July 2008

VETERANS AFFAIRS

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

G A O
Accountability•Integrity•Reliability
Highlights

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

Why GAO Did This Study

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

What GAO Recommends

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

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

What GAO Found

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

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

IT Inventory Control Test Results at Four Case Study Locations

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

Source: GAO analysis.

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

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