AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY INVENTORY MANAGEMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 24, 2007

Serial 110–36

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE

37–474 WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON VETERANS' AFFAIRS

BOB FILNER, California, *Chairman*

CORRINE BROWN, Florida
VIC SNYDER, Arkansas
MICHAEL H. MICHAUD, Maine
STEPHANIE HERSETH SANDLIN, South Dakota
HARRY E. MITCHELL, Arizona
JOHN J. HALL, New York
PHIL HARE, Illinois
MICHAEL F. DOYLE, Pennsylvania
SHELLEY BERKLEY, Nevada
JOHN T. SALAZAR, Colorado
CIRO D. RODRIGUEZ, Texas
JOE DONNELLY, Indiana
JERRY McNERNEY, California
ZACHARY T. SPACE, Ohio
TIMOTHY J. WALZ, Minnesota

STEVE BUYER, Indiana, *Ranking*
CLIFF STEARNS, Florida
JERRY MORAN, Kansas
RICHARD H. BAKER, Louisiana
HENRY E. BROWN, JR., South Carolina
JEFF MILLER, Florida
JOHN BOOZMAN, Arkansas
GINNY BROWN-WAITE, Florida
MICHAEL R. TURNER, Ohio
BRIAN P. BILBRAY, California
DOUG LAMBORN, Colorado
GUS M. BILIRAKIS, Florida
VERN BUCHANAN, Florida

Malcom A. Shorter, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

HARRY E. MITCHELL, Arizona, *Chairman*

ZACHARY T. SPACE, Ohio
TIMOTHY J. WALZ, Minnesota
CIRO D. RODRIGUEZ, Texas

GINNY BROWN-WAITE, Florida, *Ranking*
CLIFF STEARNS, Florida
BRIAN P. BILBRAY, California

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

July 24, 2007

Page

U.S. Department of Veterans Affairs Information Technology Inventory Management 1

OPENING STATEMENTS

Chairman Harry E. Mitchell 1
Prepared statement of Chairman Mitchell 29
Hon. Ginny Brown-Waite, Ranking Republican Member 3
Prepared statement of Congresswoman Brown-Waite 30
Hon. Timothy J. Walz 4

WITNESSES

U.S. Government Accountability Office, McCoy Williams, Director, Financial Management and Assurance 5
Prepared statement of Mr. Williams 31
U.S. Department of Veterans Affairs:
Hon. Robert T. Howard, Assistant Secretary for Information and Technology, and Chief Information Officer 14
Prepared statement of Mr. Howard 38
Hon. Robert J. Henke, Assistant Secretary for Management 16

SUBMISSIONS FOR THE RECORD

Space, Hon. Zachary T., a Representative in Congress from the State of Ohio 39
Stearns, Hon. Cliff, a Representative in Congress from the State of Florida, statement 39

MATERIAL SUBMITTED FOR THE RECORD

Report:
United States Government Accountability Office, Report to Congressional Requesters, July 2007, entitled, "Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation," GAO–07–505 41
Tables and Figures from GAO–07–505 **[The Tables and Figures are included in the GAO report and will not be reprinted.]**
Post Hearing Questions and Responses for the Record:
Hon. Harry E. Mitchell, Chairman, and Hon. Ginny Brown-Waite, Ranking Republican Member, Subcommittee on Oversight and Investigations, to Hon. R. James Nicholson, Secretary, U.S. Department of Veterans Affairs, letter dated July 20, 2007, requesting the VA to provide the most recent equipment inventory certification letters from all facility directors **[The information was provided to the Subcommittee and will be retained in the Committee files.]** 73

U.S. DEPARTMENT OF VETERANS AFFAIRS INFORMATION TECHNOLOGY INVENTORY MANAGEMENT

TUESDAY, JULY 24, 2007

U. S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:07 p.m., in Room 334, Cannon House Office Building, Hon. Harry E. Mitchell [Chairman of the Subcommittee] presiding.

Present: Representatives Mitchell, Walz and Brown-Waite.

OPENING STATEMENT OF CHAIRMAN MITCHELL

Mr. MITCHELL. Good afternoon. Welcome to the Subcommittee on Oversight and Investigations, and today's hearing is on information technology (IT). This hearing will come to order.

I want to thank everyone for coming here today. I am very pleased that so many folks could attend this oversight hearing on the U.S. Department of Veterans Affairs (VA) information technology inventory issues. We know that VA has serious problems with keeping track of its IT inventory. This is not just a dollar issue, although it is certainly that; it is also a security and privacy issue. VA's inventory deficiencies mean that VA cannot assure that private medical and other information belonging to the Nation's veterans remains private.

We are going to begin the hearing today by hearing from the U.S. Government Accountability Office (GAO) and their GAO report, and this is the report that is being released today: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss and Misappropriation. This was just released today, showing the results of its testing of inventory systems and procedures at four VA locations.

The results are not pretty. As you can see from the chart, and there is a chart over here, most of you cannot see it here, but Members on the dais can see it. The sample location GAO tested showed that from 6 to 28 percent of IT items listed as being in inventory could not be located. The Washington, DC, VA Medical Center could not find an astonishing 28 percent of the IT items in inventory. The missing items at the four locations had a combined value of $6.4 million.

Sad to say, this is not a recent problem. In July 2004, GAO reported that the six VA medical centers it audited did not have reli-

able property databases. GAO followed up on these sites as part of its current report and concluded that more than $13 million in IT equipment was still missing from those sites. Incredibly, an inventory being conducted by one of these sites in response to the 2004 GAO report is still not complete.

If this were not bad enough, GAO further reports that VA has seriously flawed policies and procedures. Again, the chart illustrates the extent of the problem. One line says "incorrect user organization." That means the inventory system is incorrectly identified to whom the equipment was assigned.

Look at the numbers: 80 percent of the Washington, DC, medical facility, 69 percent in Indianapolis, 70 percent in San Diego.

VA's central headquarters does better, only 11 percent, but more than makes up for this with physical location of 44 percent of its IT equipment misidentified in its inventory database.

The issue of security could not be better illustrated than by a photograph you see over here, and there is a photograph, a blowup. And this photograph is of an IT equipment storeroom at VA central headquarters. It seems hardly necessary for GAO to have pointed out that this storeroom did not meet VA's requirements for motion intrusion detection alarm, secure doors, locks and special access keys.

Security is no small matter, and we are not concerned only about hardware. GAO found hard drives at two of the four locations that were designated as excess property to be disposed of. It still had hundreds of veterans' names and Social Security numbers. This is completely unacceptable.

At this time, I ask unanimous consent that the complete GAO report be entered into the record. Seeing no objection, so ordered.

[The report, GAO–07–505, entitled, "Veterans Affairs: Inadequate Controls over IT Equipment in Selected VA Locations Pose Continuing Risk of Theft, Loss and Misappropriation," appears on p. 41.]

Mr. MITCHELL. I can assure you, we will be back to hear this. We intend to ask GAO to conduct other checks of VA's inventory system in a few months' time, and if another hearing turns out to be necessary, we will have another one.

Last week, Ms. Brown-Waite and I sent a letter to the VA—and this is part of our letter—requesting copies of the most recent annual equipment inventory certification letters from all facility directors. We also requested a list of all facility directors who did not provide certification for completing their annual inventories. I would like to thank the VA for their prompt response.

At this time, I ask unanimous consent that Ms. Brown-Waite's and my letter be entered into the record. Seeing no objection, so ordered.

[The July 20, 2007, letter to U.S. Department of Veterans Affairs Secretary Nicholson, appears on p. 73.]

Mr. MITCHELL. Before I recognize the ranking Republican Member for her remarks, I would like to swear in our witnesses, and I would like to ask all witnesses if they would please come forward and rise, both the first panel and the second panel. If you would, all please rise.

[Witnesses sworn].

Mr. MITCHELL. Thank you.

[The prepared statement of Chairman Mitchell appears on p. 29.]

Mr. MITCHELL. I now recognize Ms. Brown-Waite for opening remarks.

OPENING STATEMENT OF HON. GINNY BROWN-WAITE

Ms. BROWN-WAITE. I thank the Chairman very much, and I also thank those who will be presenting today. My goal for this hearing is not just to learn where VA is relative to the current IT inventory management, but to learn where and how they are working to improve security controls, maintenance and management of their equipment.

The July 2007 GAO report, which the Chairman just had admitted to the record, increased my growing concern over VA's control over its inventories from my reading of the weekly Security Operations Center (SOC) reports. The GAO report reflected four specific sites for their report. During this study fewer than half of the items GAO selected for testing could be located, and most of the items were information technology equipment.

GAO found that the four VA locations reported over 2,400 missing IT equipment items valued at about $6.4 million. These were identified in inventories performed during fiscal years 2005 and 2006.

Equally troubling in the information in the report was that missing items were not always reported right away, and in some instances, not for several years. At one of the locations, as shown on the easel, 28 percent of the items surveyed during the GAO audit were missing.

Mr. Chairman, I find the lack of control over equipment completely unacceptable. Here in the House of Representatives our acquisition offices perform annual equipment inventories in all offices. The Chief Administrative Officer's staff comes into our offices either to tag equipment we have purchased, remove equipment we no longer use, or inventory the equipment under our control. By keeping a centralized acquisition and inventory process, the House is able to maintain tight control over its equipment inventory. Given the results of the GAO report, it appears that the VA is unable to do likewise.

According to the report, there is also a lack of user-level accountability for the IT equipment due to weak overall control of the equipment environment. The IT personnel and IT coordinators do not have physical possession or custody of all the IT equipment under their purview. Therefore, they are not held accountable for IT equipment determined to be missing during physical inventories.

In my opinion, Mr. Chairman, there needs to be accountability for inventories from the chief executive officer clear down the line to the user who is ultimately using the product. But I guess you could also say "using or losing the product."

The weekly SOC reports consistently show missing IT-related items from the VA's inventories, whether it is listing old equipment that possibly had been disposed of after it was no longer of use to the VA, or new equipment that had been stolen.

I am heartened to note that the VA is working with local and Federal law enforcement to track down and retrieve newer stolen equipment, but dismayed to see the number of equipment items that were either transferred to other facilities and not tracked or disposed of without proper notation in the equipment inventories.

As of February 28th, the GAO report found four case-study locations covered in their report that were—2,400 IT equipment items weren't found, it was revealed, with a combined original acquisition value of about $6.4 million, as a result of inventories VA performed during fiscal years 2005 and 2006.

Based on information GAO obtained through March 2, 2007, the five case-study locations previously audited had identified over 8,600 missing IT equipment items, with a combined original acquisition value of over $13.2 million. GAO reported that the missing IT items represent record keeping errors, the loss, theft or misappropriation of IT equipment.

The GAO also cited that, because most of the nine case-study locations had not consistently performed required annual physical inventories or completed reports of survey promptly, which prevented the reporting of missing IT equipment in some instances for several years. I am also surprised when I see a report—see a SOC report reporting the first instance of listing a missing piece of IT equipment from the mid-nineties; operating systems for this equipment would be totally out of date long ago, and it leaves me wondering just how long the equipment was actually missing before it was reported.

Mr. Chairman, this is not the first time that GAO has reported on deficiencies in information technology equipment controls. In 2004, there was a similar report on VA medical centers entitled Internal Control Over Selected Operating Functions Needs Improvement. In this report, GAO indicated that the six VA medical centers they audited lacked a reliable property control database. One of the medical centers reviewed also was included in the most recent report, and yet those issues still remain.

I look forward to today's hearing and hearing from today's witnesses and those accompanying them on how VA plans on moving forward, and how quickly and efficiently we can hope and encourage them to follow up on GAO's recommendation.

I thank you, Mr. Chairman. I yield back the balance of my time.

[The prepared statement of Congresswoman Brown-Waite appears on p. 30.]

Mr. MITCHELL. Thank you.

Mr. Walz?

OPENING STATEMENT OF HON. TIMOTHY J. WALZ

Mr. WALZ. Thank you, Mr. Chairman, thank you to the Ranking Member, and thank you to our panelists for being here today at this incredibly important hearing. Those of us that go out and talk to our veterans, this issue is still very, very important and at the forefront of what they are concerned about.

I am one of those 26 million veterans who received the infamous letter saying my information may have been compromised, and what this does, from the sinking feeling of loss of personal security and the concern over data theft, is concern for the individual. It

has a very corrosive effect on trust in the VA in general, and that is the part I am most concerned about.

I am here today welcoming all of us as team players to figure out how we get at this, but I think each of the Members up here is sensing the frustration amongst our constituents and our veterans that this is another one of those issues we speak of often, yet see very little movement forward.

So this is, to me, an absolute priority. We have to make sure that faith in the VA system remains strong and that data security is protected.

So with that I look forward to these panels, and thank you again, Mr. Chairman, for holding this hearing.

Mr. MITCHELL. Thank you, Mr. Walz.

At this time, I ask unanimous consent that all Members have 5 legislative days to submit a statement for the record. Seeing no objection, so ordered.

Mr. MITCHELL. I will now proceed to Panel 1. Mr. McCoy Williams is the Director of Financial Management and Assurance for the U.S. Government Accountability Office. Mr. Williams' team was responsible for writing this troubling report on VA's IT inventory management. We look forward to hearing his views on what VA needs to do to improve inventory controls.

Mr. Williams, if you would proceed but also keep in mind that we would like to keep this at 5 minutes.

STATEMENT OF McCOY WILLIAMS, DIRECTOR, FINANCIAL MANAGEMENT AND ASSURANCE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY GAYLE L. FISCHER, ASSISTANT DIRECTOR, FINANCIAL MANAGEMENT AND ASSURANCE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILLIAMS. Thank you. Mr. Chairman, Members of the Subcommittee, Ms. Fischer and I thank you for the opportunity to discuss our recent audit of controls over IT equipment at the Department of Veterans Affairs.

In light of reported weaknesses in VA inventory controls and reported thefts of laptop computers and data breaches, the adequacy of such controls has been an ongoing concern. Today, I will summarize the results of our recent work, the details of which are included in our audit report, which the Subcommittee is releasing today. This audit followed a July 2004 report in which we identified weak practices and lax implementation of controls of equipment at the six VA medical centers we audited.

For today's testimony, I will provide the highlights of our current findings related to three key issues: first, the risk of theft, loss or misappropriation of IT equipment at selected VA locations; second, whether selected VA locations have adequate procedures in place to assure physical security and accountability over IT equipment and excess property disposal process; and third, what actions VA management has taken to address identified IT equipment inventory control weaknesses.

First, we concluded that for the four case-study locations we audited, there was an overall lack of accountability for IT equipment. Based on our tests of IT equipment inventory controls, we estimated that the percentage of inventory control failures related to

missing items ranged from 6 percent at the Indianapolis Medical Center to 28 percent at the Washington, DC, Medical Center.

In addition, we determined that VA property management policy does not establish accountability with individual users of IT equipment. Consequently, our control tests identified 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.

Our analysis of the results of physical inventories performed by the four case-study locations in our current audit identified over 2,400 missing IT equipment items with a combined original acquisition value of about $6.4 million. In addition, the five locations we previously audited had reported over 8,600 missing IT equipment items, with a combined original acquisition value of over $13.2 million.

Further, we found that missing IT items were often not reported for several months, and in some cases, several years, because most of the case-study locations had not consistently performed physical inventories or promptly completed the required report of survey.

Second, Mr. Chairman, 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. However, 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.

We also found numerous unofficial IT equipment storage locations in VA headquarters area office buildings that did not meet VA physical security requirements. For example, at some VA headquarters locations excess computer equipment was stored in open, unsecured areas.

Finally, VA has made limited progress in addressing these problems since our July 2004 report, including, among other things, clarifying property management policies and centralizing IT functions under the new Chief Information Officer (CIO) organization. However, the Department has not yet ensured consistent implementation of effective controls for accountability of IT equipment inventory.

Mr. Chairman, until these shortcomings are addressed, VA will continue to face major challenges in safeguarding IT equipment and sensitive personal data stored on this equipment from loss, theft and misappropriation.

In conclusion, Mr. Chairman, strengthening the overall control environment and establishing specific IT controls will require a renewed focus, oversight and continuing commitment throughout the organization.

This concludes our prepared statement. Ms. Fischer and I would be very happy to answer any questions that you or other Members of the Subcommittee may have at this time. Thank you.

[The prepared statement of Mr. Williams appears on p. 31.]

Mr. MITCHELL. Thank you, Mr. Williams.

In your first—in your most recent report, the GAO concluded that poor accountability and 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. This conclusion is no different than what the GAO reached in 2004. Is that true?

Mr. WILLIAMS. That is true, Mr. Chairman. While the conclusion is the same, if you look at the specific numbers as far as the amount of items that we were unable to find in the audit that we did in 2004, there has been some improvement there, but there is still a lot of work to be done. Given that amount of timeframe, there are some things that you would have expected to have been completed by this time based on those findings, but the conclusion is definitely the same.

Mr. MITCHELL. In your opinion, what is the VA's problem. Why hasn't anything really been done?

Mr. WILLIAMS. I think, to address this problem, there are two or three things that need to be done; and I think one of the things that I would start out with is that there needs to be accountability, as we have stated in the report, at the individual level.

When you have got accountability that is not assigned to the individuals in a situation which, as I like to say, when everybody is accountable, you end up with no one being accountable. Then you need to make sure that you have policies and procedures that are in place that are consistent throughout the organization, and they are carried out.

It is one thing to have policies and procedures in place, but you want to make sure you have that oversight to make sure those policies and procedures are being implemented by management in the organization.

Mr. MITCHELL. Thank you. A bad inventory system obviously raises concern about wasting taxpayers' money, but there are also security concerns, concerns that are particularly acute given the VA's recent episodes on data loss.

Your report describes concerns with the security of private veteran data. Please tell us about how the VA's inadequacy of their inventory system creates a danger for data loss.

Mr. WILLIAMS. I think one of the examples that I just finished talking about in my opening statement was, we did not find any data on those hard drives that had been identified as being sanitized. The problem comes in, the risk comes in when you have hard drives that are waiting to be sanitized, and those are in file cabinets or in storage bins and they have been there for years.

So when you leave those hard drives there, there is always the risk that someone can come along and take it and extract that information and use it for reasons that are not good.

The other concern that we had was the security around the locations where the items were actually stored. As you can tell from one of the pictures that we have here, that there are certain requirements as far as what type of security is supposed to be associated with this type of equipment. Rooms are supposed to be locked, and so forth, there are supposed to be floor-to-ceiling walls so that individuals cannot get over and take some of these items out.

So that is the concern we have. You want to make sure that you have got those controls in place so that this sensitive and very important data is properly protected and not in the hands—the possi-

bility of its being in the hands of someone that would use it for bad purposes.

Mr. MITCHELL. You mentioned just a second ago about the importance of user-level accountability and how important that is. You also pointed out that they don't have it in the VA except for IT equipment that is taken off-site.

What is the current process the VA has for assigning custody for IT equipment?

Mr. WILLIAMS. As we stated in the report, there is a process in which you basically get a hand receipt for items that you are going to be—I guess mobile items, things you take offsite.

The concern that was raised in our review of that particular area—and I will let Ms. Fischer chime in on the specific numbers if I am off. I think we requested about 15 items to look at, items to identify if the policy was actually being followed, if there was actually a hand receipt for those items being taken off; and of that number, I think six items we were unable to get the hand receipt—the documentation to show the support for this is a receipt for this item being taken out.

There were about nine other items; I think six of those nine we basically found that the documentation was recorded after the fact, I believe. And for two of the items we found it was valid. So out of those 15, we were only able to identify 2 in which the process had actually been followed.

Mr. MITCHELL. One very quick follow-up, if the Subcommittee will indulge me here.

How difficult would it be to implement a user accountability system?

Mr. WILLIAMS. I think it would take some time to set that system up initially, but from a cost-benefit standpoint, once you get that particular process set up and you do that inventory on an annual basis, or whatever basis that you decide you want to do it, I think it is a process that could be followed and implemented throughout the organization.

We have it at my organization. Once a year I get a call and I am notified that there is an inventory that is going to be performed. When that piece of equipment was assigned to me, I signed off on a sheet of paper and basically stated that, McCoy Williams, you are responsible for this particular computer, this particular device or what have you. It is only a matter of time, of another person coming through, independent verification; they will look at the Code that is on the equipment and basically check it off as being in my control.

So I don't think it is a major, major problem. I will let Ms. Fischer add.

Ms. FISCHER. Mr. Chairman, I do want to point out that the Washington, DC, Medical Center implemented user level accountability for their IT equipment during March of 2007 as we were wrapping up our work. We have looked at their policy. It looks pretty good.

When a user signs for accountability of their IT equipment, they are acknowledging at least eight rules and guidelines that they are attesting to that they will follow; and you might want to ask your witnesses today in Panel 2 how that is working for them.

Mr. MITCHELL. Thank you.

At this time I would like to recognize Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you, Mr. Chairman. I first of all thank both of you for being here.

Mr. WILLIAMS. Thank you.

Ms. BROWN-WAITE. Mr. Williams, is it that the policies VA currently has aren't being followed or that they need totally new policies?

Mr. WILLIAMS. I wouldn't say that they need totally new policies, but I think there need to be some revisions to the policies to strengthen some of the controls. But there are also some controls that they currently have in place in those policies that we found were not being followed, so I would say it is a combination.

Ms. BROWN-WAITE. A combination.

Let me ask you this. In your report you mention the fact that VA policy mandates that a report 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 is $5,000 or more.

Are you aware, has this board survey ever been appointed and has anybody ever been held accountable for missing items?

Mr. WILLIAMS. We will take this one jointly.

Ms. FISCHER. They have appointed boards of survey to further investigate items that are identified as missing in their physical inventories. We don't know of any specific instances where individuals have been held liable for lost equipment. However, VA probably has that information. You could ask the witnesses on Panel 2 if they have examples of that.

Ms. BROWN-WAITE. If I may follow up with another question for Ms. Fischer, the report mentions a problem with purchase cards.

Could you explain why IT equipment bought with a government purchase card was not recorded in the property records?

Ms. FISCHER. Yes, Congresswoman Brown-Waite. Their policy did not require the purchase card holders to notify the property officers when they acquired computer equipment with the purchase card. So it was put into service and never entered in the inventory records.

We made a recommendation, and VA has stated that they will have that policy in place this month. Our recommendation was that they, of course, implement that requirement.

Ms. BROWN-WAITE. And were they receptive to implementing that requirement? It just—to the average citizen out there, it just seems as if one hand does not know what the other hand is doing when it comes to inventory in the VA. It really does seem that way. And the sad part of it is, that translates into fewer dollars actually being used for the veterans, which I know troubles every Member of this Subcommittee up here. So is that——

Mr. WILLIAMS. Let me take that.

I would start by saying that having read VA's testimony for today, I think that if those actions that have been identified in today's testimony are followed through on, it looks like that is putting them on track to address these problems that we have identified back in 2004, as well as the problems that we have identified

in our report that is being released today. That means that it is probably too soon to tell at this particular point in time.

We have laid out the issues and we have laid out the recommendations. I think that this is a good first start, based on what I see in the testimony today. The proof will be in the actions that will follow down the road to see if these recommendations are actually implemented.

Ms. BROWN-WAITE. Based on what we have heard so far, how is the team able to find most of the equipment when VA didn't know who had the equipment or where it was?

Ms. FISCHER. They were pretty familiar with the process by the time we did our second audit; and they had a team accompanying us, and when items could not be located, they sent people out to look for, say, turn-in documentation that may exist where items hadn't been updated in inventory as being disposed of. They looked at where IT equipment was plugged into the networks. Sometimes the central system could tell them where that equipment was located. And in some cases they did a full facility search.

VA headquarters actually sent teams to the field to determine whether some of the IT equipment had been transferred to field locations without updating the inventory record. So all of these human intervention efforts helped them locate some of the items we couldn't initially identify during our inventory.

Mr. WILLIAMS. May I add a point to that, because I was involved in the 2004 inventory also; and I remember to this date one location that I actually visited, and we had the same type of assistance in which VA staff would actually go to the various locations, and we would try to identify the properties and all.

At this one particular location I recall my staff and I pulled up to the building and basically introduced ourselves and stated what we were there for, and we basically got the old-fashioned cold shoulder that you're here during my lunch time and this is not an important event for me.

I would add the attitude this time, I think, based on Ms. Fischer's team going out, is the organization understands the importance of taking these inventories and why it is important you have these good records for the property that is in your control.

Ms. BROWN-WAITE. With that, I yield back.

Mr. MITCHELL. Thank you.

Mr. Walz?

Mr. WALZ. Thank you, Mr. Williams and Ms. Fischer. I really appreciate this; I appreciate the work that you are doing on this.

I, for one, again can't stress enough that I believe that the work that the VA is doing and all the good that it is doing is almost immeasurable. But any time we have these types of issues, it totally undermines everything we are doing. So the criticalness of this and the sense of urgency is very much here with this Subcommittee.

I want to just lay out a bit of a scenario and talk to you about this, having had some experience in Federal Government. But I think—Mr. Williams had me intrigued with his idea of this individual accountability thing.

At one time, when I was a lowly GS-7, I was in charge of managing a national Guard armory, and I can remember signing those property books and being in charge of those, and I was the only one

there and there were millions of dollars of equipment, from howitzers to mop heads, and they were all on the property books. I had to be accountable for every single one of them.

I can remember turning an armory upside down looking for little radiac meters they gave us to see radiation in there that we weren't sure how to use them, but they had been given to us and they had a value; and the checklist and the accountability on that was so strong. I was absolutely there, and I actually processed some of these, on myself and others, a statement of charges if things were lost and they were under your care; and sometimes they were accidental and they would find out what happened and you would be cleared because it got run over accidentally in a training exercise. But there was no doubt in my mind somebody was watching, and I was accountable, and my commander, for every single piece of equipment. And this was back in 1989 when you had the big green printout sheets that would come.

With the ability we know now to organize data, it seems amazing to me, because every month a random inventory, a partial inventory of our whole inventory would come out to us and we would have to physically sign off at the end. It behooved you to be organized, to know where this was and to know there was a day of reckoning if it was not there.

My question is, especially on a large scale like that—there were thousands of armories across the United States, and if you don't think these inventories were detailed, it was down to every single socket in tool kits, and if you didn't have the 3/16th socket, no matter what else you had, somebody wanted to know about it and somebody was going to pay for it.

So my question to you is, it seems to me the ability to do this and the best practices and the checklist are out there. We had to close the shop at the end of the day; that included security of the primitive technology at the time. But it was locked in the vault, it was signed off, it was secured; and when I opened that vault, my signature went on that. And those sheets were checked when someone would come through, and we didn't brush you off because when someone came to say they were going to look, we had to provide it and knew we had to provide it.

So my question to you is, I know the ability to deliver this, at least I feel, is there; and I know that the culture at that time was for me to make sure I delivered it.

Is there anything about what I am saying on this that is applicable to the VA?

Mr. WILLIAMS. I will start by saying, in addition to having responsibility for the financial management at the VA, I also have responsibility for financial management at the Department of Defense and Homeland Security, so I am familiar with those property books that you are talking about.

No, you are not being unreasonable in anything that you said, because I see that type of activity taking place now at the various agencies I have responsibility for. There are other problems as far as having good systems to keep track of those property books and all that we have reported on, but that process is one that can be done, and it is not something that you have to do everything, wall to wall, at one time.

There are various ways in which you can rotate doing that inventory, maybe this unit this month, this unit that month, and so forth. If it is looking like it is going to interfere with your operations, you just shut everything down and try to do it.

There are various ways that it can be done, but nothing you have said is unreasonable to expect, nothing that you have said is unreasonable, and in my mind that couldn't be done to get this accountability down to the individual levels and have individuals accountable for the property that has been assigned to them.

Mr. WALZ. And I guess my final question is, just thinking of how these things rolled down as we have issues. After the breach in the laptop computer and the 26 million individual records, or roughly what the number was, we saw—I think VA and the government responded, and what they did was, they started strengthening those Health Insurance Portability and Accountability Act rules, making sure privacy was there. And now I see what I think is an unintended consequence in our county service officers who are having a hard time accessing the VA system in terms of they now have to get the sign-off from them for power of attorney and those types of things.

I am wondering, have we gone over on that or is that just part of strengthening this system?

Mr. WILLIAMS. That is something you have to look at. When you are looking at a control environment and you are putting controls in place, you have to look at everything from a cost-benefit standpoint, and you don't want to put anything in place that is actually going to cost you more than the benefits that you are going to expect to derive. So it is a balancing act.

Mr. WALZ. I thank you.

And I yield back, Mr. Chairman. Thank you.

Mr. MITCHELL. Thank you.

Ms. Brown-Waite?

Ms. BROWN-WAITE. The one question that I was going to ask, which may be very similar, is, in our offices we are required to keep track of anything over $500 as part of the inventory. Is part of VA's problem that a lot of the missing equipment was under not $500, but $5,000, that it was never actually inventoried before? Is that part of the problem?

Mr. WILLIAMS. Part of the problem is that a lot of these items are under that $5,000 window that we are talking about. But we did find some items missing that were over the $5,000 amount. But there are a lot of computers and things along this line that cost $2,000, $1,000, what have you. These are items that you can easily walk out the door with, and that is why we feel that it is important that, as we recommended, I think, in the 2004 report, you properly identify those items that are sensitive and less than $5,000 and make sure you put the controls in place so that those items that can easily walk out the door, that you have got some controls around them so you know where they are and you have got individuals that are accountable for those individual items.

Ms. BROWN-WAITE. When I asked about the dollar amount and found out that it is $5,000 for inventory for the VA, I was told that they inventory vehicles, ammunition, weapons, canines. What is the value of a canine? And the reason I am asking this is, think

about it, that canine is not going to jeopardize anyone's security out there. But I just find it very strange that that was the response that we got.

Mr. WILLIAMS. I will be honest with you, I asked my staff the same question before the hearing today from the standpoint of—well, my first question was, am I properly pronouncing this? I thought it was maybe some other type of equipment. But my understanding is that these are valuable assets that are used in the process of carrying out VA operations, so they are actually classified as assets that fall into that sensitive category as defined by VA.

Ms. BROWN-WAITE. I am sure that they are. My canine at home is priceless. But the point being that while my Bentley at home may be priceless—that is my dog's name, not my vehicle—certainly the canines do not have identifying information that could be misused; and I guess I am questioning the priority of the inventory.

Mr. WILLIAMS. Yes.

Ms. BROWN-WAITE. And I just found it so totally strange that canines are inventoried, but computers aren't. Laptops and Blackberries and other things aren't. The average citizen out there is asking, What the heck is going on up there?

I thank you very much.

Mr. WILLIAMS. Thank you.

Mr. MITCHELL. Mr. Walz, any other questions?

Mr. WALZ. I just had one more question and I may know this answer, but I am going to get it from the experts.

What I am reading on the San Diego facility, it talked about the personnel there created their cuff records. Can you tell me what that is?

Ms. FISCHER. They were maintaining cuff records at San Diego and at VA headquarters, and these were records maintained outside the central inventory system for various reasons. At San Diego, the IT staff did not have access to the property system, so they felt the need to keep their own records to show when they removed a computer for repair or moved one to another location, so they could track it.

They were trying to keep accountability there. The problem was, they didn't have access to the central system, so they couldn't update the central system for those changes; and so the central inventory system was out-of-date because of that.

Mr. WALZ. But it would be unfair to characterize this as a second set of books?

Ms. FISCHER. It was, in fact, a second set of records. Both sets of records, the central system and the cuff records, are considered official records.

Mr. WALZ. Okay.

Mr. WILLIAMS. I would add, if you are looking at a good control environment, you would want the records to be in your main system, you wouldn't want to be relying on cuff records. You would like to have it in your official system in a good, internal control environment.

Mr. WALZ. Very good.

Ms. FISCHER. The cuff records were on somebody's personal computer on a spread sheet.

Mr. WALZ. They were making an effort at accountability because the system was hindering them from doing what they needed to do.

Ms. FISCHER. They were the only ones that had access to the records they created, so they weren't available for management information.

Mr. WALZ. Thank you.

I yield back, Mr. Chairman.

Mr. MITCHELL. Thank you very much. Thank you for your testimony and for being here today.

At this time I would like to welcome Panel 2 to the witness table. Mr. Robert T. Howard is the Assistant Secretary for Information and Technology at the VA and the Department's CIO. Assistant Secretary Howard is a former Major General in the Army Corps of Engineers and joined the VA in 2006 to head up the IT reorganization project. The Subcommittee has been most happy with Mr. Howard's progress in this project, but we understand that there is still a long way to go. We look forward to hearing Assistant Secretary Howard's testimony.

And, Mr. Howard, would you please introduce the rest of your staff?

STATEMENTS OF HON. ROBERT T. HOWARD, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND HON. ROBERT J. HENKE, ASSISTANT SECRETARY FOR MANAGEMENT, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY ADAIR MARTINEZ, DEPUTY ASSISTANT SECRETARY, INFORMATION PROTECTION AND RISK MANAGEMENT, OFFICE OF INFORMATION AND TECHNOLOGY; ARNIE CLAUDIO, DIRECTOR, INFORMATION TECHNOLOGY OVERSIGHT AND COMPLIANCE, OFFICE OF INFORMATION AND TECHNOLOGY; RAY SULLIVAN, DIRECTOR OF FIELD OPERATIONS, OFFICE OF INFORMATION AND TECHNOLOGY; SANDFORD GARFUNKEL, DIRECTOR, VETERANS INTEGRATED SERVICE NETWORK 5, VETERANS HEALTH ADMINISTRATION; LARRY BIRO, DIRECTOR, VETERANS INTEGRATED SERVICE NETWORK 7, VETERANS HEALTH ADMINISTRATION; FERNANDO O. RIVERA, DIRECTOR, WASHINGTON, DC, VA MEDICAL CENTER, VETERANS HEALTH ADMINISTRATION; AND STEVE ROBINSON, CHIEF, ACQUISITION AND MATERIEL MANAGEMENT SERVICE, WASHINGTON, DC, VA MEDICAL CENTER, VETERANS HEALTH ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF HON. ROBERT T. HOWARD

Mr. HOWARD. Yes, sir. Thank you, Mr. Chairman. I would like to thank you for the opportunity to testify on IT asset management within the Department of Veterans Affairs.

Mr. MITCHELL. Is your microphone on?

Mr. HOWARD. Yes, sir. Anyway, I do thank you for the opportunity to testify today on IT asset management within the Department of Veterans Affairs.

I am joined today by Mr. Bob Henke, Assistant Secretary For Management, and I am also accompanied by Ms. Adair Martinez,

my Deputy Assistant Secretary for Information Protection and Risk Management; Mr. Ray Sullivan, my Director of Field Operations; Mr. Arnie Claudio, my Director of IT Oversight and Compliance.

In the group behind me are Mr. Sandford Garfunkel, Director of Veterans Health Administration's (VHA's) Veterans Integrated Services Network (VISN) 5; Mr. Larry Biro, of VISN–7, Mr. Fernando Rivera, Director of the Washington, DC, VA Medical Center; and Mr. Steve Robinson, Chief Acquisition and Materiel Management Service for the Washington, DC, VA Medical Center.

Sir, IT asset management is a critically important issue that also, as you have mentioned, has a direct bearing on our ability to enhance information protection throughout VA. As you know, the recent GAO report on VA's IT asset management found inadequate controls and risk associated with threat, loss and misappropriation of IT equipment at selected VA locations. In that report, GAO found inadequate accountability and included a number of very important recommendations with which we agree.

As the Chief of Information and Technology for VA, I am responsible for ensuring compliance with the integrity and security of VA's IT assets. I understand that when poor IT inventory procedures exist, both the loss of expensive equipment as well as the loss of any sensitive information resident in the equipment could occur.

This is a situation of the utmost importance. It is a situation that we are working hard to remedy. We are prepared to answer your questions today about procedures that already exist, as well as more rigorous and standard procedures that are being implemented.

The GAO findings demonstrate a need for more emphasis and vigilance in this area. With the establishment of a single IT authority in the VA we are now in a much better posture to improve the IT asset management situation, and we have a number of actions already under way. We currently have several systems in VA that capture IT assets, and we are working to standardize this and move to a single IT management system.

We have been able to locate some of the equipment that was reported missing. For example, regarding the items of missing equipment that were assigned to the previous Office of Information and Technology, we have been able to locate most of them. We assembled a team to conduct a search for missing items—network equipment servers, digital cameras, and so forth—that were assigned to the Office of Information and Technology prior to the consolidation of IT in the VA.

At the end of this review, which took place over a 3-month period, the team had located about 90 percent of the equipment; and though much of the equipment was found, the lack of accountability was clearly evident. You should not have to go through that in order to find your equipment.

To improve our asset management and accountability within VA, a special team has been established to develop standard procedures; a new directive and accompanying handbook on the control of information technology equipment within the VA have been prepared, and we have already implemented some of the procedures

they describe. The directive and handbook will provide clear direction on all aspects of IT asset management.

Additionally, we have expanded the responsibility of my Office of Information Technology Oversight and Compliance. This office was established in February of 2007 to conduct on-site assessments of IT security, privacy and records management at VA facilities. As of today, the office has completed over 58 assessments, and the oversight of physical security for IT assets is now a part of their assessment routine. The results of the reviews will help us support and strengthen VA IT security controls.

This office ensures that facilities are aligned with the National Institute of Standards and Technologies' recommended security controls for Federal information systems.

We must also increase awareness at the individual user level regarding accountability for IT equipment. The new directive and handbook mentioned earlier will require employees who have been assigned VA IT equipment to sign a receipt for the IT equipment in their possession. Supervisors will be held responsible for common equipment that is not assigned to individuals. The receipt used is the printout of the equipment inventory list which describes equipment assigned to employees by name. These procedures have already been implemented.

We have begun to deploy network monitoring software. This is a very critical aspect of this issue, sir, that will help us detect and monitor any device that is connected to the VA network. Special procedures are also being implemented for equipment that may be considered expendable, but which must be accounted for, not because of the cost, but because the equipment has the potential for storing sensitive information. An example of such low-cost IT equipment that must be tracked are the encrypted thumb drives being distributed throughout the VA.

In closing, I want to assure you, Mr. Chairman, that we will remain focused in our efforts to improve all aspects of the information technology environment in VA, including the overall accountability and control of IT equipment, as well as certain medical equipment that could potentially store sensitive information.

It is about the sensitive information that we are particularly concerned. This will not only reduce the loss of expensive equipment, but also the potential loss of sensitive information the equipment may contain.

Thank you for your time and the opportunity to speak to you on this issue and we would be pleased to answer any questions you may have.

Mr. MITCHELL. Thank you, Mr. Howard.

[The prepared statement of Mr. Howard appears on p. 38.]

Mr. MITCHELL. Mr. Henke, do you care to make a statement?

STATEMENT OF HON. ROBERT J. HENKE

Mr. HENKE. Sir, just two or three brief points and then we will turn to your questions, if you don't mind.

Sir, from my perspective as the agency's Chief Financial Officer, any internal control deficiency, whether it is material or not to our financial posture, our financial statements, has my attention.

First, in the GAO report, we concurred on all 12 of the recommendations and moved to change our policies and purchase card policies and modify our inventory system to add user level accountability to it.

The second thing I would like to point out is that my internal auditors also do property reviews at VA medical centers. We have visited 14 medical centers to date this year, and in some of their findings they found stations that have zero discrepancies—zero discrepancies on their equipment inventories. What that tells me is that this can be done with the right amount of management attention. Salt Lake City, Utah, zero percent discrepancies; Muskogee, Oklahoma, 3.2 percent discrepancies; Wilmington, Delaware, 4.5 percent. So with management attention it can be done.

Number three, we are going through a Sarbanes-Oxley-type process we're in year 2 of a 3-year process where we look at internal controls over our financial reporting. One of the processes we are looking at this year is property and equipment. We had some results come back, fairly mixed results. We told the teams, the national auditors we have and my auditors, to go out and do more site assessments and come back with more information.

Finally, sir, I would like to point out that you mentioned, and Ms. Brown-Waite mentioned, the 2005 and 2006 inventories that were being done. We have results for 2007 to date, on inventories, and we can speak to those. The results are very different, and I can speak to the point that I believe the institution has gotten religion about accounting for IT equipment.

Mr. MITCHELL. Thank you. I just have a couple questions.

Mr. Howard, your organization has devoted a great deal of time to ensuring that the personal data of veterans is protected from disclosure. Encryption of the data is one of the main defenses against disclosure; do you agree with that?

Mr. HOWARD. Yes, sir.

Mr. MITCHELL. If GAO reports that your inventory records are incomplete and inaccurate, how do you know if all IT equipment requiring encryption has been encrypted?

Mr. HOWARD. Sir, not all the IT equipment has been encrypted. In fact, some of it, we cannot encrypt. An example of that is IT equipment that is actually a part of a medical device that we cannot necessarily place encryption.

I would agree with you that encryption is an extremely important tool and we need to encrypt everything we possibly can, but there are some items that you can't, which means there are other methodologies you have to follow.

The basic rule that we have established in the VA is that sensitive equipment—sensitive information, rather, must be in a protected environment at all times or it must be encrypted. What I mean by that is, for example, if the Veterans Benefit Administration—they deal with paper, lots of paper; you can't encrypt it. But you also must protect it in a protected environment—listings of names and Social Security numbers, and what have you.

So although encryption is an extremely important tool, and we are expanding that to the maximum possible degree, it is not the final answer. You still have to have some procedures that must be followed where encryption can't help you.

Mr. MITCHELL. Thank you. Let me ask a further question here. Are you aware of a single instance in which the problems with the VA inventory system that the GAO has very clearly identified that have existed for years have resulted in any disciplinary action by anyone at the VA.

Mr. HOWARD. Sir, we got into that discussion this morning. The answer is "yes." I don't know about disciplinary, but I will tell you that people have been held pecuniarily liable for missing equipment; I don't know the numbers per se, but I do know that that is true.

Mr. MITCHELL. All right. One last question before I turn it over.

GAO's review of physical inventories performed by the locations tested in 2004 and 2005 and its 2007 audit found the test location reported significant loss of IT equipment as a result of their own inventories. In particular, the Los Angeles Medical Center reported losses of 8,402 items with an original acquisition value of nearly $12.5 million.

Please explain, if you can, how a single medical center managed to lose $12 million worth of IT equipment.

Mr. HOWARD. I don't know specifically what occurred at that particular facility. But what we see, quite frankly, are a number of the items that you have addressed earlier. And that is the movement of items; the equipment may be there, but it is moved somewhere else and you lose track of it. The real question is, is it truly missing or has it been moved somewhere else.

And the numbers—for example, in my own organization, in last August of 2006 internal, right after the May breach, we directed an internal inventory take place. About 1,900 items could not be located to the amount of almost $8 million. We put a team to run around try to find that stuff, and brought it down to about 440 items, which we will implement a report and survey on.

Now we should not have had to do that, but it gives you an idea of how transient this equipment is and very easy to move around. Which brings me to the point that it is not only going around with a clipboard or a scanner; software—you know, network monitoring software, is absolutely critical to solving this problem, because the equipment is too mobile. If it moves down the hall and gets plugged into the network, you need it see that right away. And there is software out that we will actually have deployed in certain parts of the VA that is tremendously helpful in keeping track of this item of equipment.

With respect to the particular facility involved, it is probably a combination of things, poor inventory procedures, as well as not keeping up with the inventory on a quarterly basis.

Mr. MITCHELL. What kind of actions are you taking to correct those problems?

Mr. HOWARD. If you want me to describe the new procedures we are putting in place, I can do that. It is different from the way it is handled right now.

Mr. MITCHELL. Maybe after everyone has a chance. My time is up.

Mr. HOWARD. Okay.

Mr. MITCHELL. Ms. Brown-Waite?

Ms. BROWN-WAITE. I thank the Chairman.

Mr. Henke, the last time you were here I realized what a difficult job you have, and that is changing the culture at VA.

GAO, in its report, stated that the VA's purchase card, credit card, does not require IT equipment bought with the purchase card to be reported to property management officials, and as a result there is no assurance of any kind of accountability over this equipment. GAO has reported that this is a continuing problem at VA headquarters.

Why did the VA wait until GAO came out with this report before taking action?

Mr. HENKE. Ma'am, this is actually the subject we discussed at our last hearing when Mr. Walz asked me what things we can could do better and differently on the purchase cards.

What we have done is changed—the policy already existed in the property policy that you need to inventory things that are sensitive or above $5,000. It simply wasn't reflected in the purchase card policy. That is not to say that people shouldn't have been doing it.

There was a policy out that said, if you buy a piece of gear, it doesn't matter how you buy it, you buy it with a purchase card or not, you have to put a bar code on it and inventory it. So this was just tightening up one of the holes we found in our policies for purchase card holders to make these purchases.

Another step that we have taken is—in part of consolidation of IT is, Mr. Howard has determined that there were too many purchases being made on purchase cards of IT equipment that were nonstandard. So we shut that down. He said, no more IT purchases using the purchase card; it was too loose. Those are the two steps we have taken to remediate that.

Ms. BROWN-WAITE. General Howard, I understand there is one facility in the GAO report which did not include computer equipment valued under $5,000 in its last inventory.

Which facility was this and under which VISN is that?

Mr. HOWARD. Ma'am, I believe that was VISN–16, Houston. I believe it was the result of improper instructions that took place.

Ms. BROWN-WAITE. And what sort of direction from the VISN or to the VISN has been given?

Mr. HOWARD. Ma'am, I am not sure how that situation has been corrected. There is clear instruction regarding sensitive items. In fact, there is a memo that Mr. McFarland and Tim McClain signed out on October of 2005 that listed and discussed equipment that was less than $5,000. So the instruction is clear; there is a directive that goes all the way back to that timeframe about what sensitive items are that must be included in inventories. In fact, we are now expanding that list as part of our new procedures.

Ms. BROWN-WAITE. Is it standardized now? If you don't know where the equipment is, how do you know what is on the laptops?

Mr. HOWARD. Ma'am, you are exactly right. The items of equipment that are listed in the previous memo that I just mentioned, the directive from October 2005 does cite personal computers and other equipment that we understand in IT; in fact, most of it is IT-type equipment, but it is not complete enough. The list that we have now is much more extensive, that we intend to follow.

Ms. BROWN-WAITE. Let me also follow up with a question that I asked the GAO and that is about a board of survey in the VA

to take possible disciplinary action as a result of loss, damage or destruction of property.

Has this been formulated? Is anyone responsible? Because let me tell you that when I owned a business, if I gave one of my employees a computer, they clearly knew that that was their responsibility. But apparently this responsibility level just doesn't appear to be evident at the government level. So tell me exactly what is being done.

Mr. HOWARD. There have been reports of survey and people have been held pecuniarily liable. I don't know about the disciplinary part, but the requirement to pay has occurred.

To what extent, I don't have that information right now, ma'am. We can get that for you.

Ms. BROWN-WAITE. Mr. Chairman, I would like to ask them to get that information to the Committee so we can know that accountability at the user level is truly taking place, because—and you guys need to convey that clearly. Here is a computer, here is a BlackBerry; it is your responsibility not to lose it, not to misplace it. You are going to be held financially responsible.

I think the Subcommittee deserves to know that information, who actually has been held responsible, personal responsibility.

Thank you. With that I yield back.

[The following information was provided by VA:]

A request was made to provide Representative Brown-Waite with a list of those employees who have been held pecuniary liable for lost and/or damaged VA equipment VA-wide.

The Veterans Health Administration (VHA), Prosthetics and Clinical Logistics Office (10FL) consulted with the Office of General Council regarding the release of a list of employee names associated with this request. We were advised that the Privacy Act protects information retrieved by a person's name or other identifier. Therefore, VA cannot disclose such information without the prior written consent of an individual, or unless another exception applies. One exception permits disclosure to either House of Congress, 5 U.S.C. § 552a(b)(9).

The Office of Management and Budget is charged by law with implementing the Privacy Act, and has determined that Section (b)(9) does not authorize the disclosure of a Privacy-Act protected record to an individual member of Congress (see OMB Guidelines, 40 Federal Register 28,948 and 28,955). Thus, the exception provides authority to disclose records only to requests from Chairs of Congressional Oversight Committees for authorized oversight purposes. To that end, we offer the attached summary and spreadsheet containing the requested data (see attachments).

[The attachment is being retained in the Committee files.]

Mr. MITCHELL. Thank you.

Mr. Walz?

Mr. WALZ. Thank you, Mr. Chairman. And thank you, General Howard, for being here. And thank you for your service, and thank you for taking on at a difficult time. I know you have been on your job slightly longer than I have been on mine here. You came at a critical time, you came at a time when expectations for change were very high.

I think the same could be same for Mr. Henke, and I appreciate your taking on this challenge; and I hope in the spirit of why we are here, working together. The ultimate outcome is all that matters, taking care of our veterans the best that we possibly can while safeguarding taxpayer dollars and resources.

So in that spirit, just a couple of things I wanted to ask. How do you think the GAO did on this report? In your opinion, how do you view it? Do you think it was a fair assessment of what is happening, and is it going to be helpful in helping correct this?

Mr. HOWARD. Sir, the GAO is always fair.

Sir, it is clearly going to help us, there is no doubt about that. Not only reports like this that put emphasis on very significant problems that we must deal with, but our own internal efforts.

I mentioned the oversight and compliance that Arnie Claudio has been doing, the SOC reports. Quite frankly, we know who is losing computers and we—in fact, we have got a whole list of that, as the Subcommittee does. You were provided the weekly summaries and we can pull that information from our database to find out what is happening with this particular piece of equipment. In fact, we have already started to collect that information; I don't have it right now, but the point is that oversight examination is very, very important.

But, sir, I would like to add one thing. The oversight and the examinations, investigations, highlight the problem, but sometimes we understaff support-type activities. Organizations tend to do that. I don't know for sure. I am looking very hard through the new IT organization.

As you know, we own all the IT folks and we are examining what we have. Where are they? Do we need more or less, or do we need to move people around? And my guess is that this area of IT, of asset management, is not adequately staffed; that is my personal opinion, and we are looking hard at that.

Mr. WALZ. That is what we need to know. I want you to know that that is what we see as our responsibility. We need to know what you need. I would say that the willingness of this Subcommittee to listen and work together is probably almost boundless, except for the one I know puts a huge constraint on you is time and patience on this right now. I know that you need those things to a certain degree, but my question to you might be, what do I tell my veterans in Minnesota, what is going on, and reassure them of the faith, and that is what we are looking for. So I really appreciate your attitude on that.

This one might be better for Mr. Sullivan. I just wanted to know if you could give me—what would it look like for me as an employee at any of the facilities, how would I start the day getting into my technology and how would I end the day?

I know in my office the computers are shut off, they are backed up, they are password secured; and anything that is done behind that is done with the rolling passwords on the key chain thing.

I am just wondering what would it look like out there in the VA system?

Mr. SULLIVAN. Exactly the same for us. You would need to come in in the morning. You would need to go through your password authentication. If you step away from your computer for any length of time or you don't use it, it goes into automatic lock mode, and you would need to come back and unlock it. At the end of the day you would log off your computer. We tend to leave our computers turned on so we can do automatic patching and assessment at night.

Some of the tools that we are talking about, we build an inventory when you log on so we know that you have a computer, we know where it is physically in that building. If it disappears from the network for a long period of time, it could be that it was turned off, but it sends an alert, so we can follow up.

Those are the technologies we are looking to standardize across the Agency.

Mr. WALZ. Where is this equipment going? Is this theft or is this misplacement?

Mr. HOWARD. Sure, some of it is theft. But theft is a minor problem; I think the bigger problem is keeping up with it.

Let me give you a good example, computers excessed—in fact, Ray could probably pile on a little more on this. Computers that are excessed, are no longer useful, some previous operating system or whatever; you know yourself that is pretty fast, the turnover of equipment like that.

Mr. WALZ. Right.

Mr. HOWARD. We have to go through certain procedures. We have to pull the hard drive, you have to cleanse it forensically, which means several times, it is a 4-hour drill to go through and clean that off. But then the equipment may get offered to redistribution within the VA, redistribution among other government agencies, redistribution to charity institutions. And you have to go through all these, just so. It is sitting there in the room as you go through all these procedures; you can't just get rid of it necessarily, you have to follow these procedures. And, quite frankly, sir, that is taking us too long, we need to move quicker on that.

Ray can tell you instances where he knows for sure items were turned in as excess, no longer required, and they sat there for long periods of time. That means the IT community and the logistics disposal community need to work hand-in-glove to make sure there is follow-up.

To do that, I intend to energize my ISOs, Information Security Officers, to do that follow-up with the material management people who handle the redistribution of assets. That is kind of out of our hands at that point. Very important capability, but it is part of the problem that we need to get our arms around.

Mr. WALZ. Thank you.

And I yield back, Mr. Chairman.

Mr. MITCHELL. Thank you.

Mr. Henke, you are the Assistant Secretary For Management, and Mr. Howard, you are the Assistant Secretary For Information and Technology, and yet neither of you, as I understand it, has line authority over the logistic folks at the medical centers and other facilities who are responsible for inventory. Is that a problem?

Mr. HOWARD. Sir, let me take that. Not for me, because I do have line authority over the CIOs. And the procedure that I mentioned to you before—I can now summarize that if you would like, the procedure that we will put in place. But it starts with the director of the facility—the director of the facility does not work for me, but they are responsible for all activities that occur at the facility, to include all the equipment that is there, the people, everything.

But it doesn't stop there. In fact, we have already implemented the procedure where the CIO, the senior IT official at the facility,

is the custodian of IT equipment, the guy who works for me, up through Ray Sullivan. And I do have authority over that person, believe me.

What does he or she do? It doesn't stop there either, because he or she, working with the director, has to designate custodians at the very service levels. The head of radiology, you are responsible for the IT equipment that is in your jurisdiction.

Now, the CIO and the IT people at that facility assist in it, but the CIO has got to take a very active role at the facility level to include mandating that individuals sign for their individual equipment and that the service chief, be it the head of radiology or whatever, signs for the common equipment that cannot necessarily be assigned to a particular individual.

That is the procedure that we are putting in place. In fact, Ray is responsible for the directive and handbook; it is in draft, but we have already implemented the procedures. I have told my people, don't wait on this thing, you do it. We actually have this working group together with the administrations and the staff agencies and Bob's people. We are in agreement that this is the direction we need to go.

But, sir, the software also has to be implemented, that Ray described earlier, to contract this stuff because it can move around so easily. One computer is down the hallway, but—all of a sudden, you lost it, but boom, when you stick it in the network, it shows right up again. This is extremely important for an all-encompassing solution.

Mr. MITCHELL. Thank you very much.

This question is for Mr. Biro.

Mr. BIRO. Yes?

Mr. MITCHELL. You are the Director for VISN–7. I have been told you decided to take this inventory issue very, very seriously and do something about it; is that correct?

Mr. BIRO. Yes.

Mr. MITCHELL. And would you tell us what you did?

Mr. BIRO. Well, I have only been in VISN–7 for 4 months. It started with VISN–7 at Birmingham, with the loss of data at Birmingham. They started an inventory that was very thorough, and I continued to support having that inventory completed, which took in over 55,000 items with focus on those that had PII, personal identifiable information.

We were down to about less than 20,000 items. For the items we couldn't find, my contribution is that, I asked for a second inventory; and we used teams of both information systems people and facility people, and we also mixed those teams up so they came from different facilities. So in 3 weeks, we knocked that list down to less than 500 items.

My other contribution is that, I am insisting on reports of survey that have been talked about over and over again, be completed on that final missing equipment list, and that the appropriate disposition take place on that equipment, that we pursue this to the end. That is going to be done within less than 30 days; they are winding those down.

To your question, then, we will look at if we can find people that need to be held accountable for that through that process. Every-

thing that has been said we have—we have software, the best way to find the equipment. Much of it is seeing where it has been used last and where it has been, because it moves all over. The biggest problem is the portability of it, but a lot is detective work. This is the kind of detective work I use in 7, and I also was using in 19. Everywhere I have worked, something has been cited and as best practice.

Salt Lake City has a perfect inventory. I used to work in VISN–4; they have a very good inventory. So it is paying attention to details and insisting on that high level of performance.

Mr. MITCHELL. Thank you. Sometimes this Subcommittee has a reputation for being very hard on the VA. We all want what is best for the veterans and taxpayers; they deserve nothing but excellence. Although we may be demanding, I really want to recognize what you deserve, and that is congratulations on the work that you are doing. You are a positive example of what can be done, and I want to thank you for that.

Also, is there any reason why what you have done in VISN–7 couldn't be done at other VISNs?

Mr. BIRO. No, there is no reason. My fellow—other 20 network directors are working on this very hard. We just got some direction today—some more. Internal controls are extremely important, and we are working on them. I am known as the leader of that effort.

Mr. MITCHELL. Thank you very much.

Mr. BIRO. So I am working on it.

Ms. BROWN-WAITE. If Mr. Garfunkel could come forward, please, I understand that you recently were promoted to VISN–5 directorship. I guess congratulations are in order.

I also understand that you were the last Director of Washington's VA Medical Center where the most current GAO report wasn't too kind about the way IT inventory was managed there.

Would you care to comment on why your last facility's IT inventory sample indicated 28 percent missing items, 80 percent incorrect user organization identifiers and 57 percent incorrect location of the equipment?

Mr. GARFUNKEL. Yes, ma'am, thank you.

First of all, no matter what I say, let me say these numbers are totally unacceptable. In the 2004 GAO audit, we had something like an 87 percent "couldn't locate the equipment"; that was down to 28 percent. I am very glad to say, as of April 2007, we now are at 4 percent.

So we have taken this audit very seriously. As GAO has testified, we now have personnel hand receipts responsible through class 3 software that was developed and we have lots of equipment that was—in fact, we know was surplussed in previous years—that should have been taken off the equipment inventory lists (EILs), that we thought were taken off the EILs, and it turns out that they were not.

So we have done the reports of survey that have identified those issues, and I think we have taken very swift and definite action since that time to assure that we have a good system in place to identify this equipment.

Ms. BROWN-WAITE. So what you are saying is, you were at 87 percent missing?

Mr. GARFUNKEL. I believe the 2004 audit was something like 87 percent missing, yes.

Ms. BROWN-WAITE. And the 28 percent found this time is good?

Mr. GARFUNKEL. No, ma'am.

Ms. BROWN-WAITE. And all of a sudden, we are down to 4 percent?

Tell me why the great discrepancy between what GAO found and what you are trying to convey to us now that is down to 4 percent.

Mr. GARFUNKEL. Well, since the GAO audit, we identified which equipment was, in fact—that we know, in fact, was surplussed. We bar-coded our equipment and the doors so we know what—by scanning the door, we know where the equipment is located. And we know what equipment belongs in there, so we can identify all the equipment.

We have begun the process of having individuals sign for their individual pieces of equipment, so they will be held responsible for it.

Ms. BROWN-WAITE. When did this procedure go into effect? Because obviously between 2004 and now it is—there were some pretty sloppy procedures going on.

Mr. GARFUNKEL. Yes, ma'am, they were pretty sloppy procedures, although obviously there was improvement from the 2004 audit.

We face lots of issues. I don't want to make a lot of excuse for it. We implemented some actions. We identified the equipment we had that is no longer on station; we know what happened to it, and we have now put some very strong processes in place.

Mr. Claudio came to our facility in, I believe, February, and while he had some recommendations, he felt we had pretty good processes in place for IT security.

Ms. BROWN-WAITE. Now, is it accurate that in the new VISN that you have four hospitals and 15 Community Based Outpatient Clinics?

Mr. GARFUNKEL. I believe that is correct, ma'am, yes.

Ms. BROWN-WAITE. And how long have you been VISN Director?

Mr. GARFUNKEL. A couple months.

Ms. BROWN-WAITE. And you don't know for sure?

Mr. GARFUNKEL. No—it is correct, yes.

Ms. BROWN-WAITE. Well, obviously I hope that the lack of accountability at the other center here at Washington VA Medical Center is not going to be continued in your new role as VISN director.

What practices are you putting into effect in VISN that you are now the director of?

Mr. GARFUNKEL. Well, I think we are certainly going to follow Mr. Biro's example to make sure we have 100 percent wall-to-wall inventory at every facility. The VA at Maryland healthcare system, they are doing that over the next couple of weeks. We will implement the process of hand receipts as new policies come out, and we will make sure these inventories are done on a regular basis.

Obviously, this issue has my attention and I will make sure it has the attention of medical directors and others and make sure we do the best job we can.

Ms. BROWN-WAITE. Mr. Henke or Mr. Howard—I don't know who to ask this of, so—are we going to have standard procedures

throughout the VA so that Mr. Biro's best management practices are carried out throughout the entire VA? Are we going to have all of these separate accounting systems out there that will be a future problem for you all?

Mr. HOWARD. Ma'am, we are moving to a centralized system. It will take time. I think you know that there are various systems used; VHA uses one system, National Cemetery Administration another, there are differences.

Several weeks ago the deputy secretary made the decision on the new enterprise-wide asset management application called Maximo; that is the one that we will begin to implement, that is for all assets. However, in the IT arena, we will need a supplement to that. The reason for it is, for normal asset management you need numbers: You need where it is, you need how much it costs, when you got it, that sort of stuff. For IT, you need much more information: What is on the device, is there any software, is it up to date, any personal identifiable information. You need to be able to see inside the item of equipment and know much more.

So we need to augment that enterprise capability with the IT asset management system. And, in fact, we have got an request for information (RFI) on the street right now to get feedback on—we know what is out there; in fact, we already have licenses for some of these items.

Nevertheless, we have got an RFI on the street. We need that capability to augment the asset management enterprise solution that is being put in place. We are talking about a process that we have to go through to remove the existing systems and introduce the new system that will take place, a Web-based system.

Ms. BROWN-WAITE. Do you have a time line? As soon as that question is answered, I will yield back.

Mr. HOWARD. On the Maximo, I think it is about a year and a half.

Bob?

Yeah. Actually, the Maximo implementation is part of Bob's organization, it is part of the FLITE program, the Financial Logistics Integrated Technology Enterprise program—the logistic subset is what I am now speaking to—that will interface with the financial system that is the other very important part.

The IT system that we use must be able to feed that, it must provide feeds of certain elements of data that can, in turn, be linked to the financial system. That is where we are heading. It will go beyond a year, that is for sure; it is very, very complicated. That is because we have to remove the existing systems as we implement the new one.

Ms. BROWN-WAITE. Thank you.

Mr. MITCHELL. Mr. Walz?

Mr. WALZ. Thank you, Mr. Chairman. Just one more question.

Again, it goes back to if this Subcommittee wants to provide anything that we can provide, but the time and patience thing is starting to wear on people. I am just noticing on the GAO report that the Tampa, Florida, inventory—am I right, that that is not completed? 14 months, ongoing, it is showing?

Mr. HOWARD. Sir, I am not sure on Tampa exactly where that stands, but the procedures for the inventory process, the way it

currently should work, it is a rolling inventory. In other words, each quarter—in fact, those were the documents that we provided the Committee today to indicate where the folks are in terms of their inventories. Every quarter, they are supposed to have so much done and they sign off on that and send it in to headquarters. The folks that you are referring to, sir, have been doing that.

We have the first two quarters of 2007, the reports—I believe we have them. Bob is looking at them right here; in fact, we have a little color code here. Obviously, if you are green, you are up to speed, you have in excess of 90 percent of your inventory done for the quarter.

We have a few red folks who may not be keeping up to speed, and these reports are provided by VHA, in this case, every quarter.

Mr. WALZ. The thing that counsel is talking to me about is, the data I am getting is, you are showing "unknown," it is showing "number of missing items, unknown"; "acquisition of missing items, unknown"; "data on report of survey, not yet prepared."

What you are saying is, there is information supplementing this that we don't have or I haven't been given?

Mr. HENKE. Yes, sir, you are looking at—the facility performed audits in 2005 and 2006, found discrepancies, they have a report, they have to survey it off the books, they have to get rid of it, find it, reconcile.

What we have here is a current status across VHA of fiscal year 2007 inventories; it tells me that we have got to date.

If I could——

Mr. WALZ. But this would not have an outside eye like GAO looking at it? This would still be internal?

Mr. HENKE. That is my understanding, sir. Those are the internal audits that Tampa did during 2005 and 2006 in their clean-up work to bring those to closure, to rest and do the surveys——

Mr. WALZ. It is safe to say at the 14-month period they were not done?

Mr. HENKE. I believe that is correct, if my review of the report is accurate.

Mr. WALZ. Am I wrong to think that is a long time?

Mr. HENKE. You are not.

Mr. HOWARD. No. 2006, we know there were some that didn't make it; they were in the red category.

Mr. HENKE. One more datapoint. For current information, through the second quarter, we across VHA had planned to inventory 4,000 equipment lists—not 4,000 items but 4,000 lists of equipment. We performed 90 percent of those, so 3,618 lists were inventoried. The results came back and we had—out of 391,000 pieces of equipment on those lists, we came back missing 0.85 percent, so that's significantly different from 2005 and 2006 reports that you may be looking at. So it shows focus on the effort.

Mr. WALZ. So there is a curve that says it is improving and that is what we will see.

Mr. HENKE. Yes, sir. Management's attention is focused on it to get the problem solved.

Mr. WALZ. I yield back, Mr. Chairman.

Mr. MITCHELL. Anything else anybody would like to add?

Let me just say, I appreciate your candidness and your work. As I said earlier, what we are here to do is to try to make sure that the veterans get what is due to them, delivery of services, as well as the taxpayers not getting shortchanged. We are concerned about excellence in all these fields.

We are also very pleased to hear that what you are doing seemed to be in the right direction. Let me just say part of the name of this Subcommittee is "oversight and investigations." We are not here—it seems to me to find out what laws need to be made, but is seems we are talking about policies that you can implement and policies that you can do and carry out for the betterment of veterans, as well as taxpayers.

We appreciate that effort and what you are doing, and I just want you to know what we can do is investigation and oversight, and we are looking to the GAO to help us out. Hopefully, when we come back with another report, things are great.

Ms. BROWN-WAITE. Mr. Chairman, I would ask to be able to ask one other question and that is of General Howard.

What other VISNs actually have exhibited some proactive, rather than reactive, initiatives to really address what appears to have been a, hopefully in the past, laissez faire or lackadaisical approach to IT control? What other VISNs are exemplary?

Mr. HOWARD. Ma'am, one for sure, in addition to Larry Biro in VISN–7; Max Lewis up in VISN–20 is doing a very good job. I would cite that VISN; in fact, that is where Ray Sullivan plants himself, that is where his office is up there in the Pacific Northwest.

Ms. BROWN-WAITE. So we have two that are truly being proactive?

Mr. HOWARD. Yes, ma'am. There are others, but those come to mind.

Ms. BROWN-WAITE. How do we get the message across to them that the taxpayers do care about the inventory and the dollars that we are being asked every year to increase for VA?

And when some of my colleagues talk about waste, fraud and abuse, I know some of the equipment is just—when someone else left, someone else picked up that computer and started using it, but you know, getting a handle on this is important. It is not just the equipment dollars, it clearly is also the availability on those computers, of identifying information that—if you don't know where the IT equipment is, you don't know what is on it and it is missing, you don't know what you are missing. That is part of the problem.

And getting that message out there is certainly our job, but it certainly is your job. I would just encourage to you do that, do a best management practices, get them moving. I know that culture in the VA is very difficult to jump-start, but you need to do it, you absolutely need to do it gentlemen.

Mr. MITCHELL. Thank you. This concludes our hearing, and I appreciate very much all the witnesses being here today and thank you again.

Mr. HOWARD. Thank you, sir.

Mr. HENKE. Thank you.

[Whereupon, at 3:41 p.m., the Subcommittee was adjourned.]

APPENDIX

Prepared Statement of Hon. Harry E. Mitchell,
Chairman, Subcommittee on Oversight and Investigations

This hearing will come to order.

Thank you all for coming today. I am pleased that so many folks could attend this oversight hearing on VA information technology inventory issues. We know that VA has serious problems with keeping track of its IT inventory. This is not just a dollar issue, although it certainly is that. It is also a security and privacy issue. VA's inventory deficiencies mean that VA cannot ensure that private medical and other information belonging to the nation's veterans remains private.

We are going to begin today by hearing from the General Accounting Office concerning GAO's report, *Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation*, released just today, showing the results of its testing of inventory systems and procedures at four VA locations. The results are not pretty. As you can see from the chart, the sample locations GAO tested show that from 6 to 28 percent of IT items listed as being in inventory could not be located. The Washington, DC VA medical center could not find an astonishing 28 percent of the IT items on inventory. The missing items at the four locations had a combined value of $6.4 million.

Sad to say, this is not a recent problem. In July 2004 GAO reported that the six VA medical centers it audited did not have reliable property databases. GAO followed up on these sites as part of its current report and concluded that more than $13 million in IT equipment was still missing from those sites. Incredibly, an inventory being conducted by one of the sites in response to the 2004 GAO report is still not completed.

If this were not bad enough, GAO further reports that VA has seriously flawed policies and procedures. Again, the chart illustrates the extent of the problem. One line says "incorrect user organization"—that means the inventory system incorrectly identified to whom the equipment was assigned. Look at the numbers—80 percent at the Washington DC medical facility, 69 percent in Indianapolis, and 70 percent in San Diego. VA's central headquarters does better—"only" 11 percent, but more than makes up for this with the physical location of 44 percent of its IT equipment misidentified in its inventory database.

The issue of security could not be better illustrated than by the photograph you see over there. That photograph is of an IT equipment storeroom at VA's central headquarters. It seems hardly necessary for GAO to have pointed out that this storeroom did not meet VA's requirements for motion intrusion detection, alarms, secure doors, locks, and special access keys.

Security is no small matter, and we are not concerned only about hardware. GAO found hard drives at two of the four locations that were designated as excess property to be disposed of that still had hundreds of veteran names and Social Security numbers. This is completely unacceptable.

I can assure you, we will all be back here. We intend to ask GAO to conduct another check of VA's inventory system in a few months time, and if another hearing turns out to be necessary, we will have one.

Last week, Ms. Brown-Waite and I sent a letter to the VA requesting copies of the most recent annual equipment inventory certification letters from all facility directors. We also requested a list of all facility directors who did not provide certification for completing their annual inventories. I would like to thank the VA for their prompt response to this request.

Prepared Statement of Hon. Ginny Brown-Waite, Ranking Republican Member

Thank you, Mr. Chairman for yielding.

Mr. Chairman, my goal for this hearing is not just to learn where VA is relative to their current IT inventory management, but to learn where and how they are working to improve security, controls, maintenance and management of their IT equipment. The July 2007 GAO report, increased my growing concerns over VA's control over its inventories, from reading the weekly SOC.

The GAO report selected four specific sites for their report. During this study, fewer than half of the items GAO selected for testing could be located, and most of the items were information technology (IT) equipment. GAO found that the four VA locations reported over 2,400 missing IT equipment items, valued at about $6.4 million, identified in inventories performed during fiscal years 2005 and 2006. Missing items were not always reported right away, and in some cases, not for several years. At one of the locations, 28 percent of the items surveyed during the GAO audit were missing.

Mr. Chairman, I find this lack of control over equipment completely unacceptable. Here in the House of Representatives, our acquisition offices perform annual equipment inventories in all offices. The Chief Administrative Officer's staff comes into our offices either to tag equipment we have received, remove equipment we no longer use, or inventory the equipment under our control. By keeping a centralized acquisition and inventory process, the House is able to maintain tight control over its equipment inventory. Given the results of the GAO report, it appears the VA is unable to do likewise.

According to the GAO report, there is also a lack of user-level accountability for IT equipment, due to weak overall control of the equipment environment. The IT personnel and IT coordinators do not have possession (physical custody) of all IT equipment under their purview, therefore, they are not held accountable for IT equipment determined to be missing during physical inventories. In my opinion, Mr. Chairman, there needs to be accountability for inventories from the Chief Executive Officer clear down the line to the user who is ultimately using the product.

The weekly SOC reports consistently show missing IT related items from the VA's inventories, whether it is listing old equipment that possibly had been disposed of after it was no longer of use to the VA, or new equipment that had been stolen. I am heartened to note that the VA is working with local and federal law enforcement to track down and retrieve newer stolen equipment, but dismayed to see the number of equipment items that were either transferred to other facilities and not tracked, or disposed of without the proper notation in the equipment inventories.

As of February 28, 2007, the GAO report found the four case study locations covered in their 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 VA performed during fiscal years 2005 and 2006. Based on information GAO obtained through March 2, 2007, the five case study locations previously audited had identified over 8,600 missing IT equipment items with a combined original acquisition value of over $13.2 million. GAO reported that the missing IT items represent record keeping errors, the loss, theft or misappropriation of IT equipment. The GAO also cited that because most of the nine case study locations had not consistently performed required annual physical inventories or completed Reports of Survey promptly, which prevented the reporting of missing IT equipment in some instances for several years. I am always surprised when I see a SOC reporting the first instance of listing a missing piece of IT equipment from the mid-nineties. Operating Systems for this equipment would be totally out of date long ago, and it leaves me wondering just how long the equipment was actually missing before reported on the SOC.

Mr. Chairman, this is not the first time that GAO has reported on deficiencies in information technology equipment controls. In July 2004, GAO issues a report titled *VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement*. In this report, GAO indicated that the six VA medical centers they 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. One of the medical centers reviewed, was also reviewed in the most recent report, and yet issues remain. I look forward to hearing from today's witnesses, and those who are accompanying them on how the VA is going to move forward to gain tighter control over its inventory, and how they plan to follow up on GAO's recommendations.

Thank you, and I yield back my time.

Prepared Statement of McCoy Williams, Director, Financial Management and Assurance, U.S. Government Accountability Office

GAO HIGHLIGHTS

Lack of Accountability and Control Weaknesses Over IT Equipment at Selected VA Locations

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. In light of these concerns and recent thefts of laptops and data breaches at VA, this testimony focuses on (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's companion report (GAO–07–505), released with this testimony, includes 12 recommendations to improve VA-wide policies and procedures with respect to controls over IT equipment, including record keeping 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.

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.

Control failures	Washington, DC, medical center	Indianapolis medical center	San Diego medical center	VA headquarters offices
Missing items in sample	28%	6%	10%	11%
Incorrect user organization	80%	69%	70%	11%
Incorrect user location	57%	23%	53%	44%
Record keeping 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. 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.

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 inves-

tigate 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.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to discuss our recent audit of controls over information technology (IT) equipment at the Department of Veterans Affairs (VA). In light of reported weaknesses in VA inventory controls and reported thefts of laptop computers and data breaches, the adequacy of such controls has been an ongoing concern. Today, I will summarize the results of our recent work, the details of which are included in our audit report, which the Subcommittee is releasing today.[1] This audit followed a July 2004 report[2] in which we identified weak practices and lax implementation of controls over equipment at the six VA medical centers we audited. As a result, personnel at the VA medical centers 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.

For today's testimony, I will provide the highlights of our current findings related to

- the risk of theft, loss, or misappropriation[3] of IT equipment[4] at selected VA locations;
- whether selected VA locations have adequate procedures in place to assure physical security and accountability over IT equipment in the excess property disposal process;[5] and
- what actions VA management has taken to address identified IT equipment inventory control weaknesses.

My statement is based on our report on VA IT inventory controls, which you are releasing today.[6] As part of our audit, we statistically tested IT equipment inventory at selected case study locations. In addition, our investigator inspected physical security at IT equipment storage sites. 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.

Summary

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. Our estimates of the percentage of inventory control failures related to these missing items ranged from 6 percent at the

---

[1] GAO, Veterans Affairs: Inadequate Controls over IT Equipment at Selected VA Locations Pose Continuing Risk of Theft, Loss, and Misappropriation, GAO-07-505 (Washington, DC: July 16, 2007).

[2] GAO, VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement, GAO-04-755 (Washington, DC: July 21, 2004).

[3] As used in this testimony, 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.

[4] For the purpose of our test work, 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 testimony, 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.

[6] GAO-07-505.

Indianapolis medical center to 28 percent at the Washington, DC, medical center.[7] In addition, we determined that VA property management policy does not establish accountability with individual users of IT equipment. Consequently, our control tests identified 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, we concluded that for the four case study locations we audited, essentially no one was accountable for IT equipment.

Our analysis of the results of physical inventories performed by the current four case study locations[8] identified over 2,400 missing IT equipment items, with a combined original acquisition value of about $6.4 million. In addition, the five other locations we previously audited had reported over 8,600 missing IT equipment items with a combined original acquisition value of over $13.2 million. Further, we found that missing IT items were often not reported for several months and, in some cases, several years, because most of the case study locations had not consistently performed physical inventories or completed Reports of Survey[9] promptly.

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.[10] However, file dates on the hard drives we tested indicated that some of them had been in the disposal process for several years without being sanitized, creating an unnecessary risk of compromising sensitive personal and medical information. We also found numerous unofficial IT equipment storage locations in VA headquarters area office buildings that did not meet VA physical security requirements. For example, at some VA headquarters locations, excess computer equipment was stored in open or unsecured areas.

Since our July 2004 report, VA management has taken some actions and has other actions under way to strengthen controls over IT equipment, including clarifying property management policies[11] and centralizing functional IT units under the new Chief Information Officer (CIO) organization. Even with these improvements, the department had not yet established and ensured consistent implementation of effective controls for accountability of IT equipment inventory, and IT inventory responsibilities 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. Our companion report released today includes 12 recommendations to VA to improve the overall control environment and strengthen key internal control activities and to increase attention to protecting IT equipment used in VA operations. VA generally agreed with our findings, noted significant actions under way, and concurred on the 12 recommendations.

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 locations we tested. As summarized in table 1, our statistical tests of key IT inventory controls at our four case study locations found significant control failures. None of the case study locations had effective controls to safeguard IT equipment from loss, theft, and misappropriation.

---

[7] Each of these estimates has a margin of error, based on a two-sided, 95 percent confidence interval, of ±7 percent or less.

[8] The Washington, DC, medical center was covered in both audits.

[9] 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.

[10] VA information resource management (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.

[11] VA Handbook 7127/4 § 5302.3, "Inventory of Equipment in Use."

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

Control failures	Washington, DC, medical center	Indianapolis medical center	San Diego medical center	VA headquarters offices
Missing items in sample	28%	6%	10%	11%
Incorrect user organization	80%	69%	70%	11%
Incorrect user location	57%	23%	53%	44%
Record keeping 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. 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.

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. Such information could include names and Social Security numbers protected under the Privacy Act 1974[12] and personal health information accorded additional protections from unauthorized release under the Health Information Portability and Accountability Act 1996 (HIPAA) and implementing regulations.[13] Although VA property management policy[14] 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 for IT equipment. Instead, these locations relied on information about user organization and user location, which was often incorrect and incomplete. 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

Our statistical tests of IT equipment existence at the four case study locations identified a total of 123 missing IT equipment items. The 123 missing IT equipment items included 44 at the Washington, DC, medical center; 9 at the Indianapolis medical center; 17 at the San Diego medical center; and 53 at VA headquarters. Our statistical tests of missing equipment found that 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 compromising sensitive personal data maintained on computer hard drives. The 123 missing IT equipment items included 53 that could have stored sensitive personal information, including 19 from the Washington, DC, medical center; 3 from the Indianapolis medical center; 8 from the San Diego medical center; and 23 from VA headquarters. Because of a lack of user-level accountability and the failure to consistently update inventory records for inventory status and user location changes, VA officials at our test locations could not determine the user or type of data stored on this equipment and therefore the risk posed by the loss of these items.

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,[15] the three medical centers we tested assigned accountability for most IT equipment to their information resource management (IRM) or IT Services organizations, and VA headquarters organizations tracked IT equipment items through their IT inventory coordinators. However, be-

[12] Privacy Act 1974, codified, as amended, at 5 U.S.C. § 552a.
[13] HIPAA, Pub. L. No. 104–191, § 264, 110 Stat. 1936, 2033–34 (Aug. 21, 1996). The Secretary of Health and Human Services has prescribed standards for safeguarding medical information in the HIPAA Medical Privacy Rule. See 45 C.F.R. pt. 164.
[14] VA Handbook 7125, Materiel Management General Procedures, § 5003 (Oct. 11, 2005).
[15] VA Handbook 7125, Materiel Management General Procedures, § 5003.

cause these personnel 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. Because of this weak overall control environment, we concluded that at the four case study locations essentially no one was accountable for IT equipment.

Absent user-level accountability, accurate information on the using organization and location of IT equipment is critical to maintaining effective asset visibility and control over IT equipment items. However, as table 1 shows, we identified high failure rates in our tests for correct user organization and location of IT equipment. Because property management system inventory records were inaccurate, it is not possible to determine the timing or events associated with lost IT equipment as a basis for holding individual employees accountable.

Although our *Standards for Internal Control in the Federal Government*[16] requires timely recording of transactions as part of an effective internal control structure and safeguarding of sensitive assets, we found that VA's property management policy[17] 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.

Errors in IT Equipment Inventory Status and Item Description Information

We found errors related to the accuracy of other information in IT equipment inventory records, including equipment status (e.g., in use, turned-in, disposal), serial numbers, model numbers, and item descriptions. As shown in table 1, estimated overall error rates for record keeping were lower than the error rates for the other control attributes we tested. Even so, the errors we identified affect management decision making and create waste and inefficiency in operations. 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 Survey information on identified losses of IT equipment. 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, $12.4 million of which was identified at the Los Angeles medical center. 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 record keeping 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. Although physical inventories should be performed over a finite period, at most of the 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. According to VA Police and security specialists,[18] it is very difficult to conduct an investigation after significant amounts of time have passed because the details of the incidents cannot be determined.

The timing and scope of the physical inventories performed by the case study locations varied. For example, the Indianapolis medical center had performed annual physical inventories in accordance with VA policy for several years. The Washington, DC, medical center performed a wall-to-wall physical inventory in response

[16] GAO, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1 (Washington, DC: November 1999).

[17] VA Handbook 7127/3, Material Management Procedures, pt. 1, § 5002–2.3, and VA Handbook 7127/4, Material Management Procedures, pt. 4, § 5302.3.

[18] 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.

to our July 2004 report. 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. In addition, the San Diego and Houston medical centers had not followed VA policy for including sensitive items, such as IT equipment valued at less than $5,000, 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 at our four case study locations 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 at two medical centers had required motion detection alarm systems and special door locks. We also found numerous instances of informal IT storage areas at VA headquarters that 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 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

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 and 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 hundreds of unique names and Social Security numbers on VA headquarters computers and detailed medical histories with Social Security numbers on computer hard drives at the San Diego medical center. Our limited tests of hard drives that were identified as having been subjected to data sanitization procedures did not find data remaining on these hard drives. 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 noted excessive delays—up to 6 years—in performing data sanitization once the computer systems had been identified for disposal, posing an unnecessary risk of losing the sensitive personal and medical information contained on those systems.

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, requiring storerooms to have walls to ceiling height, overhead barricades that prevent "up and over" access from adjacent rooms, motion intrusion detection alarm systems, and 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; however, we identified deficiencies related to lack of intrusion detection systems at the Washington, DC, and San Diego medical centers and inadequate door locks at the Washington, DC, medical center. In response to our findings, these facilities initiated actions to correct these weaknesses.

We also found numerous informal, undesignated IT equipment storage locations that did not meet VA physical security requirements. For example, at the VA headquarters building, our investigator found that the physical security specialist was unaware of the existence of IT equipment in some storerooms. Consequently, these storerooms had not been subjected to required physical security inspections. Further, 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. The wall opening into the storeroom had yellow tape labeled "CAUTION" above the doorway. The storeroom was within an IT work area that had dropped ceilings that could provide "up and over" access from adjacent rooms, and it did not meet VA's physical security requirements for motion intrusion detection and alarms and secure doors, locks, and special access keys. In another headquarters building, we observed excess IT equipment stacked in the corners of a large work area that had multiple doors and open access to numerous individuals. We also found that VA headquarters IT coordinators used storerooms and closets with office-type door locks and locked filing cabinets in open areas to store IT equipment that was not cur-

rently in use. The failure to provide adequate security leaves the information stored on these computers vulnerable to data breach.

Status of VA Actions to Improve IT Equipment Management

Mr. Chairman, although VA strengthened existing property management policy[19] 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, additional actions are needed to establish effective control in this area. For example, pursuant to recommendations made in our July 2004 report, VA updated its property management policy to clarify that IT equipment valued at under $5,000 is to be included in annual inventories. However, as noted in this testimony and described in more detail in our companion report, VA had not taken action to assure that these items were, in fact, subjected to physical inventory. In addition, the new CIO organization has no formal responsibility for medical equipment that stores or processes patient data and does not address roles or necessary coordination between IRM and property management personnel with regard to inventory control of IT equipment. The Assistant Secretary for Information and Technology, who serves as the CIO, told us that the new CIO organization structure will include 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. To assure accountability and safeguarding of sensitive IT equipment, effective implementation will be key to the success of VA IT policy and organizational changes.

Our companion report released today made 12 recommendations to VA to strengthen accountability of IT equipment and minimize the risk of theft, loss, misappropriation, and compromise of sensitive data. These included recommendations for revising policies related to record keeping requirements to document essential inventory events and transactions, ensuring that physical inventories are performed in accordance with VA policy, enforcing user-level accountability for IT equipment, and strengthening physical security of IT equipment storage locations. VA management agreed with our findings and concurred with all 12 recommendations. In VA's written comments provided to us, it noted actions planned or under way to address our recommendations.

Concluding Remarks

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 agency wide 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 disciplinary action for any lost equipment; 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. We appreciate VA's positive response to our current recommendations and planned actions to address them. If effectively implemented, these actions will go a long way to assuring that the weaknesses identified in our last two audits of VA IT equipment will be effectively resolved in the near future.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you may have at this time.

Contacts and Acknowledgments

For further information about this testimony, please contact McCoy Williams at (202) 512–9095 or williamsm1@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Major contributors to this testimony include 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; Lori B. Tanaka; Chris J. Rodriguez; Special Agent Ramon J.

[19] VA Handbook 7127/4, Materiel Management Procedures (Oct. 11, 2005).

Rodriguez; and Danietta S. Williams. In addition, technical expertise was provided by Keith A. Rhodes, Chief Technologist, and Harold Lewis, Assistant Director, Information Technology Security, Applied Research and Methods.

Prepared Statement of Hon. Robert T. Howard, Assistant Secretary for Information Technology and Chief Information Officer, U.S. Department of Veterans Affairs

Thank you, Mr. Chairman. I would like to thank you for the opportunity to testify on IT asset management within the Department of Veterans Affairs. I am joined today by Mr. Robert J. Henke, Assistant Secretary for Management. I am also accompanied by:

- Ms. Adair Martinez, my Deputy Assistant Secretary for Information Protection and Risk Management
- Mr. Ray Sullivan, my Director of Field Operations
- Mr. Arnie Claudio, my Director for IT Oversight and Compliance
- Mr. Fernando O. Rivera, Director of the Washington DC VA Medical Center and
- Mr. Steve Robinson, Chief Acquisition and Materiel Management Service for the Washington DC VA Medical Center

IT asset management is a critically important issue that also has a direct bearing on our ability to enhance information protection throughout VA. As you know, a recent GAO report (GAO report 07–505) on VA's IT asset management found inadequate controls and risk associated with theft, loss, and misappropriation of IT equipment at selected VA locations. In that report, GAO found inadequate accountability and included a number of important recommendations—with which we agree.

As the Chief Information Officer for VA, I am responsible for ensuring compliance with the integrity and security of VA's IT assets. I understand that when poor IT inventory procedures exist, both the loss of expensive equipment, as well as the loss of any sensitive information resident on the equipment, could occur. This is a situation of the utmost importance. It is a situation that we are working hard to remedy. I am prepared to answer your questions today about procedures that already exist, as well as more rigorous and standard procedures that are being implemented.

The GAO findings demonstrate a need for more emphasis and vigilance in this area. With the establishment of a single IT authority in the VA, we are now in a much better posture to improve the IT asset management situation and have a number of actions already underway. We currently have several systems in VA that capture IT assets, and we are working to standardize this and move to a single IT asset management system.

We have been able to locate some of the equipment that was reported missing. For example, regarding the items of missing equipment that were assigned to the previous Office of Information and Technology organization, we have been able to locate most of them. We assembled a team to conduct a search for missing items (e.g. network equipment, servers, digital cameras, and so forthetera) that were assigned to the Office of Information and Technology prior to the consolidation of IT in VA. At the end of this review, which took place over a 3-month period, the team had located about 90 percent of the equipment and although much of the equipment was found, the lack of accountability was clearly evident.

To improve our asset management and accountability within VA, a special team has been established to develop standard procedures. A new Directive and accompanying Handbook on the *Control of Information Technology Equipment within the VA* have been prepared and we have already implemented some of the procedures they describe. The Directive and Handbook will provide clear direction on all aspects of IT asset management.

Additionally, we have expanded the responsibilities of my Office of Information Technology Oversight and Compliance. This office was established in February 2007 to conduct on-site assessments of IT security, privacy and records management at VA facilities. As of today, the office has completed over 58 assessments. The oversight of physical security for IT assets is now a part of their assessment routine. The results of the reviews will help us support and strengthen VA IT security controls. This office ensures that facilities are aligned with the National Institute of Standards and Technology's recommended security controls for Federal Information Systems.

We must also increase awareness at the individual user-level regarding accountability for IT equipment. The new Directive and Handbook, mentioned earlier, will

require employees, who have been assigned VA IT equipment, sign a receipt for the IT equipment in their possession. Supervisors will be held responsible for common equipment that is not assigned to individuals. The receipt used is the printout of the Equipment Inventory List, which describes equipment assigned to employees by name. These procedures have already been implemented. We have also begun to deploy network monitoring software that will help us detect and monitor any device that is connected to the VA network.

Special procedures are also being implemented for equipment that may be considered "expendable" but which must be accounted for, not because of the cost, but because the equipment has the potential for storing sensitive information. An example of such low-cost IT equipment that must be tracked are the encrypted thumb drives being distributed throughout the VA.

In closing, I want to assure you Mr. Chairman that we will remain focused in our efforts to improve all aspects of the Information and Technology environment in the VA—including the overall accountability and control of IT equipment. This will not only reduce the risk of loss of expensive equipment but also the potential loss of sensitive information the equipment may contain. Thank you for your time and the opportunity to speak on this issue. I would be happy to answer any questions you may have.

Congress of the United States
Washington, DC
July 24, 2007

Dear Members of the House Veterans' Affairs Committee Subcommittee on Oversight and Investigations,

I would like to submit for the record my most sincere apologies for my absence this afternoon. An unexpected family emergency has called me away from my Congressional duties. While I would like very much to be in attendance to review the GAO and VA testimony regarding IT Inventory Management, I must attend to my daughter who has fallen ill.

I appreciate your understanding on this matter. Please know that I remain committed as ever to the important work of this Subcommittee and those that is serves.

Sincerely,

Zack Space
Member of Congress

Statement of the Hon. Cliff Stearns,
a Representative in Congress from the State of Florida

Mr. Chairman,

Thank you for holding this very important hearing regarding inventory management of the VA's IT equipment. I have long been concerned regarding the security of personal information at the VA, particularly with regard to the immediate need to equip each laptop with basic security encryption. However, there is a critical oversight we must address before we can fully encrypt all VA laptops, and that is we do not know how many laptops there are to secure! The VA has yet to complete a full and accurate accounting of all its IT equipment and systems. Without that, it is a fool's errand to pursue real IT security.

On February 28, 2007, we heard testimony from Mr. Gregory Wilshusen of the GAO that the Department of Veterans Affairs needed to address longstanding weaknesses in its IT security. He testified that the GAO had made several recommendations in 2002 for improving security management, including the basic restriction of access to IT equipment and network to only authorized users. However, Mr. Wilshusen summarized that, "In the auditors' report on internal controls prepared at the completion of VA's 2006 financial statement audit, information technology security controls were identified as a material weakness because of serious weaknesses related to access control, segregation of duties, change control, and service continuity. These areas of weakness are virtually identical to those that we had identified years earlier." And here we are again to hear basically the same testimony as a result of yet another investigation of IT security by the GAO.

In its most recent report, the GAO stated that the six VA medical centers it audited lacked a reliable property control database and had problems with implementation of VA inventory policies and procedures. They then make several rec-

ommendations, such as clarifying existing policy regarding sensitive items that must be accounted for in the property control records; providing a more comprehensive list of the type of personal property assets that are considered sensitive for accountability purposes; and reinforcing the VA's requirement to attach bar code labels to agency property. Unfortunately, GAO's tests of physical inventory controls at four VA locations identified 123 missing IT equipment items that could have stored sensitive data, including 53 missing computers! At these locations, investigators discovered there were over 2,400 missing IT equipment items, totaling around $6.4 million. Immediate reporting of missing items as recommended by the GAO in 2002 is clearly not followed through in practice, as many missing items were not reported for several months and, in some cases, several years.

This dangerous mix of a lack of user accountability and hopelessly inaccurate records creates an environment that will lead to further loss of equipment, and makes another security breach highly likely. For these IT security weaknesses to have been identified and yet unaddressed for over five years is frankly inexcusable. I look forward to hearing from our panel of witnesses regarding what steps they are taking now to correct this problem, and how they will work to ensure that this round of recommendations are implemented department wide.

Thank you.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE, 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, GAO–07–505

GAO Highlights

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

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 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, DC	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%
Record keeping 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.

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.

What GAO Recommends

GAO makes 12 recommendations to improve VA-wide policies and procedures with respect to controls over IT equipment, including record keeping 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.

CONTENTS

	Page
Letter	45
Results in Brief	46
Background	48
Inadequate IT Inventory Control and Accountability Pose Risk of Loss, Theft, and Misappropriation	51
Physical Security Weaknesses Increase Risk of Loss, Theft, and Misappropriation of IT Equipment and Sensitive Data	60
VA Actions to Improve IT Management and Controls Have Been Limited	63
Conclusions	64
Recommendations for Executive Action	64
Agency Comments and Our Evaluation	65
Appendix I: Objectives, Scope, and Methodology	65
Appendix II: Comments from the Department of Veterans Affairs	68
Appendix III: GAO Contact and Staff Acknowledgments	72
Tables	
Table 1: Current IT Equipment Inventory Control Failure Rates at Four Test Locations	52
Table 2: Number of Missing IT Equipment Items at Four Test Locations, Including Items That Could Have Stored Sensitive Information	53
Table 3: Number of Missing IT Equipment Items by Headquarters Office and Missing Items That Could Have Stored Sensitive Personal Data and Information	55
Table 4: Estimated Percentage of IT Inventory Control Failures Related to Correct User and Location at the Four Test Locations	56
Table 5: Estimated Percentage of Other IT Inventory Record Keeping Failures at Four Test Locations	57
Table 6: Summary of Physical Inventories and Missing IT Equipment Identified by the Four Current Case Study Locations as of February 28, 2007	59
Table 7: Summary of Physical Inventories and Missing IT Equipment Identified by Five Case Study Locations Previously Audited as of March 2, 2007	60
Table 8: Population of VA IT Equipment at Locations Selected for Testing	66
Table 9: Number of Computer Hard Drives in the Property Disposal Process Selected for Testing at Four Locations	67
Figures	
Figure 1: VA's IT Property Management Process	49
Figure 2: Photograph of Unsecured IT Equipment Storeroom in the VA Headquarters Building	62

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 1982
HHS: Department of Health and Human Services
HIPAA: Health Information Portability and Accountability Act 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

U.S. 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 reported [1] 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 inventories [2] 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 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 misappropriation [5] 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 dis-

[1] GAO, *VA Medical Centers: Internal Control over Selected Operating Functions Needs Improvement,* GAO–04–755 (Washington, DC 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.*

[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.

posal 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 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, DC, 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.

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, DC, 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 lo-

[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.

[7] The Washington, DC, 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.

[9] GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD–00–21.3.1 (Washington, DC 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.

cations, 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.

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 Survey [11] 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 record keeping 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 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 imple-

[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.

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

mentation 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 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, DC, 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—VIHA, 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.

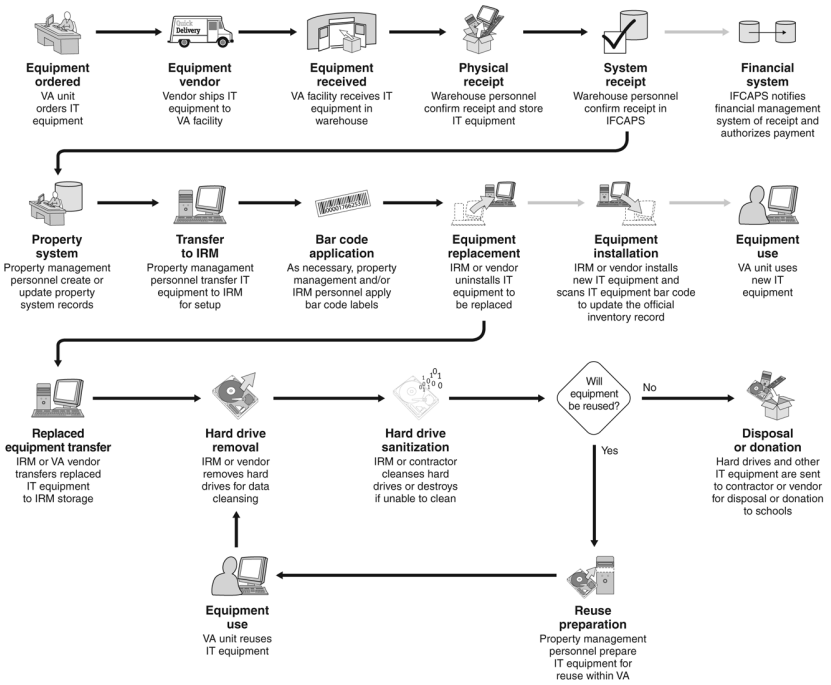
VA's IT Property Management Process

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.

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]

[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 1982 (FMFIA), and GAO/AIMD–00–21.3.1.

Figure 1—VA's IT Property Management Process



Source: GAO.

Request and Ordering of IT Equipment

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, DC, 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 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,

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

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 (ElL) 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.

Physical Inventories of IT Equipment and Reports of Survey

VA policy[18] 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 policy[19] 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, elec-

[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.

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

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

tronic notification is given to property management and IRM personnel, who use this documentation to ensure 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 1974[20] and, when information concerns an individual's health, the Health Insurance Portability and Accountability Act 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 Eraser™. IRM personnel complete VA Form 0751, "Information Technology Equipment Sanitization Certification," to document the erasing of the hard drives. Hard drives that Data Eraser™ 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 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 organiza-

[20] Privacy Act 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 healthcare 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.

[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.

tion, (3) inaccurate information on user location, and (4) other record keeping errors. None of the case study locations had effective controls to safeguard IT assets from risk of loss, theft, and misappropriation.

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

Control failures	Washington, DC, 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 location	57%	23%	53%	44%
Record keeping 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. 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 1974[24] and information concerning an individual's health is accorded additional protections from unauthorized release under HIPAA and implementing regulations.[25] Although VA property management policy[26] 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 that VA's property management policy[27] 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.

[24] Privacy Act 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).
[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.

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

Test Results	Washington, DC, medical center	Indianapolis medical center	San Diego medical center	VA headquarters
Number of missing items in each sample	44	9	17	52
Total missing items that could have stored sensitive data	19	3	8	23

Source: GAO analysis.
Note: After we completed our analysis, Washington, DC, 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 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.

Washington, DC, Medical Center

Our physical inventory existence testing at the Washington, DC, medical center identified an estimated 28 percent failure rate[28] 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 policy[29] that implements federal records management law and NARA guidance[30] 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, DC, medical center, 9 items related to the 550 older IT equipment items of questionable status. Washington, DC, 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 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, DC, 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.

[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.

With regard to the use and type of data stored on the 19 computers that our tests identified as missing, Washington DC, 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 percent[31] 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 record keeping errors. The user of the third item, a computer, was not known.

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 policy[32] 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 visibility[33] 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 percent[34] 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 use or if any of these items were lost, stolen, or misappropriated. VA property management policy[35] 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.

---

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

[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.

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

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 offsite 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 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 rate[36] 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	27 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.
[a] All other includes 17 additional VA headquarters organizations. The missing item in this category related to the Human Resource Management Office.

[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 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

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

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

Officials told us they use hand receipts[39] 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 offsite. We received nine hand receipts—one that had expired, six that were dated after the date of our request, and two 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, DC, medical center officials initiated actions to establish user-level accountability for individual employees and unit heads who have shared workstations. In March 2007, Washington, DC, 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.

Table 5—Estimated Percentage of Other IT Inventory Record Keeping Failures at Four Test Locations

Test Location	Inventory status information	Serial number	Item description	Total failures
Washington, DC, 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

[38] The margin of error, based on a two-sided, 95 percent confidence interval is ±3 percent.

[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.

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 Survey[40] information on identified losses of IT equipment. VA policy[41] 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 record keeping 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.

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, DC, 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

[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.

[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.

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, 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, DC, medical center	2005 thru 2006	Mar. 2006 thru Oct. 2006	1,133	$1,758,096
Indianapolis medical center	2005 2006	Dec. 2004 Oct. 2006	6 112	$23,206 $79,230
San Diego medical center*	2005 2006	Dec. 2004 Ongoing	42 15	$135,344 $24,418
VA headquarters offices	2006 and ongoing	Not yet finalized	1,162	$4,385,444

Source: GAO analysis.
*The 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, DC, 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 locations[43] 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 rec-

[43] The Washington, DC, medical center was covered in both audits.

ommendations; and (3) complete, within established timeframes, 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.

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	Original items 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.
[a] The 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 three 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 1974[45] and personal medical information accorded additional protections under HIPAA[46] 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.

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, DC, and San Diego medical center IRM equipment storerooms lacked motion intrusion detection alarm systems and the Washington, DC, medical center IRM storeroom did not meet door locking requirements. Based on our investigator's find-

[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 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.

ings, physical security specialists at the San Diego and Washington, DC, medical centers told us they have recommended that required intrusion detectors be installed in their IRM storerooms. In addition, the Washington, DC, 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 policy[47] 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 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 policy[48] 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.

---

[47] VA Handbook 7127/4, Materiel Management Procedures (Oct. 11, 2005).
[48] Universal Serial Bus (USB) Flash Drive User Guide 2.0 (Mar. 9, 2007).

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 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 timeframes 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 walkthroughs 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, DC, VA medical center-that had the most significant problems identified in our July 2004 report and two other geographically 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, DC, 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.
[a] Includes 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, DC, 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.

---

[1] GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD–00–21.3.1 (Washington, DC: 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 1982, to issue standards that provide the overall framework for establishing and maintaining internal control.

[2] GAO, *Internal Control Management and Evaluation Tool,* GAO–0l–1008G (Washington, DC: 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.

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 (Le., 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 record keeping 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 medical centers	Drives with data	Sanitized drives	Total
Washington, DC	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, DC
June 22, 2007

Mr. McCoy Williams
Director
Information Management Issues
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20540

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 win 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 nine 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.

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 an 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

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.

- **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 online 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 win expeditiously assign the Report of Survey to a Survey Board to determine if the 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 tl1em in performance of their job. Supervisors are also responsible for any property not directly assigned to an individual employee in their area.

O/A'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 win 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 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 rath-

er 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 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 frontline 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.**

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:

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 tile 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.

COMMITTEE ON VETERANS' AFFAIRS

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
July 20, 2007

Honorable R. James Nicholson
Secretary
U.S. Department of Veterans Affairs
810 Vermont Ave., NW
Washington, DC 20420

Dear Secretary Nicholson:

On Tuesday, July 24, 2007, the Subcommittee on Oversight and Investigations of the House Committee on Veterans' Affairs will conduct a hearing on *IT Inventory Management.* This hearing will be held at 2:00 PM in room 334 Cannon House Office Building.

The Subcommittee requests the most recent equipment inventory certification letters from all facility directors. We also would like a list of any facility directors who did not the latest annual provide certification for completing their annual inventories.

Please contact Geoffrey Bestor, Esq., Staff Director of the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, at (202) 225–3569 if you have any questions.

Sincerely,

HARRY E. MITCHELL
Chairman

GINNY BROWN-WAITE
Ranking Republican Member

[The information was provided to the Subcommittee and will be retained in the Committee files.]