required motion detection alarm systems and special door locks. In response to our findings, physical security specialists at the four case study locations told us that they had recommended that the needed mechanisms be installed. We also found numerous instances of IT equipment storage areas at VA headquarters offices that had not been formally designated as IT storerooms, and these informal IT storage areas did not meet VA physical security requirements.

In addition, 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 that pose a risk of data breach.⁴⁴ For example, our tests of computer hard drives in the excess property disposal process found that hard drives at two of the four case study locations that had not yet been sanitized contained hundreds of names and Social Security numbers. We also found that some of the hard drives had been in the disposal process for several years without being sanitized, creating an unnecessary risk that sensitive personal information protected under the Privacy Act of 1974⁴⁵ and personal medical information accorded additional protections under HIPAA⁴⁶ could be compromised. Weaknesses in physical security heighten the risk of data breach related to sensitive personal information residing on hard drives in the property disposal process that have not yet been sanitized.

Weaknesses in Procedures for Controlling Excess Computer Hard Drives

As previously discussed, VA requires that hard drives of excess computers be sanitized prior to reuse or disposal because they can store sensitive personal and medical information used in VA programs and activities, which could be compromised or used for unauthorized purposes. For example, our limited tests of excess computer hard drives in the disposal process that had not yet been sanitized found 419 unique names and Social Security numbers on three of the six Board of Veterans Appeals hard drives and one record on one of two VHA hard drives we tested. Our tests of five San Diego medical center hard drives that had not yet been sanitized found that one hard drive held at least 20 detailed patient medical histories, including 5 histories that contained Social Security numbers. Our limited tests of hard drives that were identified as having been subjected to internal or contractor data sanitization procedures did not find data remaining on these hard drives.

⁴⁴ VA IRM personnel and contractors follow NIST Special Publication 800-88 guidelines as well as more stringent DOD policy in DOD 5220.22-M, *National Industrial Security Program Operating Manual*, ch. 8, § 8-301, which requires performing three separate erasures for media sanitization.

⁴⁵ Privacy Act of 1974, *codified, as amended*, at 5 U.S.C. § 552a.

⁴⁶ Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033-34 (Aug. 21, 1996), and implementing regulations at 45 C.F.R. pt. 164.

However, our limited tests identified some problems that could pose a risk of data breach with regard to sensitive personal and medical information on hard drives in the disposal process that had not yet been sanitized. For example, our IT security specialist found that five hard drives stored in a bin labeled by the San Diego medical center as holding hard drives that had not been erased had in fact been sanitized. The lack of proper segregation and tracking of hard drives in the sanitization process poses a risk that some hard drives could make it through this process and be selected for reuse without having been sanitized. Further, based on the file dates on some of the computer hard drives that had not yet been sanitized at the San Diego and Indianapolis medical centers, our IT security specialist noted excessive delays—up to 6 years—in performing data sanitization once the computer systems had been identified for removal from use and disposal. Excessive delays in completing hard drive sanitization and disposal procedures pose an unnecessary risk when sensitive personal and medical information that is no longer needed is not removed from excess computer hard drives in a timely manner.

Physical Security Weaknesses at IT Storage Locations Pose Risk of Data Breach

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 to the underside of the slab (floor) above. IRM storerooms are required to have overhead barricades that prevent “up and over” access from adjacent rooms. Warehouse, IRM, 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. Intrusion detection alarms for storerooms outside facility grounds, such as outpatient clinics, are required to be connected remotely to a commercial security alarm monitoring firm, local police department, or security office charged with building security. Finally, IRM 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.

Most of the designated IT equipment storage facilities at the four case study locations met VA IT physical security requirements in VA Handbook 0730/1; however, we identified some deficiencies. For example, our investigator found that the Washington, D.C., and San Diego medical center IRM equipment storerooms lacked motion intrusion detection alarm systems and the Washington, D.C., medical center IRM storeroom did not meet door locking requirements. Based on our investigator’s

findings, physical security specialists at the San Diego and Washington, D.C., medical centers told us they have recommended that required intrusion detectors be installed in their IRM storerooms. In addition, the Washington, D.C., medical center reduced the number of keys to its IRM storerooms and changed storeroom locks to meet established requirements. Designated IT equipment storage facilities at the Indianapolis medical center met VA physical security requirements.

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, our investigator observed an IT workroom at the Indianapolis medical center where new IT equipment was placed on the floor. This room lacked a motion detection alarm system and the type of locking system prescribed in VA policy. Indianapolis VA Police told our investigator that such a level of security was not required for this room under VA policy, because it was not designated as a storeroom. In addition, at the VA headquarters building, our investigator found that the physical security specialist was unaware of the existence of IT equipment in some storerooms. Thus, these storerooms had not been subjected to required physical security inspections. VA Police and physical security specialists at our test locations agreed with our investigator's assessment that the physical security of these IT storerooms was inadequate.

During our statistical tests, we observed one IT equipment storeroom in the VA headquarters building IT Support Services area that had a separate wall, but no door. As shown in figure 2, the wall opening into the storeroom had yellow tape labeled "CAUTION" above the doorway. The store room was within an IT work area that had dropped ceilings that could provide "up and over" access from adjacent rooms, such as the employee store, and no alarm or intrusion detector. This storeroom did not meet VA's physical security requirements for motion intrusion detection and alarms and secure doors, locks, and special access keys.

Figure 2: Photograph of Unsecured IT Equipment Storeroom in the VA Headquarters Building



Source: GAO.

In another headquarters building, which housed VA's Office of General Counsel, we observed excess IT equipment, including computers with hard drives that had been awaiting turn-in and disposal for several months. This IT equipment was stacked in the corners of a large work area that had multiple doors and open access to numerous individuals, including vendors, contractors, employees, and others. Because our limited tests found sensitive personal data and information on hard drives that had not yet been sanitized, the failure to provide adequate security leaves this information vulnerable to data breach. Further, because software that can be used to image, or copy, this information is readily available, it is important to provide adequate security for these items. For example,

imaging software, such as “Foremost,” which was one of the imaging software products used by our IT security specialist, can be downloaded at no cost from the Internet and used to copy information from one hard drive to another in a few minutes. Thus, it is possible for a data breach to occur without theft of the IT equipment on which the data reside.

We also found that VA headquarters IT coordinators used storerooms and closets with office-type door locks to store IT equipment that was not currently in use. Other headquarters organizations stored laptops that were in the “loaner pool” for use by employees on travel or at home in locked filing cabinets in open areas. In addition, during our test work, we observed that very few IT equipment items had been secured by locked cables. Physical security of IT equipment is of particular concern at the VA medical centers because these centers provide open access to visitors, students, contractors, and others. The lack of secure storage leaves this IT equipment and any sensitive personal information stored on this equipment vulnerable to theft, loss, misappropriation, and data breach.

VA Actions to Improve IT Management and Controls Have Been Limited

Although VA has strengthened existing property management policy⁴⁷ in response to recommendations in our July 2004 report, issued several new policies to establish guidance and controls for IT security, and reorganized and centralized the IT function within the department under the CIO, these actions have not yet been fully implemented. For example, the CIO has no formal responsibility for medical equipment that stores or processes patient data. VA headquarters CIO officials agree that this is an area of vulnerability that needs to be addressed. In addition, the new CIO organization structure does not address roles or necessary coordination between IRM and property management personnel with regard to inventory control of sensitive IT equipment items. The Assistant Secretary for Information and Technology, who serves as the CIO, told us that his staff is aware of this problem and the new CIO organization structure includes a unit that will have responsibility for IT equipment asset management once it becomes operational. However, this unit has not yet been funded or staffed.

Regarding new policies, on October 11, 2005, VA revised its Handbook on materiel management procedures to emphasize that annual inventory requirements for sensitive items valued at under \$5,000 include IT

⁴⁷ VA Handbook 7127/4, *Materiel Management Procedures* (Oct. 11, 2005).

equipment, and specifically lists these items as including desktop and laptop computers, CD drives, printers, monitors, and handheld portable telecommunication devices. However, as noted in this report, VA has not ensured that sensitive IT equipment items valued at less than \$5,000 have been subjected to annual physical inventories. In addition, on March 9, 2007, at the time we began briefing VA management on the results of our audit, VA's Office of Information and Technology issued a policy⁴⁸ that includes assignment of user-level accountability for certain IT equipment, including external drives, desktop and laptop computers, and mobile phones that can be taken offsite for individual use. However, this policy had not yet been coordinated with property management officials who will be responsible for implementing the policy.

On August 4, 2006, VA issued a new directive *entitled Information Security Program*, which requires, in part, periodic evaluations and testing of the effectiveness of all management, operational, and technical controls and calls for procedures for immediately reporting and responding to security incidents. A thorough understanding of the IT inventory control process and required internal controls within this process will be key to effective testing and oversight. Managers were not always aware of the inherent problems in their IT inventory processes discussed in this report, including the lack of required controls. Because the directive does not provide specific information on how these procedures will be carried out, the CIO is developing supplementary user guides. Effective implementation will be key to the success of VA IT policy and organizational changes.

Conclusions

Poor accountability and a weak control environment have left the four VA case study organizations vulnerable to continuing theft, loss, and misappropriation of IT equipment and sensitive personal data. To provide a framework for accountability and security of IT equipment, the Secretary of Veterans Affairs needs to establish clear, sufficiently detailed mandatory policies rather than leaving the details of how policies will be implemented to the discretion of local VA organizations. Keys to safeguarding IT equipment are effective internal controls for the creation and maintenance of essential transaction records; a disciplined framework for specific, individual user-level accountability, whereby employees are held accountable for property assigned to them, including appropriate

⁴⁸ *Universal Serial Bus (USB) Flash Drive User Guide 2.0* (Mar. 9, 2007).

disciplinary action; and maintaining adequate physical security over IT equipment items. Although VA management has taken some actions to improve inventory controls, strengthening the overall control environment and establishing and implementing specific IT equipment controls will require a renewed focus, oversight, and continuing commitment throughout the organization.

Recommendations for Executive Action

We recommend that the Secretary of Veterans Affairs require that the medical centers and VA headquarters offices we tested and other VA organizations, as appropriate, take the following 12 actions to improve accountability of IT equipment inventory and reduce the risk of disclosure of sensitive personal data, medical data, or both.

To help minimize the risk of loss, theft, and misappropriation of government IT equipment used in VA operations, we recommend that the Secretary take the following eight departmentwide actions.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- Require that IRM 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.

- 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.

To assure inventory accuracy and prompt resolution of inventory discrepancies and improve security of IT equipment and any sensitive data stored on that equipment, we recommend that the Secretary require the CIO to take the following four actions.

- 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.
- Establish a process for reviewing Reports of Survey for lost, missing, and stolen IT equipment items to identify systemic weaknesses for appropriate corrective action.
- Establish and implement a policy requiring IRM 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.
- 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.

Agency Comments and Our Evaluation

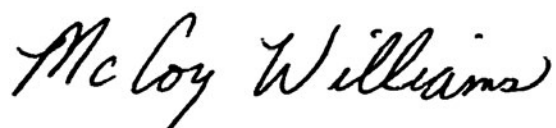
In written comments dated June 22, 2007, on a draft of this report, VA generally agreed with our findings, noted significant actions under way, and concurred on the 12 recommendations. For example, with regard to establishing detailed requirements for what transactions must be recorded to document inventory events, VA stated that it is performing a comprehensive update of department policies and procedures and plans to provide additional training and equipment audits, as necessary. With regard to establishing user-level accountability, VA stated that it is developing a policy that will require (1) unit heads or their designees to sign for all IT equipment issued to their service/unit and (2) hand receipts for IT equipment at the user-level.

VA also provided technical comments regarding the information in tables 6 and 7. Specifically, VA stated that our data did not specify whether the estimated value provided for missing IT equipment was based on a depreciated loss value or a replacement value. Consistent with VA's

reporting requirements for its Reports of Survey on lost personal property items, which include IT equipment, we used the original acquisition value for our estimates. Accordingly, we revised the column headings in the tables to note that the reported dollar value of missing items relates to the original acquisition value. Further, VA stated that some of the missing equipment included in our estimate may, in fact, have been properly disposed of but the proper documentation was not available. As stated in our report, proper documentation of key equipment events, such as transfer, turn-in, and disposal, must be documented by an inventory transaction, financial transaction, or both, as appropriate. Because the property system had not been updated to reflect a transfer, turn-in, or disposal and no hard copy documentation had been retained, it is not possible to determine whether any of the missing IT equipment items had been properly sent to disposal, and VA has no assurance that they were not lost or stolen.

As agreed with your offices, unless you announce its contents earlier, we will not distribute this report until 30 days from its date. At that time, we will send copies to interested congressional committees; the Secretary of Veterans Affairs; the Veterans Affairs Chief Information Officer; the Acting 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 williamsm1@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 III.



McCoy Williams
Director
Financial Management and Assurance

Appendix I: Objectives, Scope, and Methodology

Pursuant to a request from the Chairman and Ranking Minority Member of the House Committee on Veterans' Affairs, we audited the Department of Veterans Affairs (VA) information technology (IT) equipment inventory controls. Our audit covered the following.

- An assessment of the risk of loss, theft, and misappropriation of VA IT equipment items based on statistical tests of VA IT equipment inventory at selected case study locations and our investigator's evaluations of physical security and VA law enforcement investigations of incidents of loss or theft.
- Results of physical inventories of IT equipment performed by case study locations covered in this audit and our previous audit.
- An assessment of the adequacy of VA's physical security and accountability procedures for IT equipment in the property disposal process.
- Management actions taken or under way to address previously identified IT equipment inventory control weaknesses.

We used as our criteria applicable law and VA policy, as well as our *Standards for Internal Control in the Federal Government*¹ and our *Internal Control Management and Evaluation Tool*.² To assess the control environment at our test locations, we obtained an understanding of the processes and controls over IT equipment from acquisition to issuance and periodic inventories and disposal. We performed walk-throughs of these processes at all four test locations. 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 one location—the Washington, D.C., VA medical center—that had the most significant problems identified in our July 2004 report and two other geographically

¹ 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.

² 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.

dispersed VA medical centers. We also tested inventory at VA headquarters as a means of assessing the overall control environment, or “tone at the top.” Table 8 shows the VA locations selected for IT equipment inventory control testing and the number and reported value of IT equipment items at each location.

Table 8: 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 |
|----------------------------------|--|---|
| Washington, D.C., medical center | 168 of 8,728 ^a | \$33,065,322 |
| Indianapolis, IN medical center | 144 of 7,614 | 29,101,577 |
| San Diego, CA medical center | 148 of 11,604 | 48,077,071 |
| VA headquarters | 344 of 25,353 | 31,301,951 |

Source: GAO analysis of VA facility IT equipment inventory.

Note: The data represent current inventory at the time we pulled our samples. The reported value is the original acquisition cost.

^aIncludes 4,127 leased IT equipment items.

To follow up on actions taken in response to recommendations in our July 2004 report for improving physical inventories, we obtained and reviewed information on physical inventory results at the four case study locations as well as the five other case study locations previously audited.

We performed appropriate data reliability procedures, including an assessment of each VA test location’s procedures for assuring data reliability, and tests to assure that IT equipment inventory was sufficiently complete for the purposes of our work. Our procedures and test work identified a limitation related to IT equipment inventory completeness at our four test locations. IT equipment inventories at the Indianapolis and San Diego medical centers and VA headquarters organizations did not include all IT equipment acquired with purchase cards or purchased directly from local vendors. Also, the Washington, D.C., medical center inventory did not include one inventory category consisting of 149 older computer monitors and workstations. This data limitation prevented us from projecting 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 universe of current, recorded IT equipment inventory at the time of our tests, we selected stratified random probability samples of IT equipment, including medical equipment with data storage capability, at each of the three medical center locations. For the 23 VA headquarters organizations, we stratified our sample by 6 major offices and used a seventh stratum for the remaining 17 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.

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 controls 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 transactions as a whole. We present the results of our statistical samples for each population as (1) our projection of the estimated error overall and for each control attribute as point estimates and (2) the two-sided, 95 percent confidence intervals for the failure rates.

Our investigator supported our tests of IT physical inventory controls by assessing physical security and reporting of missing items for purposes of law enforcement investigations. As part of our assessment, our investigator interviewed VA Police at the three medical centers and federal agency law enforcement officers at VA headquarters about reports and investigations of lost, stolen, and missing IT equipment. Our investigator also met with physical security specialists at each of the test locations to discuss the results of physical security inspections and the status of VA actions on identified weaknesses.

To determine if the four test locations had adequate procedures for control and removal of data from hard drives of IT equipment in the property disposal process, our IT security specialist selected a limited

number of computer hard drives for testing. We attempted to test a total of 10 hard drives in each category—drives with data and drives that had been sanitized—at each of the four test locations. Because some hard drives we selected were damaged or computer systems pulled for hard drive testing did not contain hard drives, the number of hard drives actually tested was less than the number we selected for testing. At the San Diego medical center, 5 hard drives selected for testing that were labeled as unerased had in fact been sanitized, and we included these hard drives in our sanitization testing. Table 9 shows the numbers of hard drives tested at the four locations we audited.

Table 9: Number of Computer Hard Drives in the Property Disposal Process Selected for Testing at Four Locations

| Test location | Drives with data | Sanitized drives | Total |
|--------------------------------------|-------------------------|-------------------------|--------------|
| Medical centers | | | |
| Washington, D.C. | 4 | 4 | 8 |
| Indianapolis | 5 | 6 | 11 |
| San Diego | 10 | 15 | 25 |
| VA headquarters offices | | | |
| Veterans Health Administration | 2 | 1 | 3 |
| Board of Veterans Appeals | 6 | 8 | 14 |
| Office of Cyber Information Security | 3 | 1 | 4 |
| VA headquarters, subtotal | 11 | 10 | 21 |

Source: GAO analysis.

In performing these tests, our specialist used SMART™ and Foremost software. SMART™ is a software utility that has been designed and optimized to support forensic data practitioners and information security personnel in pursuit of their respective duties and goals. SMART™ is currently used by federal, state, and local law enforcement; U.S. military and intelligence organizations; accounting firms; and forensic data examiners. Foremost is a program used to recover files based on their headers, footers, and internal data structures. Foremost, originally developed by the United States Air Force Office of Special Investigations and the Center for Information Systems Security Studies and Research, is now available to the general public. In addition, our investigator performed physical security inspections and assessed accountability over computer hard drives in the disposal process.

To identify management actions taken in response to previously identified control weaknesses, we interviewed VA officials at our test locations, walked through the IT inventory processes to observe controls as implemented, and met with VA's Chief Information Officer (CIO). We also obtained and reviewed copies of new and revised VA policies and procedures.

We briefed VA managers at our test locations and VA headquarters, including VA medical center directors, VA headquarters information resource management and property management officials, and VA's CIO on the details of our audit, including our findings and their implications. On April 9, 2007, we requested comments on a draft of this report. We received comments on June 22, 2007, and have summarized those comments in the Agency Comments and Our Evaluation section of this report. We conducted our audit work from September 2006 through March 2007 in accordance with generally accepted government auditing standards, and we performed our investigative work in accordance with standards prescribed by the President's Council on Integrity and Efficiency.

Appendix II: Comments from the Department of Veterans Affairs



THE DEPUTY SECRETARY OF VETERANS AFFAIRS
WASHINGTON

June 22, 2007

Mr. McCoy Williams
Director
Information Management Issues
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Williams:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report: ***VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*** (GAO-07-505) and generally agrees with its findings. VA supports GAO's conclusion that improving the overall control environment for sensitive information technology (IT) equipment requires renewed focus, oversight, and continued commitment throughout the organization.

The Department has already taken significant actions, including the recent transformation of VA's IT program to a single authority under the Chief Information Officer. This will enable the Department to centralize and standardize IT equipment accountability policies and procedures, and replicate identified IT inventory best practices across VA.

Accomplishing this task will require a concerted effort by many different offices within the Department. VA will analyze why VA medical center employees were found to have used their own systems to track IT equipment assigned to their units instead of updating records through VA's existing formal control system. Accordingly, the Department will convene a formal work group to include representatives from at least the Office of Information and Technology, Office of Acquisition and Materiel Management, the Office of Security and Law Enforcement, the Veterans Health Administration, and the Office of Human Resources and Administration to ensure development of a comprehensive strategy to address all of GAO's recommendations.

Additionally, during the past 9 months VA Central Office (VACO) has revised and implemented procedures to improve the reconciliation process of future annual VACO inventories. These procedures include refresher training for all Equipment Inventory Listing (EIL) Officials, incorporating property accountability and responsibility in New Employee Orientation, and strengthening controls over the employee clearance process to ensure greater property accountability as individuals depart VACO.

Page 2

Mr. McCoy Williams

The Department is finalizing new policy directives that will require senior IT officials at the facility level to maintain an inventory of all IT equipment. The VA Office of Acquisition and Materiel Management provides current policy regarding the use and protection of VA-owned IT equipment. Department officials will reinforce those policies across all business lines.

I appreciate your efforts to illuminate continuing weaknesses that undermine VA's efforts to protect the sensitive personal information the Department needs to provide services to our Nation's veterans. The enclosure discusses each of GAO's recommendations in detail. It also suggests some technical clarification for the report's overall accuracy.

Sincerely yours,



Gordon H. Mansfield

Enclosure

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)

To help minimize the risk of loss, theft, and misappropriation of government IT equipment used in VA operations, GAO recommends that the Secretary of Veterans Affairs take the following departmentwide actions.

- **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.**

Concur - VA is performing a comprehensive update of Department policies and procedures on equipment management, and we will include detailed requirements as appropriate.

To improve awareness of and compliance with existing policies and procedures, the Veterans Health Administration (VHA) recently issued 11 standard operating procedures with detailed guidance to supplement VA policy and procedures on equipment management.

In addition, VA's Office of Acquisition and Materiel Management (OA&MM) is working with VHA, the Veterans Benefits Administration, the National Cemetery Administration and the Office of Information and Technology (OI&T) to identify specific ways to improve compliance with VA's policies and procedures on equipment management. Topics under review include:

- ◇ launch of a nationwide training program on equipment accountability;
- ◇ review of logistical organizational structures;
- ◇ implementation of a logistics certification program; and
- ◇ issuance of a memorandum to facility directors emphasizing the importance of equipment management and recommended actions to strengthen local programs.

Finally, OA&MM is collaborating with VHA's Office of Business Oversight to include additional areas of audit for equipment management. This will also include a review of audit findings to determine where policies and procedures need enhancement.

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)
(Continued)

- **Revise VA purchase card policy to require purchase card holders to notify property management officials of IT equipment and other property items acquired with a government purchase card at the time the items are received so that they can be recorded in property management systems.**

Concur - The Office of Finance will revise VA purchase card policy to require purchase card holders to notify property management officials of IT equipment and other property items acquired with a government purchase card at the time the items are received so that they can be recorded in property management systems. Target completion date is July 2007.

On page 7, under "Requests and Ordering of IT Equipment," the sentence that begins on line 7 is no longer applicable. Headquarters offices may no longer place individual orders or use purchase cards to acquire IT equipment per recent guidance from the Chief Information Officer (CIO).

- **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.**

Concur - The Office of Information and Technology is developing an operations policy that requires the senior IT official at a facility to maintain an inventory of all IT equipment and to have the business/service unit head or designee sign for all IT equipment issued to their service/unit. Also, the policy will require issuing of hand receipts for IT equipment at the user-level.

- **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.**

Concur - For VA Central Office (VACO), O/A's Property Management Division is responsible for processing Report of Surveys from Central Office organizations for lost or damaged VA property. The Property Management Division will expeditiously assign the Report of Survey to a Survey Board to determine if the

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)
(Continued)

employee(s) should be held financially liable or if disciplinary actions should be taken as a result of the loss, damage, or destruction of the property.

When the Survey Board recommends that an employee should be held financially liable, a copy of the Report of Survey, complete findings and recommendations will be sent directly to the employee, instructing them to submit a written concurrence or objections to the findings within 10 working days to the approving official. An employee's failure to submit a written reply to the approving official within 10 working days will be submitted as acceptance of financial liability. Employees have the right to have an adverse survey finding reviewed by higher authority if requested within 10 working days after receiving notification of findings. The decision of the higher approving authority will be final. VA supervisors are responsible for ensuring that their employees are held accountable for VA property assigned to them in performance of their job. Supervisors are also responsible for any property not directly assigned to an individual employee in their area.

OIA's Property Management Division is also implementing new VACO procedures to increase supervisory awareness and accountability for property lost, damaged, or destroyed by employees under their supervision, when supported by findings and recommendations from the Survey Board. This procedure includes the issuance of a memorandum from the approving official and Report of Survey findings, to the employee's supervisor with a courtesy copy to the second-line supervisor and Employee Relations, Central Office Human Resources Service, recommending that the supervisor take corrective action, including disciplinary action as appropriate, against the employee. Employee Relations, Central Office Human Resources Service, will follow up with the employee's immediate and second-line supervisors to ensure appropriate action is taken within 45 calendar days.

- **Establish specific timeframes for finalizing a Report of Survey once an inventory has been completed so that research on missing items is completed in an expeditious manner and does not continue indefinitely without meeting formal reporting requirements.**

Concur – OI&T is developing an operations policy that will include the requirement that a Report of Survey will be completed within 15 working days following completion of annual inventory. In VACO, after an annual Equipment Inventory is conducted, the Not Found Property Report must be reconciled within

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)
(Continued)

15 days of receiving the report. (In the past, the Office of Administration [OA] has honored organizational requests to extend this timeframe for equipment believed misplaced rather than stolen.) Equipment that cannot be reconciled must immediately be reported on a Report of Survey to the Property Management Division. Property Management Division will immediately conduct an investigation on the missing equipment by forming a Board of Survey. Recent memorandums to the various VACO department heads addressed these procedures. Details were also provided to Equipment Inventory List (EIL) Officials in VACO.

- **Establish a mechanism to monitor San Diego, California, and Houston, Texas, medical center and other VA organization adherence as appropriate, to VA policy for performing annual inventories of sensitive items under \$5,000, including IT equipment.**

Concur – The Veterans Health Administration's (VHA) Prosthetics and Clinical Logistics Office (P&CLO) is monitoring all VA medical centers to ensure adherence to policy requiring an annual inventory of all items. To facilitate this effort, all facilities are required to report their Electronic Inventory List compliance on a quarterly basis to the Deputy Under Secretary for Health for Operations and Management (DUSHOM). This monitoring includes sensitive items under \$5,000. P&CLO will disseminate further direction to the field on sensitive items through annual training, reminders at the materiel management conference calls, and e-mails.

- **Require that IRM 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.**

Concur – VA's current asset management system (AEMS/MERS) allows for IRM and IT Services to be given restricted access to the AEMS/MERS system in order to record/update inventory records to reflect status and location. Hand scanners can be purchased locally as needed. Nevertheless, VHA's P&CLO is working with the DUSHOM to disseminate a memorandum to all VA medical centers directing them to give access to AEMS/MERS for all applicable

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)
(Continued)

information resource management and IT staff involved in IT asset management. P&CLO and DUSOHOM will provide direction in the memorandum to ensure open communication between IT staff and logistics staff in coordination of either procuring bar code scanners or making available existing bar code scanners at the medical centers. The memorandum will specify follow-up through regular conference calls and e-mails as required. Lastly, P&CLO is working with OI&T to establish better communication in defining roles and responsibilities of front line staff in updating the equipment records as appropriate.

- **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.**

Concur – The current version of the Security and Law Enforcement policy (0730/1) is referenced in this report. This version has undergone a large-scale revision and is in the Department concurrence process. There is a new requirement to the revised policy that each VA facility establish a Security Management Committee (SMC). One of the tasks of the SMC is to develop a local strategic security plan (SSP). The SSP is intended as a framework for identifying a facility's security needs and resolutions.

We also wish to note that specific physical security requirements for IT resources and spaces have been updated. In addition, IT spaces are now required to be protected with physical access control systems (PACS). In previous versions, this was an optional item.

To assure inventory accuracy and prompt resolution of inventory discrepancies and improve security of IT equipment and any sensitive data stored on that equipment, GAO recommends that the Secretary require the CIO to take the following four actions:

- **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.**

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation**
(GAO-07-505)
(Continued)

Concur – OI&T is developing a policy that requires the senior IT official at a facility to maintain an inventory of all IT equipment and to have the business/service unit head or designee sign for all IT equipment issued to their service/unit. The policy will require issuing of hand receipts for IT equipment at the user-level. The senior IT official at a facility will be required to complete an annual survey that ensures IT equipment inventory records are complete and up-to-date.

- **Establish a process for reviewing Reports of Survey for lost, missing, and stolen IT equipment items to identify systemic weaknesses for appropriate corrective action.**

Concur – OI&T is developing a policy that will include the requirement that a report of survey will be completed within 15 working days following completion of annual inventory. The policy will also require an analysis of the reports to identify any weakness trends.

- **Establish and implement a policy requiring IRM Personnel and IT coordinators to inform Physical Security Officers of the location of all IT equipment storage locations so that these store rooms can be subjected to required inspections.**

Concur - OI&T is developing a policy that will require the senior IT official at every facility to provide IT equipment storage locations to facility security personnel to perform regular inspections.

- **Establish and implement a policy for reviewing the results of physical security inspections of IT equipment store rooms and ensure that needed corrective actions are completed.**

Concur - OI&T is developing a policy that will require senior IT Officials at every site to complete corrective actions addressed from all physical security inspections of IT equipment store rooms.

Technical comments:

Enclosure

Department of Veterans Affairs (VA) comments to
Government Accountability Office (GAO) draft report
**VETERANS AFFAIRS: *Inadequate Controls over IT Equipment at Selected
VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation***
(GAO-07-505)
(Continued)

Pages 4 and 20, and Tables 6 and 7, portray IT equipment that cannot be accounted for as having a combined potential financial loss in the millions of dollars. However, the report does not specify whether this cost estimate is provided as a depreciated loss value or a replacement value. Distinguishing between the two is very important as it directly impacts the loss estimate value. For instance, if IT equipment was purchased in previous years, it depreciates at a significant determined rate. On the other hand, if GAO used replacement costs to estimate the loss value, it needs to further clarify which year values it used (i.e. 2002 values, 2005 values, or current 2007 values). In addition, the tally of unaccounted-for equipment that GAO used for its estimate of loss value was surmised as a result of this audit. However, VA could, in fact, have properly disposed of some of the "missing" equipment, but the proper documentation of the disposal is just not available. If this is the case, then it should not be subject to having a replacement cost associated with it.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

McCoy Williams, (202) 512-9095 or williamsm1@gao.gov

Acknowledgments

In addition to the contact named above, Gayle L. Fischer, Assistant Director; Andrew O'Connell, Assistant Director and Supervisory Special Agent; Abe Dymond, Assistant General Counsel; Monica Perez Anatalio; James D. Ashley; Francine DelVecchio; Lauren S. Fassler; Dennis Fauber; Jason Kelly; Steven M. Koons; Christopher D. Morehouse; Chris J. Rodriguez; Special Agent Ramon J. Rodriguez; Lori B. Tanaka; and Danietta S. Williams made key contributions to this report.

Technical expertise was provided by Keith A. Rhodes, Chief Technologist, and Harold Lewis, Assistant Director, Information Technology Security, Applied Research and Methods.

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). 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 and select "Subscribe to 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, D.C. 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

E-mail: fraudnet@gao.gov

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548