GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-07-505, a report to congressional requesters

July 2007

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 williamsm1@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.