Department of Veterans Affairs

Office of Inspector General

Evaluation of Alleged Information Technology Equipment Mismanagement and Privacy Act Violations at the VA Loma Linda Healthcare System

Information Technology Service and the Materiel Management Section needed to improve equipment inventory control procedures.

Report No. 04-00856-31 December 2, 2005

VA Office of Inspector General
Washington, DC 20420

Department of Veterans Affairs
Office of Inspector General
Washington, DC 20420

TO: Director, VA Loma Linda Healthcare System (605/00)

SUBJECT: Evaluation of Alleged Information Technology Equipment Mismanagement and Privacy Act Violations at the VA Loma Linda Healthcare System

Summary

The Office of Inspector General (OIG) evaluated allegations related to the mismanagement of information technology (IT) equipment and possible violations of the Privacy Act of 1974 at the VA Loma Linda Healthcare System. The anonymous complaint received by the OIG's Hotline Division alleged that: (1) the healthcare system's IT Service had not inventoried IT equipment and certified the accuracy of inventory records in over 2 years, (2) a complete "Report of Survey"[1] (ROS) investigation for $991,000[2] of missing IT equipment had not been performed and the equipment was removed from inventory records without explanation, (3) a wall-to-wall physical inventory might reveal additional missing equipment, and (4) the loss of the IT equipment may have allowed the unauthorized disclosure of sensitive patient and employee information and resulted in possible violations of the Privacy Act.

We substantiated the first allegation that IT Service had not inventoried IT equipment and certified the accuracy of the inventory records in over 2 years. We also substantiated the allegation that the healthcare system did not perform a complete ROS investigation because the Police and Security Service did not investigate the loss of the IT equipment. However, we believe the healthcare system's board of survey (board) findings provided sufficient explanation to justify the removal of the missing equipment from the equipment inventory listings (EILs). An IT Service wall-to-wall inventory and an OIG inventory spot check did not substantiate the allegation that significant amounts of IT equipment were still missing after the completion of the ROS investigation. We could not evaluate the validity of the last allegation that the loss of IT equipment had resulted in

[1] A "Report of Survey" (VA Form 90-1217) is used by authorized staff to document investigations and related findings and recommendations pertaining to the loss, damage, or destruction of Government property.

[2] The IT Service equipment values referenced in the report are based on the equipment's original acquisition costs recorded in the healthcare system's inventory records and do not reflect depreciation or obsolescence. At the time the healthcare system removed the $991,000 of missing equipment from the inventory records, the age of the equipment ranged from 3 to 26 years, and the equipment had a total estimated depreciated value of less than $1,000.

the unauthorized disclosure of sensitive information and possible violations of the Privacy Act due to insufficient records.

We recommended that the Healthcare System Director ensure that:

- The IT Service Chief and staff receive training on the required equipment inventory control procedures, including the EIL evaluation and certification process.

- The IT Service Chief and staff conduct the required physical inventories of IT Service equipment at least annually and certify the accuracy of EILs.

- The Materiel Management (MM) Section staff coordinate IT equipment additions, removals, transfers, and turn-ins with the IT Service staff to ensure that all equipment is accurately recorded on EILs.

- The MM Section notifies the Healthcare System Director in writing when responsible officials do not complete required inventories and EIL certifications.

- The IT Service staff complete and submit turn-in documentation for excess or obsolete equipment as required by VA policy.

- All healthcare system staff are reminded to promptly forward ROS forms to the Police and Security Service.

- The Police and Security Service Chief conducts investigations and completes "Uniform Offense Reports" when the reported losses of equipment may involve theft.

- The healthcare system staff update EIL location information when IT equipment locations change.

Introduction

The healthcare system provides primary, tertiary, long-term, and extended care in the areas of medicine, surgery, behavioral medicine, neurology, oncology, dentistry, geriatrics, and physical medicine and rehabilitation. Outpatient care is provided at the Loma Linda facility and at five community-based outpatient clinics located in Victorville, Sun City, Palm Desert, Corona, and Upland, California. The healthcare system is part of the Desert Pacific Healthcare Network, Veterans Integrated Service Network (VISN) 22, and serves a veteran population of about 300,000 in a primary service area that covers the eastern California counties of San Bernardino and Riverside. The healthcare system is affiliated with the Loma Linda University Medical Center and Loma Linda University Health Care and supports 99 medical resident positions in medicine, psychiatry, and surgery. Approximately 375 medical residents and 265 medical students rotate through the healthcare system each year. The healthcare system also supports training programs in audiology and speech pathology, dentistry, podiatry, nursing, medical records administration, social work, laboratory technology, pharmacy, respiratory therapy, psychology, physical therapy, and occupational therapy.

An anonymous complaint received by the OIG's Hotline Division alleged that:

- IT Service had not inventoried IT equipment and certified the accuracy of inventory records in over 2 years.
- The healthcare system had not performed a complete ROS investigation for about $991,000 of missing equipment and removed the equipment from its inventory records without explanation.
- A wall-to-wall physical inventory might reveal additional missing equipment.[3]
- The loss of the IT equipment may have allowed the unauthorized disclosure of sensitive patient and employee information and resulted in possible violations of the Privacy Act.

To assess the validity of these allegations, we reviewed ROS records and IT Service EIL records from fiscal year (FY) 2000 to January 2004; the results of an August 2003 wall-to-wall IT Service equipment inventory; IT Service records for donated equipment for the period of FY 2000 to January 2004; and applicable laws, policies, and procedures. We interviewed selected healthcare system staff regarding the allegations including the Police and Security Service Chief, the Acting MM Section Chief, the IT Service Chief, and the Information Security Officer. We also conducted an inventory spot check of selected IT Service equipment items to determine if we could identify any additional missing equipment items and tested the reliability of IT Service EIL information. Our evaluation was conducted in accordance with Generally Accepted Government Auditing Standards for staff qualifications, independence, and due professional care; fieldwork standards for planning, supervision, and evidence; and reporting standards for performance audits.

Background

To safeguard Government property, such as IT equipment, VA supply, procurement, and MM policies (VA Handbooks 7125 and 7127) require facilities to implement management controls that maintain accountability for equipment throughout its life. VA facilities assign staff the responsibility of managing and maintaining control over equipment through the use of an EIL. The EIL is a descriptive list which contains each equipment item's acquisition date, physical description, bar code, location, and acquisition cost. EIL information is maintained on the healthcare system's Veterans

[3] Because it is normal for some equipment to be lost during routine VA facility operations, the complainant's main concern appeared to be that any inventories completed after the May 2003 ROS investigation might reveal additional missing equipment.

Health Information Systems and Technology Architecture (VistA) system and responsible staff must ensure that the information is updated as needed to maintain proper control and accountability for assigned equipment.[4]

By signing the EILs, employees acknowledge receipt of equipment and certify on a specific date that all equipment listed on the EILs is present, accounted for, and needed. To ensure the EILs' accuracy and completeness and verify that equipment has not been lost, damaged, or destroyed, healthcare system staff conduct physical inventories to reconcile the EILs with the equipment on hand. The frequency of the required inventories is based on each EIL's last inventory date and the inventory's results. For example, if 95 to 99 percent of an EIL's items are located during the inventory, VA Handbook 7127 requires the next inventory to be completed again in 12 months.

When inventories identify missing equipment, the MM Section staff are required to adjust and update the EILs through the preparation of adjustment vouchers that explain and support the basis for removing the equipment from the inventory records. When equipment is lost or missing, VA Handbook 7125 also requires the completion of a ROS investigation process where:

- Employees report the loss of the equipment to their supervisors.
- The supervisor initiates a preliminary investigation and formally records the results of the investigation on a ROS form.
- The supervisor provides the ROS form to Police and Security Service which initiates its own investigation and documents the investigation in a VA-required "Uniform Offense Report" (VA Form 10-1393).
- The MM Section Chief reviews the ROS form and all records related to the missing equipment to ensure the equipment is actually missing.
- If the ROS involves the loss of VA property valued at $5,000 or more or a VA employee may be assessed financial liability or a disciplinary action as a result of the loss, the facility Director is required to establish a ROS board.
- The board, comprised of impartial and qualified persons, investigates the reported loss to determine what property can be recovered, the value of the property that is unrecoverable, who is responsible for the loss, and if there is financial liability or negligence or violations that require disciplinary action.

[4] VistA is an automated information system, comprised of over 90 separate business packages, that supports the day-to-day activities of VA medical facilities' operations including health data systems; registration, enrollment, and eligibility; provider systems; management and financial systems; and education systems.

- The ROS documentation, including the board's report and a "Uniform Offense Report," will provide satisfactory explanation of the circumstances surrounding the loss of Government property and an assessment of whether disciplinary actions and/or damages should be pursued.

- The facility Director typically reviews and approves the board's ROS report which documents the board's investigation, findings, and recommendations.

After the Director approves the board's ROS report, the MM Section Chief must keep a complete copy of the approved report with the supporting documents and an adjustment voucher showing the removal of the unrecoverable equipment from the EILs in the ROS file and provide a copy of the entire ROS file to Police and Security Service.

Results

Issue 1: Equipment Inventory Control Procedures Were Not Followed

We substantiated the allegation that IT Service had not inventoried equipment and certified the accuracy of its EILs in over 2 years. Although required by VA Handbook 7127, IT Service had not performed the physical inventories of IT equipment at least annually and certified the accuracy of its EILs in almost 10 years. Furthermore, MM Section was aware that IT Service was not following VA equipment inventory control procedures during this period but did not notify the Director as required by VA policy.

From December 1994 to January 2004, IT Service Chiefs did not complete required IT equipment inventories and EIL certifications because they did not want to accept and certify EILs which had significant inaccuracies pre-dating their tenures. During this period, two prior Service Chiefs, four Acting Service Chiefs, and the current Service Chief, appointed in November 2000, were responsible for managing IT Service. Inaccuracies in the EILs were not effectively addressed and worsened over time due to turnover in the IT Service Chief's position, the IT Service Chiefs' and staff's lack of training and inexperience with equipment inventory control procedures, the healthcare system's operational decision to consolidate all of the healthcare system's IT equipment on five IT Service's EILs, and a lack of coordination between IT Service and MM Section in the management of the EILs.

We verified that breakdowns in IT equipment control procedures and related EIL problems developed as early as 1996. In August 1996, the IT Service Chief sent the MM Section Chief a memo stating that 179 items, valued at about $316,000, were missing but a ROS was never initiated and the equipment was never removed from the EILs. In addition, the healthcare system transferred IT equipment inventory from other services to IT Service but did not document when the transfers occurred or reconcile EIL information for the transferred items. Consequently, during the 1990s, IT Service became responsible for about 5,500 IT equipment items located in over 1,000 rooms, various outbuildings, and 8 remote sites, but it had no assurance that its 5 EILs were accurate or that the EILs did not include equipment that was already missing.

IT Service EIL inaccuracies were also exacerbated by a lack of coordination between MM Section and IT Service in the management of the EILs.[5] From January 1997 to August 1998, MM Section staff placed inventory tags on any IT equipment in the facility that was not tagged and added it to IT Service's EILs. However, MM Section staff often did not include adequate equipment descriptions and location information in VistA when the equipment was added, so IT Service staff had a difficult time locating the equipment during subsequent EIL inventories.

By the time the current IT Service Chief was appointed in November 2000, IT Service EIL records included equipment items that had been missing since at least 1996, previously turned-in equipment items, non-operational equipment whose parts had long since been scavenged for use with other equipment, equipment with incomplete EIL descriptions, and equipment with incorrect location information.

From July 2000 to January 2004, MM Section staff sent IT Service delinquency notices and granted IT Service extensions to complete its EIL inventories and certifications. However, the current IT Service Chief acknowledged that he refused to certify the EILs from November 2000 to FY 2004 because the EILs were inaccurate. Instead, he initiated a wall-to-wall inventory of all IT Service equipment items to identify and locate all of the items for which IT Service was responsible. From December 2001 through May 2002, IT Service staff inventoried 5,072 equipment items listed on the EILs, reconciled VistA inventory information with the physical inventory, and identified 419 missing items. Based on the inventory's results, the IT Service Chief submitted 3 ROS forms in May 2003 to the MM Section Chief for the 419 missing items valued at about $991,000. The healthcare system completed a ROS investigation for these missing items in June 2003 and removed them from IT Service's EILs because they were deemed unrecoverable. (See discussion of the ROS in Issue 2.)

During a subsequent inventory conducted in January 2004, the IT Service staff determined that its five EILs were about 97 percent accurate. After this inventory and the related VistA EIL updates were completed, the IT Service Chief certified the IT Service's EILs containing 5,536 equipment items, valued at about $14.5 million, for the first time in about 10 years.

Recommendation 1. We recommended that the Healthcare System Director ensure that: (a) the IT Service Chief and staff receive training on the required equipment inventory control procedures, including the EIL evaluation and certification process; (b) the IT Service Chief and staff conduct the required physical inventories of IT Service equipment at least annually and certify the accuracy of EILs; (c) the MM Section staff coordinate IT equipment additions, removals, transfers, and turn-ins with IT Service staff to ensure that

[5] MM Section ensures EIL inventories are completed, conducts quarterly inventory spot checks of EILs to verify inventory accuracy, provides assistance with EIL equipment description problems, receives and disposes of excess or obsolete equipment turned-in by responsible officials, and adjusts and updates inventory records.

all equipment is accurately recorded on EILs; and (d) the MM Section notifies the Healthcare System Director in writing when responsible officials do not complete required inventories and EIL certifications.

The Healthcare System Director agreed with the finding and recommendations and reported that IT Service staff received training on inventory control procedures, EIL evaluations, and certification processes and now perform a wall-to-wall inventory of all healthcare system areas. Each technician's annual performance plan now includes a performance standard for measuring their ability to maintain accurate inventory records, and MM Section and IT Service staff work jointly to account for all new equipment additions, removals, transfers, and turn-ins. All new equipment received is scanned into VistA for accurate identification. To track equipment throughout its life expectancy, each item is bar coded and VistA system records are updated using bar code scanners when inventory spot checks and annual physical inventories are conducted. Furthermore, services must submit a request for an extension if they require additional time, and the Finance and Logistics Chief may authorize a short extension. However, if services are not timely in their response to the extension, the Healthcare System Director will be notified of the delinquency. We will follow up on planned actions until they are complete.

Issue 2: The Report of Survey Process Was Incomplete But Equipment Inventory Adjustments Were Explained

We substantiated the allegation that the healthcare system's ROS process was incomplete because Police and Security Service did not investigate the loss of the 419 IT equipment items when it became aware of it as required by VA Handbook 7125. However, the ROS board's investigation provided sufficient explanation and justification for the healthcare system's removal of the missing equipment from IT Service's EILs. The board's investigation found that most of the missing equipment was unrecoverable due to poor record keeping, a breakdown in equipment inventory control procedures, and unreported theft possibly going back as far as 1996. Although Police and Security Service should have completed and documented its investigation in a "Uniform Offense Report" as part of the ROS process, we acknowledge that the prolonged breakdown in equipment control procedures and the length of time between when the equipment was lost and when it was reported missing would have limited the effectiveness of an investigation.

After the IT Service Chief reported the 419 missing equipment items, valued at about $991,000, to the MM Section Chief in May 2003, the MM Section Chief provided the ROS information to the Healthcare System Director in May 2003 as required by VA policy. During this period, the IT Service Chief also notified the Police and Security Service Chief of the IT equipment inventory problems but did not provide Police and Security Service with copies of the ROS forms that had been completed. Police and Security Service did not receive the ROS forms until the MM Section Chief provided them in July 2003. In the mean time, the Healthcare System Director convened a board composed of the Pathology and Laboratory Medicine Service Administrative Officer, a VISN 22 Network Business Center MM Manager, the Nutrition and Food Service Administration Chief, and the Imaging Service Chief Technologist to investigate the missing equipment and to make recommendations.

From May to June 2003, the board conducted its investigation. The board interviewed the IT Service Chief, two IT Specialists, an Inventory Management Specialist, the Warehouse Chief, the Media Section Chief, a Patient Education Specialist, and the MM Section Chief regarding the missing equipment. The board also reviewed IT Service EILs, MM Section Turn-In Logs for the EILs, and MM Section ROS Logs. The board did not conduct a physical inventory of IT equipment because MM Section staff were in the process of completing a wall-to-wall inventory at the time the board convened. The board identified conditions which had weakened the healthcare system's IT equipment inventory controls and increased inaccuracies in EIL records:

- The healthcare system consolidated all IT equipment from the EILs of the using services to IT Service's five EILs without ensuring the accuracy of the equipment information before the consolidation occurred.

- The MM Section implemented a practice of adding equipment to IT Service EILs that it identified during its inventories without coordinating the addition of the equipment with IT Service.

- The MM Section did not have operational scanners to effectively track and manage the movement of equipment in the healthcare system even though rooms and equipment were bar coded.

Consequently, the board also found that IT Service EILs were inaccurate and concluded that several items should have been removed from IT Service EILs before the May 2003 ROS was initiated:

- In 1996, the former IT Service Chief reported to the MM Section that 179 IT equipment items, valued at about $316,000, were missing. However, the former IT Service Chief did not initiate an ROS at that time and the items were not removed from IT Service EILs.

- Eighteen items, valued at about $64,000, had been reported missing on the May 2003 ROS forms but, in fact, had been turned-in and were not lost.

- Parts had been scavenged from computer systems but turn-in documents had not been submitted to remove the equipment from the EILs.

- Healthcare system staff had disposed of IT equipment items in preparation for a Joint Commission on Accreditation of Healthcare Organizations visit but did not prepare required turn-in documents and remove the equipment from IT Service EILs.

Based on these findings, the board deleted the 18 items that were not lost from the ROS. For the remaining 401 equipment items, valued at about $927,000, the board deemed the equipment items unrecoverable because it considered it unlikely that any additional items would be found after MM Section staff completed its current on-going equipment inventory and after IT Service staff had already spent about 1,605 hours trying to locate the missing equipment. Consequently, the board concluded that all of the missing equipment items should be removed from inventory records and that none of the healthcare system's staff could be held personally or financially responsible for the lost equipment. The board also made 13 recommendations to improve equipment tracking, IT Service and MM Section equipment inventory control procedures, the management and maintenance of EILs, and the healthcare system's equipment turn-in process. The Healthcare System Director approved the board's ROS report and recommendations in June 2003.

After the board issued its ROS report, the MM Section completed a wall-to-wall IT equipment inventory. The inventory results were consistent with the board's findings. The inventory located an additional 32 items, valued at about $52,000, that IT Service had previously reported missing on the May 2003 ROS forms. Of the 32 items that MM Section staff found, 24 were still in use and 8 had been scavenged for parts. In addition to the 24 items still in use, 13 had incorrect locations listed on the EILs and 1 had an incorrect equipment description.

Through our interviews with the IT Service and MM Section staff and reviews of IT Service and MM Section records, we also confirmed that the breakdown in IT equipment inventory procedures at the healthcare system had led to the conditions described in the board's report. During a series of IT Service and MM Section inventories conducted during the 3-year period of FY 2001 to FY 2003, healthcare system staff encountered equipment items with missing bar codes, problems locating equipment because of erroneous EIL equipment descriptions, and equipment items that should have been removed from the EILs when the items were turned-in or were inoperable and scavenged for parts. We also confirmed that the EILs had not been properly updated to reflect transfers or the removal of excess or obsolete equipment. For example, we determined that IT Service EILs were not updated when equipment items were turned-in during healthcare system-wide computer hardware upgrades. Because the removal of this equipment was never documented using turn-in forms, the IT equipment items were never removed from the EILs and they became part of the 419 items that IT Service reported missing on the May 2003 ROS forms.

In conclusion, the healthcare system did not fully comply with VA's ROS policy even though it developed sufficient information to justify and explain the removal of the missing equipment from IT Service EILs. Although Police and Security Service did not receive the ROS forms from IT Service as required by policy, it was made aware of the situation and given the complete ROS file in July 2003. The Police and Security Service Chief stated an investigation was not conducted and the loss was not reported to the Federal Bureau of Investigations because he did not consider the missing equipment to be a criminal incident warranting an investigation. However, VA policy requires investigations to be conducted to the extent necessary to determine whether a crime has been committed and to collect and preserve basic information and evidence related to the incident. Because the disappearance of some of the equipment reported missing in May 2003 could have involved theft, the Police and Security Service Chief should have, at a minimum, documented on a "Uniform Offense Report" the pertinent facts and information that lead him to conclude that a criminal investigation was either not necessary or not feasible.

Recommendation 2. We recommended that the Healthcare System Director ensure that: (a) IT Service staff complete and submit turn-in documentation for excess or obsolete equipment as required by VA policy, (b) all healthcare system staff are reminded to promptly forward ROS forms to Police and Security Service, and (c) the Police and Security Service Chief conducts investigations and completes "Uniform Offense Reports" when the reported losses of equipment may involve theft.

The Healthcare System Director agreed with the finding and recommendations and reported that IT Service staff now complete and submit turn-in documentation electronically to ensure that paperwork is not lost over time. Documentation of the known theft of equipment is completed within 24 hours of an incident and submitted to the Police and Security Service. In addition, the Police and Security Service now has a criminal investigator position to conduct investigations and prepare "Uniform Offense Reports" when losses of equipment may involve theft**.** We will follow up on planned actions until they are complete.

Issue 3: A Wall-To-Wall Inventory Did Not Reveal Significant Amounts of Additional Missing IT Equipment

We did not substantiate the allegation that there were still significant amounts of missing IT equipment after the May 2003 ROS. In January 2004, IT Service conducted a wall-to-wall inventory of IT equipment after the missing equipment identified in the May 2003 ROS was removed from its EILs. As a result of this inventory, IT Service staff determined that its five EILs were about 97 percent accurate. This equipment inventory accuracy rate fell well within the VA Handbook 7127 standard of 95 to 99 percent for an acceptable annual inventory, and therefore, VA policy did not require IT Service to perform another EIL inventory for another 12 months. The inventory did not identify any additional missing equipment items but did identify labeling and location problems. Also, the inventory actually found 11 items, valued at about $23,000, that had been previously reported as missing on the May 2003 ROS forms.

From April 13–14, 2004, we performed an inventory spot check of IT Service EILs for 100 randomly selected equipment items, valued at about $166,000, to determine if we could identify any additional missing items. Our inventory spot check located all of the randomly selected items but 8 (8 percent) of the 100 items, valued at about $11,000, were not at the locations listed on the EILs. Based on the discrepancies from our judgment sample, as many as 440 IT Service equipment items (5,500 IT Service equipment items x 8 percent) could have incorrect locations listed on the EILs.

As demonstrated by the May to June 2003 ROS process, incorrect EIL information can result in the misclassification of equipment as "lost" and make equipment more vulnerable to misuse and theft. Consequently, IT Service and responsible healthcare system staff needed to ensure the accuracy and completeness of EIL location information for IT equipment even though a wall-to-wall inventory and our inventory spot check did not identify significant amounts of additional missing IT equipment.

Recommendation 3. We recommended that the Healthcare System Director ensure that healthcare system staff update EIL location information when IT equipment locations change.

The Healthcare System Director agreed with the finding and recommendation and reported that all IT Service staff involved in moving equipment were given rights to change the location field in the VistA system and received training in two methods of modifying the location information so that they can choose the most appropriate method. Each technician's annual performance plan now includes a performance standard for measuring their ability to maintain accurate inventory records, and the healthcare system counsels staff about EIL inventory location problems when they are discovered. We will follow up on planned actions until they are complete.

Issue 4: Sufficient Information Was Not Available To Determine If Unauthorized Disclosures of Sensitive Information Had Occurred in Violation of the Privacy Act

We could not assess the validity of the allegation that the loss of about $991,000 of IT equipment had resulted in the unauthorized disclosure of sensitive patient and employee information and possible violations of the Privacy Act of 1974 because of insufficient records. The Privacy Act requires that sensitive information about an individual in the custody of the Federal Government be protected from unauthorized disclosure and provides for both civil and criminal penalties for violation of the act. Subsequently, VA Handbook 6210 requires the removal or permanent erasure of VA data from IT equipment, such as computer hard drives, when equipment is removed from service to prevent the unauthorized disclosure of sensitive information. In addition, VA requires all employees to protect sensitive information and provides employees with training on how to safeguard it from unauthorized disclosure.

Of the 419 IT equipment items reported missing on the May 2003 ROS forms, 238 were items such as modems, computer monitors, multimedia equipment, and printers that did not have any data storage capabilities. The remaining 181 items were computers used in the day-to-day operations of the healthcare system. As a result, these computers may have contained sensitive VA patient or employee. However, we have no means of verifying whether or not these computers contained sensitive data. Similarly, if they contained sensitive information, we had no way to ascertain if healthcare system staff had used passwords or encryption software to reduce the risk of unauthorized disclosure.

Based on our review, IT Service had procedures in place to ensure that the hard drives of excessed and donated computers were erased to prevent the possible unauthorized disclosure of sensitive information. However, we could not verify if the 181 missing computers on the May 2003 ROS had been removed from the facility and if they had been removed, whether the hard drives had been properly erased due to the lack of information and records regarding their final disposition. At the time of our review, the healthcare system had not received any complaints or reports indicating that any unauthorized disclosures of sensitive information or violations of the Privacy Act had occurred due to the loss of these computers.

Conclusion

During a 10-year period, IT Service and MM Section staff did not follow VA-required equipment inventory procedures and did not effectively manage and safeguard the healthcare system’s IT equipment inventory. Consequently, IT EIL inventory controls and records had deteriorated to the point where IT Service staff had to report the loss of 419 items, valued at about $991,000, in May 2003. The healthcare system’s ROS board determined that these items were unrecoverable, and that they should be removed from IT Service EILs. We agreed with the board’s findings but found that the healthcare system had not fully complied with VA’s ROS policy. IT Service did not submit the ROS forms to Police and Security Service to formally report the missing equipment, and even after MM Section provided Police and Security Service the ROS file, it still did not complete the required investigation. Subsequent healthcare system wall-to-wall inventories, as well as our own inventory spot check, did not identify excessive amounts of additional missing equipment after the completion of the ROS process in June 2003. Finally, insufficient records prevented us from evaluating whether the loss of 181 computers resulted in the unauthorized disclosure of sensitive information and Privacy Act violations.

Healthcare System Director Comments

The Healthcare System Director agreed with the findings and recommendations and provided acceptable improvement plans. (See Appendix A, pages 14–16, for the full text of the Healthcare System Director's comments.) We will follow up on planned actions until they are completed.

For the Assistant Inspector General for Auditing

(o*riginal signed by Gerald Grahe, Deputy Assistant General for Auditing for:)*

JANET C. MAH

Director, Los Angeles Audit Operations Division

Appendix A

Healthcare System Director Comments

VA LOMA LINDA
HEALTHCARE SYSTEM

A Division of VA Desert Pacific Healthcare Network

Department of Veterans Affairs **Memorandum**

Date: September 7, 2005

From: Director, VA Loma Linda Healthcare System

Subject: **Evaluation of Allegations Regarding the Mismanagement of Information Technology Equipment and Privacy Act Violations**

To: Director, Los Angeles Operations Division, Office of Inspector General (52LA)

1. The following documents the steps the VA Loma Linda Healthcare system has taken to address recommendations in the OIG report dated August 10, 2005.

2. Recommendation 1. *We recommend that the Healthcare System Director ensure that: (a) the IT Service Chief and staff receive training on the required equipment inventory control procedures, including the EIL evaluation and certification process; (b) the IT Service Chief and staff conduct the required physical inventories of IT Service equipment at least annually and certify the accuracy of EILs; (c) the MM Section staff coordinate IT equipment additions, removals, transfers, and turn-ins with IT Service staff to ensure that all equipment is accurately recorded on EILs; and (d) the MM Section notifies the Healthcare System Director in writing when responsible officials do not complete required inventories and EIL certifications.*

   Concur. The IT Service staff have been trained on inventory control procedures, EIL evaluations and certification processes. Currently IT staff performs a wall-to-wall inventory of all areas affiliated with VA Loma Linda Healthcare System. In addition, keeping current records on moves and equipment locations has been added to all technical staff performance appraisals. With these additions, the Chief is now able to certify the accuracy of EILs in his charge. **Implementation Date: Training began for IT staff in December 2000 and is ongoing. Additional training will be provided to the IT Service Chief and staff by October 24, 2005.**

The Materiel Management and IT staff have worked jointly to account for all new equipment additions, removals, transfers, and turn-ins. All new equipment received is scanned into the AEMS/MERS system for accuracy of identification. The equipment is bar coded and tracked throughout its life expectancy with ongoing updates through spot inventory and annual inventory using bar code scanners to update the AEMS/MERS records. Delinquent notices are sent to services and they are informed if they require additional time they should submit a request for extension. The Chief, Finance and Logistics may authorize a short extension, and if services are not timely in their response to the extension, the Facility Director will be notified of the delinquency. **Implementation Date: June 2003**

3. Recommendation 2. *We recommend that the Healthcare System Director ensure that: (a) the IT Service staff complete and submit turn-in documentation for excess or obsolete equipment as required by VA policy, (b) all healthcare staff are reminded to promptly forward ROS forms to Police and Security Service, and (c) the Police and Security Chief conducts investigations and completes a "Uniform Offense Report" when the reported loss of equipment may involve theft.*

   Concur. The IT Service staff complete and submit turn-in documentation electronically now, to ensure that paperwork is not lost over time. Documentation of known theft of equipment is filed within 24 hours of knowledge of an incident by paper form 2237, as specified by local policy. This paperwork is submitted to Police Service. **Implementation Date: May 2001. Staff is continually trained to submit ROS forms to Police Service.**

   The Police Service now has a criminal investigator position. The investigator will conduct investigations and prepare the Uniform Offense Reports when loss of equipment may involve theft.
   Implementation Date: October 2004

4. Recommendation 3. *We recommend that the Healthcare System Director ensure that healthcare system staff update EIL location information when IT equipment locations change.*

   Concur. Several actions have been put in place to help improve accuracy of EIL location information by IT staff: a) all staff involved in moving equipment have been given rights to change the location field in VistA, the database which generates the EIL reports, b) these staff have had training in two methods of modifying the location information so that they can choose the most appropriate method at the time they are working, c) accurate record keeping for inventory control has been included in each technician's yearly performance appraisal, and d) problems are discussed and staff counseled when discrepancies are found. **Implementation Date: 2001 - April 2005 (rights to technicians to change location started in 2001; performance standards added in 4/2005).**

5. Every effort is being made to not only improve the system of record keeping used for equipment inventory by IT Service, but also to learn from past problems, suggest improvements, and strive to minimize errors and problems caused by the scope of this issue. We are committed to inventory improvement.

Dean Stordahl

Dean R. Stordahl

Appendix B

OIG Contact and Staff Acknowledgments

OIG Contact	Janet Mah (310) 268-4335
Acknowledgments	Julio Arias Andrew Hamilton

Appendix C

Report Distribution

VA Distribution

Deputy Secretary (001)
Chief of Staff (00A)
Executive Secretariat (001B)
Under Secretary for Health (10)
Deputy Under Secretary for Health for Operations and Management (10N)
Management Review Service (10B5)
Director, VISN 22
Director, VA Loma Linda Healthcare System

This report will be available in the near future on the OIG's Web site at http://www.va.gov/oig/52/reports/mainlist.htm. This report will remain on the OIG Web site for at least 2 fiscal years after it is issued.