Office of Inspector General

Controls Over Laptops

March 31, 2008
Inspection Report No. 441

Office of Inspector General

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

To: Corey Booth, Chief Information Officer

Cathy English, Acting Associate Executive Director, Office of Administrative Services

From: H. David Kotz, Inspector General

Date: March 31, 2008

Re: Office of Inspector General – Controls Over Laptops Inspection (No. 441)

Attached is our final inspection report on the Controls Over Laptops. Your comments to the draft report have been incorporated as appropriate.

Management concurred with all 5 of our recommendations. We appreciate the courtesy and cooperation that was extended to our staff during this inspection.

Attachment

cc: Peter Uhlmann
Diego Ruiz
Cristal Perpignan
Mark Degner
Daniel Lisewski
Darlene Pryor

Richard Hillman, GAO

Table of Contents

CONTROLS OVER LAPTOPS

EXECUTIVE SUMMARY

The Office of the Inspector General of the Securities and Exchange Commission conducts regular audits and inspections of Agency operations to promote the effectiveness, integrity and efficiency of the SEC.

We conducted an inspection of the Office of Information Technology's (OIT) control over laptops. Our inspection concluded that OIT does not have the proper accountability over laptops. Although laptops are not considered accountable property, they are sensitive items containing proprietary information, and if lost could result in negatively affecting the SEC's image. The SEC is privy to an enormous amount of non-public and sensitive market data and most of it is stored on laptops. We are aware of OIT's encryption initiative and we commend them for this necessary security control. However, this review looked at controls over laptops (the equipment) and recognizes that encryption can mitigate the risk of data being accessed, but this still does not eliminate the need to have proper accountability over the equipment.

Based on our findings in this inspection, we recommend that laptops be deemed sensitive property within the SEC and are accounted for properly. According to the SEC's property management manual, sensitive property refers to items that have characteristics deemed sensitive because they are potentially pilferable, dangerous, vital to continued operations, or if lost could negatively affect the Agency's image.

We also determined that control over laptops is weak due to the lack of an inventory, or another method of accountability to ensure that the SEC has an accurate account of its laptops. Furthermore, we were unable to trace ownership of laptops to specific individuals. Therefore, if a laptop were lost or stolen, the SEC would have difficulty identifying its rightful owner. As a result of these weaknesses, laptops are susceptible to loss and theft.

Commission management concurred with our five recommendations. Their formal written response is included as Appendix C.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our objective was to assess the adequacy of controls over laptops and compliance with relevant guidelines. To accomplish our inspection objective, we:

- Interviewed members of the Office of Administrative Services' Property Management Office (PMO) and Office of Information Technology's Asset Management Branch (AMB).
- Reviewed policies and procedures for control of laptops, existing laptops and movement from one location to another.
- Reviewed physical inventory documentation.
- Evaluated the use of the SEC-406A Property Transaction Report Form (Form 406A).
- Reviewed data found in hardware/software release reports in order to trace laptops from original purchase to issuance to an SEC employee.
- Analyzed a judgmental sample of hardware/software releases in calendar year 2007.

The scope of the inspection was limited to laptops only. This review did not look at any other IT equipment or the data on the laptops. We did not look at the procedures for acquisition, surplus or physical security of laptops. Consequently, our review and report focus on data that could be obtained from OAS and AMB affecting the overall efficiency and effectiveness of laptop controls and found deficiencies which we believe warrant quick action.

We conducted this inspection from October 2007 to February 2008 in accordance with the *Quality Standards for Inspections,* issued in January 2005, by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency.

BACKGROUND

This inspection was performed because of concerns within the Federal government relating to the protection of sensitive property and information as well as the discovery of internal problems within the SEC regarding the accountability of IT equipment. We also recognize that establishing and maintaining effective accountability controls over laptop computers is essential and necessary to ensure that valuable and proprietary data is not lost or stolen, causing undue damage to the agency and its image.

Responsibilities

PMO is responsible for the overall property management within the SEC. PMO issues property management regulations to cover policies and procedures relative to:

- Requirement determinations.

- Acquisitions.
- Receiving.
- Controls.
- Maintenance.
- Accountability.
- Inventory.
- Utilization.
- Disposal.

The office also provides program oversight concerning organizational performance of property management responsibilities and ensures compliance with SEC Property Management Directives.

AMB is responsible for information technology asset management, inventory tracking (software/hardware), and infrastructure upgrades/deployments. Their duties include planning, coordinating and deploying management for releases of new software and hardware throughout the SEC. AMB also plans, coordinates, and oversees all physical moves of technology equipment and they oversee inventory management and reconciliation for all technology equipment. AMB serves as the inventory control point for the acquisition, storage and issuance of IT equipment. AMB is the utilization coordinator for the reassignment and disposal of IT assets. AMB and PMO interface regarding all IT property issues.

INSPECTION RESULTS

We found several issues with controls over laptops. We concluded that effective accountability of laptop computers simply did not exist. First, the draft property management policy does not identify Commission-wide items such as laptops as sensitive property. Secondly, a Commission-wide inventory of laptop computers has not been performed since 2003. Thirdly, due to the absence of a baseline inventory, we were unable to trace ownership of laptops to a specific individual. As a result of these weaknesses, laptops are extremely susceptible to theft without detection.

We discussed the deficiencies mentioned above with OIT and OAS, and they agreed to take action to resolve these issues.

POLICY

PMO is responsible for establishing the policy governing property management to include laptops.

PMO's current property management regulation and manual, SECR 9-2 and SECM 9-1, dated July 2003, state that the objective is to establish cost effective accounting, tracking, and proper use of government property and its removal, transfer, or other

disposal in an authorized and appropriate manner. This policy although fairly old, clearly outlines how the SEC will account for and control accountable property with an acquisition cost of $5,000 or more, primarily through the use of conducting inventories. The policy contains procedures for conducting inventories on accountable property and moving and transferring furniture and equipment, including IT equipment. It delegates authority for all IT equipment to OIT. Due to the vast difference in costs of IT equipment, the SEC has both inventoried and non-inventoried IT items. Consequently, laptops are accounted for as non-inventory items and are not subject to an annual inventory.

The Commission's current policy delegates control of non-inventoried property with an acquisition cost less than $5,000 to Directors and Office Heads within the agency. The policy states that they are responsible for maintaining reasonable controls over their non-inventoried property to safeguard it against improper use, theft, and undue deterioration. It also states that special inventories over non-inventoried property may be called for if deemed appropriate by PMO.

During this review we reviewed other Federal agencies policies on laptops and found that they identified laptops as sensitive property and conducted annual inventories, despite acquisition costs. The OIG believes that items such as laptops should be identified as sensitive. SEC's current property management policy states that SEC does not have sensitive property. We understand that OAS is currently revising this policy. The draft policy indicates that the SEC may have sensitive property and assigns the responsibility for identifying the sensitive property to Directors and Office Heads.

We reviewed a recent GAO[1] report of the Department of Veterans Affairs that was similar in scope to this inspection and concluded "policies requiring annual inventories of sensitive items, such as IT equipment... have not been enforced." SEC has a similar deficiency; however, we found that policy requiring annual inventories of sensitive items has not been developed primarily because the SEC has not identified any sensitive property.

In order for sensitive property to be identified throughout the SEC and to ensure that the issues with sensitive property are properly addressed, senior management's involvement is imperative. Although PMO and AMB have taken some actions to address issues over sensitive property, such as updating policies and procedures and developing a spreadsheet to track the issuance of laptops; this task requires the commitment and use of IT specialists throughout the SEC.

Therefore, we believe that OAS should change the draft to identify agency-wide sensitive property to include laptops. The policy should also establish a means to account for and track the items through the use of annual inventories. In addition, the policy should also require Directors and Office Heads that manage sensitive items to put internal controls in-place which may include requiring receipt

[1] GAO-07-1100T Entitled " Lack of Accountability and Control Weaknesses over IT Equipment at Selected VA Locations" dated July 24, 2007, Testimony Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives.

signatures, producing separate listings of sensitive items and/or limiting access to sensitive items.

We recognize that sensitive items which do not meet the accountable and capitalized property thresholds will not be included in the Accountable and Capitalized Property System (TRAQs) but they still should be accounted for properly.

Recommendation A

OAS should revise its draft policy to identify Commission-wide sensitive items and allow Directors and Office Heads to determine if they have additional items that should be deemed sensitive.

Recommendation B

OAS should require a method of accountability for sensitive property that will ensure that SEC has an accurate accounting of laptops.

INVENTORY

We found that a complete inventory of laptops has not been performed. In 2005, AMB began a laptop inventory; however, AMB officials said it was not completed due to resource constraints. AMB currently has a branch chief and staff of seven individuals that are responsible for procurement, receiving, tracking, storage, distribution, maintenance and the disposal of IT equipment. In order for them to be able to properly account for IT assets, they must utilize the help of IT specialists throughout the SEC.

Our inspection further found that other Federal agencies track and account for sensitive property such as laptops by conducting annual inventories. We tried to determine the total number of laptops in the SEC and how many of them were assigned to OIT, but could not get a definitive answer. When we asked AMB how they accounted for the laptops within the SEC, we were told they rely on Microsoft Systems Management Server (SMS), reports to give them an accounting. SMS is an automated discovery tool used by SEC to capture information for equipment attached to the network. This tool is effective for providing a snapshot of the equipment logged onto the network and can be used to forecast network use, but we believe it should not be used as an inventory tool because the results are too sporadic. For example, the SEC has employees and contractors that are mobile, who may not log onto the network on any given day. Thus, their equipment would not be captured through SMS until they log on to the network.

OIG believes that a baseline inventory must be performed immediately for sensitive property and AMB should solicit help from IT specialists (assigned to other offices and divisions) within the SEC to conduct the inventory.

Recommendation C

OIT, through AMB should complete a full inventory of laptops to establish a baseline level.

ACCOUNTABILITY

AMB is responsible for the oversight of inventory management and the reconciliation for all technology equipment (i.e., accountable and sensitive property). This branch serves as the inventory control point for the acquisition, storage and issuance of IT equipment.

In this review, we were unable to determine the total number of laptops within the SEC, and therefore, we concluded that sensitive property is not being appropriately controlled. The reason this has occurred is due to the lack of oversight over non-inventoried (sensitive) property. Accountability of sensitive property is crucial because sensitive property and the data that resides on the equipment could negatively affect the SEC's image. For example, an SEC laptop could have sensitive and valuable information pertaining to an ongoing enforcement investigation. If the laptop containing this information were lost or stolen, proprietary and stock-related information could be used improperly.

We are aware of OIT's future plans to encrypt all laptops so that data will not be assessable in the event it is loss. We commend OIT for this needed security control. Although encryption can mitigate the risk that data is illegally accessed, it still does not eliminate the need to have proper accountability over the equipment. AMB has not established and ensured consistent implementation of effective controls for accountability. They are in the process of revising the procedures, however, most of the current procedures primarily address accountable property, and very little is discussed about how to account for sensitive property such as laptops.

In performing this inspection we asked AMB how they accounted for and tracked laptops to users within the SEC. They responded that since laptops were not accountable property, they do not have a policy in-place to account for them other than through SMS. They also stated that they recently developed a hardware/software release report and can provide the Form 406A (supporting property transaction forms) for the equipment identified in the report. However, we found that the report only shows equipment that has been released since January 2007. Prior to the release report, a centralized record for laptops was not in existence for laptops that were assigned to a specific user. Therefore, based on the information received from AMB and our review, we concluded that the SEC does not have appropriate control over its laptops and is unable to trace ownership of laptops to a specific SEC employee. This problem exists for two reasons. First, laptops are not accountable property, and therefore, AMB does not have a policy or procedure to account for them. Secondly, as outlined below, the process for issuing laptops is confusing and the information on the Form 406A is inaccurate or incomplete.

Issues with the Property Transaction Form 406A

The lack of accountability with individual users of IT equipment poses a risk of loss, theft, and misappropriation[2]. AMB's current process relies on the Form 406A as its record of who is accountable for the equipment. From the data AMB provided we could not determine what individual employees were accountable for the equipment because the Form 406A was incomplete and inconsistently applied.

[2] "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."

A judgmental sample pulled from the hardware and software release report of the completed Form 406A on file with AMB revealed that the procedures are inconsistently implemented. We found that there were important details missing from the form such as, the contact information of the person receiving the laptop (printed name, phone and room number), as well as, the details of why the equipment was given to the person (i.e., new employee, loaner) Specifically, we found the following issues:

- Remarks indicated equipment was released to employees who did not have possession of the equipment.
- Laptops were released to individuals that we could not locate or determine if they were employed by SEC.
- Laptops appeared to be released as loaners and did not show that they were returned.
- Laptops were given to other SEC employees whose names did not appear on the form.

The lack of user level accountability and inaccurate records on status, location, and item descriptions make it difficult to determine who is responsible for laptops and the data on the equipment.

Recommendation D

OIT, through AMB should revise the procedures to establish clear accountability for laptops. Among these procedures there should be included a requirement that documents the issuance and receipt of the equipment to a specific SEC employee.

Recommendation E

OAS should specify a form to account for sensitive property. This form needs to include contact information of the person receiving the equipment (i.e., printed name, number, email, and location).

DISCUSSION OF MANAGEMENT COMMENTS

Commission management concurred with all of our five recommendations. Their formal written response is included as Appendix C.

APPENDIX A

Definitions/Criteria from GAO, OMB and SEC's Internal Policy and Procedures

TRAQ. The Official Agency Accountable Property System used to record all transactions for accountable property.

Accountable Property. Identifies items of personal property with an acquisition cost of $5,000 and above and all leased property regardless of dollar value. Accountable property must be tracked on individual property records in TRAQ and is subject to annual wall to wall inventories.

Sensitive Property. Items designated by a Director or Office Head to have characteristics deemed sensitive because they are potentially pilferable, dangerous, vital to continued operations, or if lost could negatively affect the Agency's image.

Microsoft Systems Management Server. An automated discovery tool used on the SEC network. It allows SEC to capture information for equipment attached to the network, and distribute relevant software and updates to SEC workstations. SMS also provides useful reporting functions against any SEC workstation with SMS Client software installed.

Property Management Program SECR 9-2, dated July 2003. Prescribes the policies and procedures used in accounting for personal property purchased, leased, or loaned by the SEC. It applies to all SEC employees. Its overall objective is cost effective accounting, tracking, and proper use of government property and its removal, transfer, or other disposal in an authorized and appropriate manner. This policy states that the SEC has determined it does not have any sensitive items.

Property Management Program Manual SECM 9-1, dated July 2003. Provides guidance and instruction on implementing the SEC's Property Management Program (PMP) and supplements the regulations found at SECR 9-2 and the operating instructions for the PMP automated tracking system. It designates OIT as responsible for assigning IT equipment to Divisions/Offices; for transferring and moving equipment from one Division/Office to another, including regional offices, and documenting the assignments/transfers on Form 406A.

GAO, *Standards for Internal Control in the Federal Government*, dated November 1, 1999. Requires agencies to establish physical controls to safeguard vulnerable assets, such as IT equipment, which might be vulnerable to risk of loss.

OMB Circular No. A-123, dated December 21, 2004. States funds, property, and other assets are safeguarded against waste, loss, unauthorized use or misappropriation.

APPENDIX B

LIST OF RECOMMENDATIONS

Recommendation A

OAS should revise its draft policy to identify Commission-wide sensitive items and allow the Directors/Office Heads to determine if they have additional items that should be deemed sensitive.

Recommendation B

OAS should require a method of accountability for sensitive property that will ensure that SEC has an accurate accounting of laptops.

Recommendation C

OIT, through AMB should complete a full inventory of laptops to establish a baseline level.

Recommendation D

OIT, through AMB should revise the procedures to establish clear accountability for laptops. Among these procedures there should be included a requirement that documents the issuance and receipt of the equipment to a specific SEC employee.

Recommendation E

OAS should specify a form to account for sensitive property. This form needs to include contact information of the person receiving the equipment (i.e. printed name, number, email, and location).

APPENDIX C

MANAGEMENT'S COMMENTS

March 14, 2008

To: Renee Stroud
Manager for Information Technology Audits
SEC, OIG

From: Cathy English
Acting, Associate Executive Director
Office of Administrative Services

Re: Comments to Draft Laptop Controls Inspection Report

Thank you for including us in the Review of the Draft Laptop Controls Inspection Report. Our comments reflect the Office of Administrative Services perspective and responsibilities and focus on overall policy for SEC-wide property and do not address OIT specific concerns or processes.

We agree with your position that laptops should be deemed sensitive items and should be annually inventoried and have internal controls in place. Our overall concern is distinguishing the difference between the accountability processes for sensitive items versus accountable and capitalized items. We agree with Recommendations A & B, but hope the language can be clarified to avoid confusion.

We suggest that Recommendation A be reworded to read the following:

OAS should revise the SEC's draft policy to identify Commission-wide sensitive items and allow the Directors/Office Heads to determine if they have additional items that should de deemed sensitive. The policy should also require that Directors/Office Heads who manage those sensitive items should have in place internal controls, which may include receipt signatures, separate listings and/or limited access. Sensitive items which do not meet the accountable and capitalized property thresholds will not be included in the Accountable and Capitalized Property System (TRAQs).

We suggest that Recommendation B be reworded to read the following:

OAS should revise the SEC draft policy to require Directors/Office Heads to

conduct annual inventories of sensitive items such as laptops.

Finally, we suggest that Recommendation E be revised to help further avoid confusion of the accountable and sensitive property processes by using the form SEC 2040 (8-83) Hand Receipt for Sensitive Items, rather than the form 406A. We suggest that Recommendation E be reworded to read the following:

OAS should revise the form 2040 (6-83) to include contact information of the person receiving the equipment (i.e. printed name, number, e-mail, and location.

Again, thanks for the opportunity to comment.

APPENDIX C

MANAGEMENT'S COMMENTS (cont.)

MEMORANDUM

March 31, 2008

TO: David Katz
Inspector General

FROM: Corey Booth
Chief Information Officer

Re: Comments on laptop controls audit (No. 441)

Thank you for your office's hard work on this inspection, and for the opportunity to review and comment on the findings. As you know, we fully support the agency's efforts to improve its internal controls, and ensuring appropriate accountability over the agency's IT equipment is clearly an important issue.

We concur with the OIG's assessment that we should improve accountability over laptops. This improved accountability starts with the designation of laptops as sensitive property. We agree that this designation is warranted because, although laptops are not otherwise covered under the agency's accountable-property controls because of their dollar value, they are nevertheless valuable and highly portable pieces of equipment that should be managed appropriately to protect the agency's image. Some concerns were also raised during the audit regarding the sensitive nature of the information stored on agency laptops, and the potential risks of compromising the confidentiality of that information. However, OIT is currently encrypting all laptops throughout the SEC; the initiative will be complete by the end of June 2008, which should render this risk negligible going forward. As a result, our primary concern is for the value of the hardware assets.

The report recommends a set of specific measures to improve laptop accountability, including regularly scheduled inventories and improved documentation of laptop issuance. We intend to do so with a combination of automated tools and manual effort. We will also work closely with the Office of Administrative Services to ensure coordination on a policy level, as well as with the various other headquarters and regional offices whose IT specialists distribute, maintain, and transfer laptops and other equipment within those offices.

We look forward to implementing these measures to improve laptop accountability and control. We appreciate the OIG's ongoing support in helping us build a more effective information technology program for the Commission.