U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

# Controls Over the SEC's Inventory of Laptop Computers

September 22, 2014
Report No. 524

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

OFFICE OF
INSPECTOR GENERAL

# MEMORANDUM

September 22, 2014

**TO:** Jeffery Heslop, Chief Operating Officer, Office of the Chief Operating Officer

**FROM:** Carl W. Hoecker, Inspector General, Office of Inspector General

**SUBJECT:** *Controls Over the SEC's Inventory of Laptop Computers*, Report No. 524

Attached is the Office of Inspector General's (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) controls over its inventory of laptop computers. The report contains four recommendations for corrective action that, if fully implemented, should strengthen the SEC's inventory controls over its laptop computers.

On September 4, 2014, we provided you with a draft of our report for review and comment. In your September 16, 2014, response, you concurred with our recommendations. We have included your response as Appendix III in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how your office will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Mary Jo White, Chair
Erica Y. Williams, Deputy Chief of Staff, Office of the Chair
Luis A. Aguilar, Commissioner
Paul Gumagay, Counsel, Office of Commissioner Aguilar
Daniel M. Gallagher, Commissioner
Benjamin Brown, Counsel, Office of Commissioner Gallagher
Michael S. Piwowar, Commissioner
Mark Uyeda, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein

Anne K. Small, General Counsel, Office of the General Counsel
Timothy Henseler, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Thomas A. Bayer, Director, Office of Information Technology
Pamela C. Dyson, Deputy Director, Office of Information Technology
Rhea Kemble Dignam, Regional Director, Office of the Regional Director, Atlanta Regional Office
Roderick Goodwin, Assistant Regional Director, Office of the Assistant Regional Director for Operations, Atlanta Regional Office
Julie K. Lutz, Regional Director, Office of the Regional Director, Denver Regional Office
Christopher Friedman, Assistant Regional Director, Office of the Assistant Director of Regional Operations, Denver Regional Office
Andrew Calamari, Regional Director, Office of the Regional Director, New York Regional Office
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

# Executive Summary

Controls Over the SEC's Inventory of Laptop Computers
Report No. 524
September 22, 2014

## Why We Did This Audit

Laptop computers (laptops) are portable and easy to conceal and often contain sensitive information. Consequently, they are at risk of loss and theft and must be properly safeguarded and accounted for. To support the agency's mission, employees and contractors of the U.S. Securities and Exchange Commission (SEC) use laptops, some of which process and store commercially valuable, market-sensitive, proprietary, and other nonpublic information. However, recent Office of Inspector General (OIG) investigative and review work identified weaknesses in the SEC's laptop inventory records and encryption controls. We initiated this audit to evaluate the effectiveness of the agency's information technology (IT) inventory program and its controls over laptops.

## What We Recommended

OIT is undertaking an agencywide IT inventory, which includes laptops, and plans to replace its IT inventory management system. However, additional actions are needed to improve the agency's controls over laptops. We made four recommendations for corrective action that address policies and procedures for maintaining inventories of laptops; coordination between OIT organizations; notifications about unaccounted-for laptops; and a review of IT inventory management system user accountability. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

## What We Found

To evaluate the SEC's IT inventory program and its controls over laptops, we reviewed a statistical sample of 244 laptops assigned to the SEC's headquarters and 3 of its regional offices. We also reviewed a judgmental sample of an additional 244 laptops assigned to those offices, for a total of 488 laptops reviewed. We determined that the SEC had addressed prior OIG recommendations about laptop accountability and has controls for safeguarding laptops throughout their lifecycles. However, we identified needed improvements.

Specifically, the SEC's IT inventory contained incorrect information for a significant number of laptops. For example, Office of Information Technology (OIT) management decided not to update the inventory to reflect the correct location of 921 laptops that had been located at the Operations Center, which the SEC closed in October 2013. OIT plans to update the location information for these assets when the ongoing agencywide inventory is complete. The inventory also included incorrect location information for 82 (or about 17 percent) of the 488 laptops we reviewed, and incorrect user information for 105 (or about 22 percent) of the 488 laptops we reviewed. In addition, 24 laptops could not be accounted for, and 4 laptops were in the custody of users although the assets were not included in the inventory. Finally, the SEC's procedures for sharing information about lost or stolen laptops were inadequate.

These weaknesses existed because personnel did not always understand their roles and responsibilities, and related policies and procedures were inadequate, had not been effectively communicated, and were not consistently followed. As a result of our testing, we questioned the reliability of the SEC's IT inventory and estimated that it may reflect incorrect information for over 1,000 laptops. Furthermore, we estimated that as many as 202 laptops assigned to the locations we reviewed may be unaccounted for. By not ensuring that inventory records are accurate and that all laptops are accounted for, the SEC is not consistently safeguarding sensitive assets and may be unaware of lost or stolen laptops. In the event that lost, stolen, or otherwise unaccounted-for laptops are not protected by encryption software, which we reported as a finding in our May 2014 *Review of the SEC's Practices for Sanitizing Digital Information System Media* (Report No. 521), the SEC is at risk for the unauthorized release of sensitive, nonpublic information.

We also identified a lack of segregation of duties and compensating controls in the SEC's IT inventory management system. Specifically, at least 88 employees and contractors with access to and custody of laptops also have the ability to delete asset records from the inventory database. This creates opportunities for the misappropriation of laptops without management's knowledge.

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/about/offices/inspector_general.shtml.

# TABLE OF CONTENTS

# ABBREVIATIONS

| | |
|---|---|
| AMB | Asset Management Branch |
| ARO | Atlanta Regional Office |
| CSIRC | Computer Security Incident Response Center |
| DRO | Denver Regional Office |
| GAO | Government Accountability Office |
| IT | information technology |
| ITSM | Information Technology Service Management |
| laptop | laptop computer |

| | |
|---|---|
| NYRO | New York Regional Office |
| OIG | Office of Inspector General |
| OIT | Office of Information Technology |
| OMB | Office of Management and Budget |
| Rev. | Revision |
| RFID | radio frequency identification |
| SEC | U.S. Securities and Exchange Commission |
| SECR | SEC Administrative Regulation |

# Background and Objectives

## Background

Because of their portability, ease of concealment, and the sensitivity of the information they often contain, laptop computers (laptops) are at risk of loss and theft and must be properly safeguarded and accounted for. To support the agency's mission, employees and contractors of the U.S. Securities and Exchange Commission (SEC) use laptops – some of which process and store nonpublic information[1] – in their offices, at alternate work locations, and while on official travel. According to the SEC's Information Technology Service Management (ITSM) system, as of April 1, 2014, the agency's information technology (IT) inventory included a total of 5,525 laptops distributed to users at the SEC's headquarters in Washington, D.C., its Operations Center (which the SEC closed in October 2013),[2] its 11 regional offices,[3] and its 2 data centers. Table 1 describes the purported distribution of these laptops.

**Table 1. Distribution of SEC Laptops by Location**

| SEC Location | Number of Laptops | Percentage of Total |
|---|---|---|
| Headquarters | 2,795 | 50.59% |
| Operations Center | 921 | 16.67% |
| Regional Offices | 1,726 | 31.24% |
| Data Centers | 2 | .04% |
| No Location Identified[4] | 81 | 1.47% |
| *Total* | *5,525* | *100.01%*[a] |

Source: The SEC's ITSM system as of April 1, 2014.
[a] The total percentage does not equal 100 due to rounding.

[1] SEC Administrative Regulation SECR 23-2a*, Safeguarding Non-Public Information*, January 21, 2000, defines nonpublic information as "information generated by or in the possession of the SEC that is commercially valuable, market sensitive, proprietary, related to an enforcement or examination matter, subject to privilege, or otherwise deemed non-public by a division director or office head, and not otherwise available to the public."

[2] In October 2013, the SEC closed the Operations Center located in Alexandria, Virginia, and moved personnel and the assets assigned to those personnel, including laptops, to the agency's headquarters.

[3] The SEC's regional offices are located in Atlanta, Boston, Chicago, Denver, Fort Worth, Los Angeles, Miami, New York, Philadelphia, Salt Lake City, and San Francisco.

[4] The SEC's ITSM system did not include a physical location for these 81 laptops.

In March 2008, the Office of Inspector General (OIG) reported that the SEC did not effectively account for laptops. As stated in Inspection Report No. 441, *Controls Over Laptops*, we found that the SEC's property management guidance did not identify laptops as sensitive property,[5] and the SEC's Office of Information Technology (OIT) had not performed an SEC-wide baseline inventory of laptops since 2003. Because there was no baseline inventory, the OIG was unable to trace custody of laptops to specific individuals. As a result, we made five recommendations to strengthen controls over the SEC's laptop inventory. Management concurred with the recommendations and implemented corrective actions, including designating laptops as sensitive property and developing a methodology for accounting for sensitive property such as laptops.[6] However, in August 2013, the OIG began investigating reports of stolen SEC laptops and identified inaccurate inventory records.

**Federal Guidance.** The Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, establishes guidance for internal control in Federal agencies. According to the Circular, Federal managers are responsible for establishing and maintaining internal control to achieve the objectives of (1) effective and efficient operations, (2) reliable financial reporting, and (3) compliance with applicable laws and regulations. The safeguarding of assets is a subset of these objectives. Specifically, Federal managers should design controls to provide reasonable assurance of preventing or promptly detecting unauthorized acquisition, use, or disposition of assets.[7] Therefore, the SEC's controls over laptops should be designed to provide reasonable assurance that laptops support the agency's mission and are safeguarded throughout their lifecycles.

**SEC Administrative Regulations, Policies, and Procedures.** Various SEC property management and IT administrative regulations, policies, and procedures address controls over the agency's laptops. The documents establish roles and responsibilities for laptop inventory management and describe the agency's asset management information systems. The agency's primary property management directive is SEC Administrative Regulation SECR 09-02, Revision (Rev.) 1, *Property Management Program* (SECR 09-02), which designates laptops as sensitive property. Additional policies and procedures that establish controls over laptops and asset management include, but are not limited to, the following:

[5] According to SEC Administrative Regulation SECR 09-02, Revision 1, *Property Management Program*, September 11, 2012, the SEC defines "sensitive property" as "items designated by [Office of Information Technology] Information Security to have characteristics deemed sensitive from a data perspective and vital to continued operations and, if lost, could negatively affect the agency's image."

[6] U.S. Securities and Exchange Commission, Office of Inspector General, Inspection Report No. 441, *Controls Over Laptops*, March 31, 2008. The report can be accessed at: http://www.sec.gov/oig/reportspubs/ir441.pdf.

[7] OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, December 21, 2004, Attachment pp. 6 and 7.

- SEC ISS-AM-PD-0022, *AMB Receiving Procedure* (Draft), July 12, 2013;
- SEC ISS-AM-PD-0022*, Maintenance, Repair, and Return Material Authorization Procedure* (Draft), July 29, 2013; and
- SEC OIT, Security Operations, *SEC Incident Response Capability Handbook*, April 2014.

Appendix II lists other relevant SEC policies and procedures.

*Roles and Responsibilities.* According to the SEC's regulations, policies, and procedures, several offices within the OIT share responsibility for maintaining accountability for the agency's laptops. These offices include the OIT's Asset Management Branch (AMB), the Computer Security Incident Response Center (CSIRC), and the Service Desk. The AMB is responsible for receiving physical assets including laptops, updating the SEC's inventory records, and ensuring that laptops are managed according to sensitive property requirements.[8] The CSIRC is responsible for responding to information system security incidents such as reports of lost or stolen laptops.[9] And the Service Desk is responsible for collecting requests for additional IT assets including laptops and updating the ITSM system.[10]

SEC directors, office heads, and regional office IT Specialists are also responsible for maintaining accountability for laptops. Specifically, directors and office heads are responsible for maintaining control over property assigned to their respective organizations, including sensitive property such as laptops.[11] Regional office IT Specialists are responsible for the shipment, receipt, and distribution of IT assets (including laptops) returned for maintenance as well as for notifying the AMB of their actions and updating the ITSM system accordingly.[12] SEC employees and contractor staff are responsible for ensuring the proper use, care, and protection of all personal property (including laptops) in their possession, and for reporting immediately to supervisors any personal property that is lost, missing, damaged, or destroyed.[13]

*Asset Management Information Systems Used to Track Laptops.* In addition to assigning roles and responsibilities, SEC policies and procedures describe the following systems used for asset management: the ITSM system, RF Code™, and Computrace®. These systems are used to collect and track data such as a laptop's asset tag number, serial number, manufacturer, location, and assigned employee, and can assist in locating lost or stolen assets. Collectively, each laptop's asset tag number, serial

[8] SEC ISS-AM-PD-0022, p. 2, and SECR 09-02, Section 1-6 N.2, p. 12 and Section 6-2 E, p. 31.

[9] Securities and Exchange Commission, Office of Information Technology, Security Operations, *SEC Incident Response Capability Handbook*, April 2014, p. 1.

[10] SECR 09-02, Section 1-5, p. 6, and Section 2-4 A, p. 16.

[11] SECR 09-02, Section 1-6 F, p. 8, and Section 6-2 E.1, p. 31.

[12] SEC ISS-AM-PD-0022, p. 2.

[13] SECR 09-02, Section 1-6 P, p. 14.

number, and RF Code™ create a unique identifier that is used to track the asset throughout its lifecycle.

The ITSM system is considered the SEC's IT inventory management system[14] and primary mechanism for ensuring accountability for the agency's IT assets, including laptops. The system contains a record of each SEC IT asset with a purchase price greater than $350. The system includes a subcomponent called the Configuration Management Database, which is used to baseline and manage the inventory of all IT assets, including laptops. It also has an IT ticketing component that the OIT's Service Desk uses to request maintenance and repair of IT assets and to track assets when changes in custody occur during the lifecycle of the asset.[15]

The SEC also uses RF Code™ and Computrace® to manage and track IT assets such as laptops. These two systems play key roles in locating lost or stolen laptops. RF Code™ is comprised of radio frequency identification (RFID) transmitters, RFID readers, and a database. Before entering laptops in the SEC's inventory, OIT staff mount an RFID transmitter on each asset. Staff then enter each laptop's unique identifier into the RF Code™ database along with the unique tag number from the assigned RFID transmitter. RFID readers located throughout the SEC's headquarters and regional offices read the active transmissions from the laptops' RFID transmitters, thereby providing real-time location information about the laptops within each SEC facility.

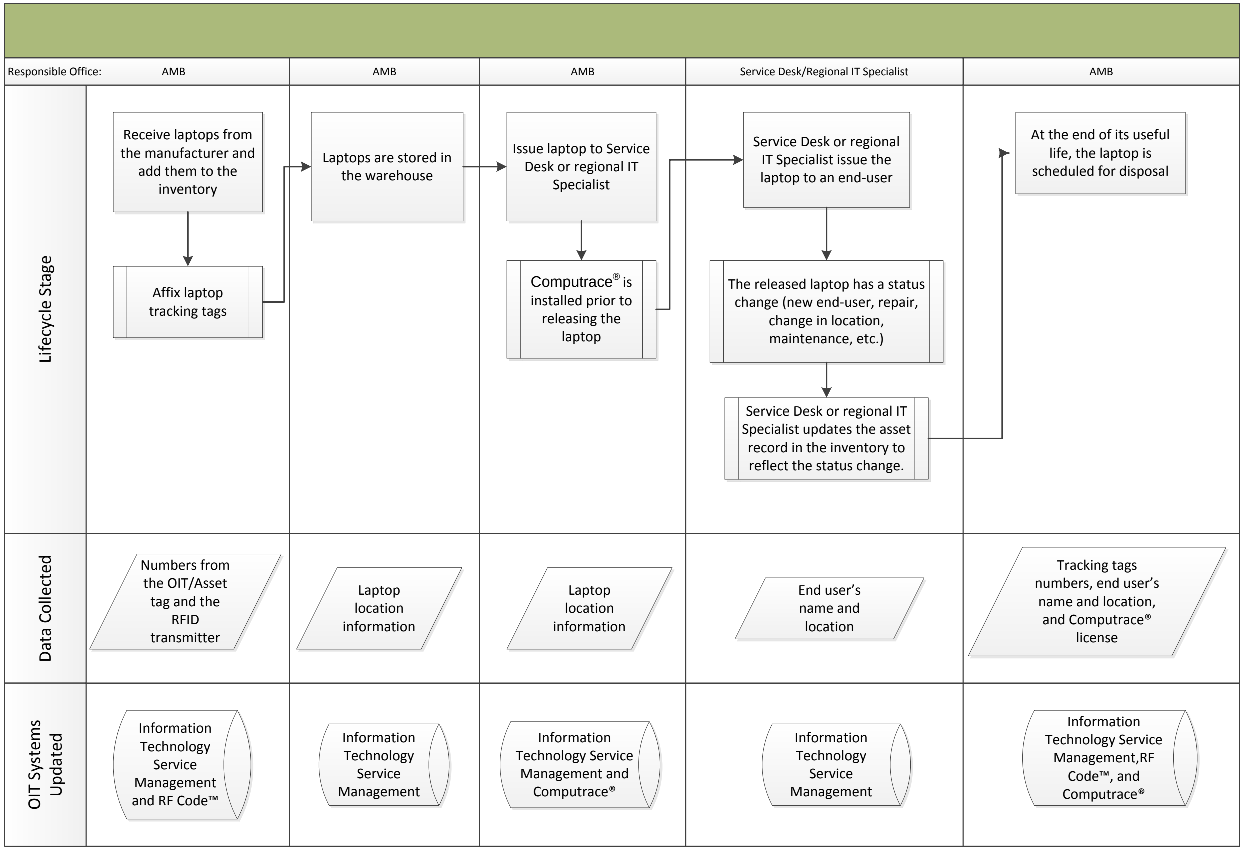
Computrace® is also installed on a laptop before it is issued to an end user. When a user logs into an internet service provider, the Computrace® software will report to the SEC the user's identification and the laptop's location. Computrace® complements RF Code™ by providing real-time position and user information for laptops outside of the SEC's facilities and, therefore, outside the range of the RFID readers. During our testing of the accuracy and completeness of the ITSM system, we were able to locate several laptops with RF Code™ and Computrace® that we could not locate using the ITSM system alone.

**Lifecycle of an SEC Laptop.** SEC laptops pass through several stages from initial receipt from a manufacturer to disposal. The figure below illustrates each stage, the necessary inventory updates that should occur during each stage, the types of information that should be collected, the system(s) that should be updated, and the office responsible for completing the updates.

[14] SECR 09-02, Section 1-5, p. 6.

[15] SECR 09-02, p. 6.

## Figure. Lifecycle of an SEC Laptop


Responsible Office:
AMB
AMB
AMB
Service Desk/Regional IT Specialist
AMB
Lifecycle Stage
Receive laptops from the manufacturer and add them to the inventory
Affix laptop tracking tags
Laptops are stored in the warehouse
Issue laptop to Service Desk or regional IT Specialist
Computrace® is installed prior to releasing the laptop
Service Desk or regional IT Specialist issue the laptop to an end-user
The released laptop has a status change (new end-user, repair, change in location, maintenance, etc.)
Service Desk or regional IT Specialist updates the asset record in the inventory to reflect the status change.
At the end of its useful life, the laptop is scheduled for disposal
Data Collected
Numbers from the OIT/Asset tag and the RFID transmitter
Laptop location information
Laptop location information
End user's name and location
Tracking tags numbers, end user's name and location, and Computrace® license
OIT Systems Updated
Information Technology Service Management and RF Code™
Information Technology Service Management
Information Technology Service Management and Computrace®
Information Technology Service Management
Information Technology Service Management,RF Code™, and Computrace®

Source: OIG generated. Legend: Process □ Sub-process ▥ Data ▱ Database ⬭

## Objectives

Our objective was to evaluate the effectiveness of the SEC's IT inventory program and its controls over laptops. Specifically, we sought to

- determine whether the OIT had established policies, procedures, and supporting documentation to properly identify, track, and safeguard the SEC's laptops throughout their lifecycles;
- evaluate the SEC's procedures for receiving laptops and adding them to the IT inventory;
- evaluate the SEC's procedures for updating the status of laptops in the IT inventory;
- evaluate the SEC's procedures for reporting lost or stolen laptops;
- assess the IT controls over the information systems used to track laptops; and
- evaluate whether the SEC effectively addressed prior recommendations for corrective action from the OIG's Inspection Report No. 441, *Controls Over Laptops*.

To accomplish our objectives, we selected from the SEC's IT inventory a statistical sample of 244 laptops. We also selected a judgmental sample of an additional 244 laptops, for a total of 488 laptops reviewed. We chose to select assets assigned to the SEC's headquarters and 3 of its 11 regional offices: the Atlanta Regional Office (ARO), the Denver Regional Office (DRO), and the New York Regional Office (NYRO). According to the ITSM system, there were a total of 3,601 laptops assigned to these locations, or about 65 percent of the SEC's total population of 5,525 laptops as of April 1, 2014.

Appendices I and II include additional information on our scope and methodology; review of internal controls; sampling methodology; prior coverage; and the applicable Federal laws and guidance and SEC regulations, policies, and procedures.

# Results

## Finding 1: The SEC's Laptop Inventory Controls Need Improvement

To ensure that assets are properly safeguarded, OMB Circular A-123 requires Federal managers to establish controls that provide reasonable assurance of preventing or promptly detecting unauthorized acquisition, use, or disposition of assets.[16] We determined that the SEC had addressed the OIG's prior recommendations about laptop accountability. In addition, the agency has policies, procedures, and IT systems for identifying, tracking, and safeguarding sensitive property, including laptops, throughout their lifecycles. The procedures include controls for receiving laptops, maintaining inventory records, and reporting lost or stolen laptops. Finally, the SEC's primary mechanism for ensuring accountability for its laptops is the ITSM system. However, we identified needed improvements in the SEC's IT inventory program and controls over its laptops. Specifically, we determined the following:

- The SEC's IT inventory contained incorrect information for a significant number of laptops. For example, OIT management decided not to update the inventory to reflect the correct location of 921 laptops that had been located at the Operations Center, which the SEC closed in October 2013. OIT plans to update the location information for these assets when the ongoing agencywide inventory is complete. The inventory also did not specify a location for another 81 laptops. Finally, the inventory included incorrect location information for 82 (or about 17 percent) of the 488 laptops we reviewed and incorrect user information for 105 (or about 22 percent) of the 488 laptops we reviewed.

- Twenty-four laptops included in the inventory and selected for review could not be accounted for.[17]

- The SEC's procedures for sharing information about lost or stolen laptops were inadequate.

These weaknesses existed because personnel did not always understand their roles and responsibilities; and related policies and procedures were inadequate, had not been effectively communicated to regional office personnel, and were not consistently followed. As a result of our testing, we questioned the reliability of the SEC's IT inventory and estimated that it may reflect incorrect location and/or user information for over 1,000 laptops, or nearly one-third of the 3,601 assets assigned to the locations we reviewed. Furthermore, we estimated that as many as 202 laptops assigned to the

[16] OMB Circular A-123, p. 7.

[17] We considered a laptop "accounted for" if: (1) we physically observed the laptop; (2) the person in possession of the laptop provided correct identifying information by email; or (3) an SF-120, Report of Excess Personal Property, was provided for the laptop.

locations we reviewed may be unaccounted for. By not ensuring that inventory records are accurate and that all laptops are accounted for, the SEC may be unaware of lost or stolen laptops. In the event that lost, stolen, or otherwise unaccounted-for laptops are not protected by encryption software, which we reported as a finding in our May 2014 *Review of the SEC's Practices for Sanitizing Digital Information System Media* (Report No. 521), the SEC is at risk for the unauthorized release of sensitive, nonpublic information.

**The SEC's IT Inventory Contained Incorrect Information.** According to SEC policy, AMB and IT Service Desk personnel update the SEC's IT inventory,[18] and ensure that laptops are managed according to sensitive property requirements. Regional office IT Specialists are also responsible for keeping the AMB informed and updating the ITSM system. We determined that AMB staff received laptops and added them to the inventory.[19] However, we reviewed the SEC's inventory records and selected a statistical sample of 244 laptops and a judgmental sample of an additional 244 laptops (for a total of 488 laptops reviewed)[20] and determined that SEC personnel had not ensured that the inventory contained accurate information.

For example, 921 laptops in the inventory were reported as assigned to the SEC's Operations Centers, which the SEC closed in October 2013. When asked why assets were still assigned to the Operations Center although they had been moved to the SEC's headquarters or other facilities, AMB personnel stated that OIT management decided not to update the assets' location in the ITSM system until personnel complete the agencywide inventory initiated in April 2014. The inventory is expected to be complete by the end of 2014. We also noted that the inventory did not specify a location for another 81 laptops.

In addition, we determined that the inventory included incorrect location information for 82 (or about 17 percent) of the 488 laptops included in our sample. Of the 82 laptops we reviewed with incorrect location information, 34 were identified through statistical sampling methods, as shown in Table 2, and the remaining 48 were identified through judgmental sampling, as shown in Table 3. In some instances, the discrepancies were

[18] SECR 09-02 4-8 OIT Inventory Procedures states, "The AMB Branch Chief shall prescribe the frequency and types of inventories to be performed." AMB staff told us that IT Service Desk personnel update inventory records, including the records for laptops, when the status of each asset changes (i.e., when the asset is released to a user, disposed of, etc.). In addition, the AMB performs biennially inventories and updates the ITSM system as necessary at that time.

[19] To assess the AMB's controls over receiving laptops and adding them to the ITSM inventory, we selected a judgmental sample of 30 laptops received as recorded in the AMB's receiving log and compared supporting information to the ITSM inventory and found no exceptions. We also noted that receiving operations are witnessed by security personnel.

[20] We selected the statistical sample from the SEC's inventory records and visited the SEC's headquarters, the ARO, the DRO, and the NYRO to verify each asset's existence and the accuracy of the recorded information (referred to as existence testing). While performing existence testing, we judgmentally selected laptops found at each location and traced them back to the inventory records to determine whether the records were accurate and complete (referred to as completeness testing). Appendix I further describes our sampling methodology.

a matter of wrong room numbers in the same building. In others, the assets were found in different SEC facilities. For example, according to the inventory, one laptop should have been located at the SEC's headquarters but was found in the Chicago Regional Office. Another laptop that should have been located at the NYRO was found at the SEC's headquarters.

We also determined that end user information included in the inventory was incorrect for a total of 105 of the 488 laptops included in our sample (or about 22 percent). As shown in Tables 2 and 3, respectively, 50 of the laptops with incorrect end user information were identified through statistical sampling methods and another 55 were identified through judgmental sampling. For example, in one instance the inventory showed that a laptop was "Released to customer" although it had been slated for disposal.

In some cases, both location and user information were incorrect.[21] For example, the inventory showed that one laptop was assigned to a user at the NYRO. However, using the SEC's employee directory and Computrace®, we determined that both the user and the laptop were at the Miami Regional Office, and the laptop had been assigned to another user.

Finally, in at least one case, the basic asset information included in the SEC's inventory was incorrect. The laptop was assigned to a user at the SEC's headquarters but was incorrectly identified in the ITSM system as a monitor.

Because of the inaccuracy of the agency's IT inventory records, time-consuming and extraordinary efforts were required to locate or account for some laptops in our review. Staff had to examine local inventory records, search through boxes and storage areas containing laptops scheduled for disposal, and request tracking using RF Code™ and Computrace®. In addition, when we projected the results of our statistical sample to the total population of the sample, as shown in Table 2, we estimated that the SEC's IT inventory may reflect incorrect location and/or user information for over 1,000 laptops, or nearly one-third of the 3,601 assets assigned to the locations we reviewed. Although we cannot project the results of our judgmental sample, shown in Table 3, we believe the testing results support the conclusion that the SEC's IT inventory records contained inaccurate information.

[21] We determined that the inventory records included both incorrect location information and incorrect user information for 6 of the sampled laptops from the SEC's headquarters, 15 of the sampled laptops from the ARO, 2 of the sampled laptops for the DRO, and 8 of the sampled laptops for the NYRO.

**Table 2. Statistical Sampling: Summary of Existence Testing Results and Projections of Incorrect IT Inventory Information by Location**

| SEC Location | Number of Sampled Laptops with Incorrect Information | | Statistical Sample Size | Percentage Incorrect | Population Size | Projection to Population[22] |
|---|---|---|---|---|---|---|
| Headquarters | *Incorrect Location* | 13 | 74 | 17.56% | 2,795 | 491 |
| | *Incorrect End User* | 12 | | 16.21% | | 453 |
| ARO | *Incorrect Location* | 12 | 56 | 21.42% | 120 | 26 |
| | *Incorrect End User* | 21 | | 37.50% | | 45 |
| DRO | *Incorrect Location* | 8 | 52 | 15.38% | 118 | 18 |
| | *Incorrect End User* | 4 | | 7.69% | | 9 |
| NYRO | *Incorrect Location* | 1 | 62 | 1.61% | 568 | 9 |
| | *Incorrect End User* | 13 | | 20.97% | | 119 |
| *Total* | *Total with Incorrect Location Information* | *34* | *244* | | *3,601* | *544* |
| | *Total with Incorrect End User Information* | *50* | | | | *626* |

Source: OIG generated.

[22] We are 90 percent confident that the number of laptops with incorrect location information at the locations reviewed is as follows:

- between 455 (lower limit) and 527 (upper limit) for the SEC's headquarters;
- between 24 (lower limit) and 28 (upper limit) for the ARO;
- between 17 (lower limit) and 19 (upper limit) for the DRO; and
- between 8 (lower limit) and 10 (upper limit) for the NYRO.

We are 90 percent confident that the number of laptops with incorrect end user information at the locations reviewed is as follows:

- between 421 (lower limit) and 485 (upper limit) for the SEC's headquarters;
- between 40 (lower limit) and 50 (upper limit) for the ARO;
- between 8 (lower limit) and 10 (upper limit) for the DRO; and
- between 109 (lower limit) and 129 (upper limit) for the NYRO.

**Table 3. Judgmental Sampling: Summary of Completeness Testing Results and Incorrect IT Inventory Information by Location**

| SEC Location | Number of Sampled Laptops with Incorrect Information | | Judgmental Sample Size | Percentage Incorrect |
|---|---|---|---|---|
| Headquarters | *Incorrect Location* | 17 | 74 | 22.97% |
| | *Incorrect End User* | 6 | | 8.11% |
| ARO | *Incorrect Location* | 21 | 56 | 37.50% |
| | *Incorrect End User* | 23 | | 41.07% |
| DRO | *Incorrect Location* | 1 | 52 | 1.92% |
| | *Incorrect End User* | 4 | | 7.69% |
| NYRO | *Incorrect Location* | 9 | 62 | 14.52% |
| | *Incorrect End User* | 22 | | 35.48% |
| *Total* | *Total with Incorrect Location* | *48* | *244* | |
| | *Total with Incorrect End User* | *55* | | |

Source: OIG generated.

**Some Laptops Could Not Be Accounted For.** Although most of the 244 laptops from our statistical sample and existence testing procedures were found, 24 could not be located, including 11 from the ARO and 8 from the DRO. The 19 assets from the ARO and DRO were reported to have been returned to the SEC's headquarters for disposal; however, OIT personnel in headquarters could not find the laptops or provide an SF-120, Report of Excess Personal Property, showing that the laptops had been disposed of. When asked about these 24 laptops, OIT officials stated that they are conducting a biennial IT inventory throughout the SEC regional offices and headquarters. The inventory is expected to be completed by the end of 2014. OIT personnel stated that this ongoing agencywide inventory will enable them to locate assets that are not on-line and cannot be discovered electronically.

Based on the results of our testing, we estimated that as many as 202 laptops assigned to the locations we reviewed may be unaccounted for. Table 4 summarizes and projects the unaccounted-for laptops in our statistical sample by location.

**Table 4. Statistical Sampling: Summary and Projections of Unaccounted-for Laptops by Location**

| SEC Location | Number of Sampled Laptops Unaccounted for | Statistical Sample Size | Percentage Unaccounted for | Population Size | Projection to Population[23] |
|---|---|---|---|---|---|
| Headquarters | 4 | 74 | 5.41% | 2,795 | 151 |
| ARO | 11 | 56 | 19.64% | 120 | 24 |
| DRO | 8 | 52 | 15.38% | 118 | 18 |
| NYRO | 1 | 62 | 1.61% | 568 | 9 |
| *Total* | *24* | *244* | | *3,601* | *202* |

Source: OIG generated.

In addition to identifying 24 laptops that were unaccounted for during our existence testing, we also found during our completeness testing 4 laptops (1 at each SEC facility reviewed) in the custody of end users, although the assets were not recorded in the ITSM system.

**Procedures for Sharing Information About Lost or Stolen Laptops Were Inadequate.** We interviewed CSIRC staff and determined that, when a laptop is lost or stolen, the SEC's procedures require end users to complete a Lost/Theft form and report the loss or theft to either the OIT or the designated IT Specialist. CSIRC personnel then notify SEC senior management and the Department of Homeland Security of a possible release of personally identifiable information, if appropriate.[24] Subsequently, as part of their incident tracking and reporting process, CSIRC personnel maintain information in their own incident management system, called ARCHER, and notify AMB personnel of the lost or stolen device. However, CSIRC staff stated that they do not have access to the RF Code™ or Computrace® systems for tracking, locating, and recovering laptops, which may hinder their ability to respond to reports of lost or stolen laptops. In addition, they are not responsible for updating ITSM.

[23] We are 90 percent confident the number of unaccounted-for laptops at the locations reviewed is as follows:

- between 144 (lower limit) and 158 (upper limit) for the SEC's headquarters;
- between 22 (lower limit) and 26 (upper limit) for the ARO;
- between 17 (lower limit) and 19 (upper limit) for the DRO; and
- between 8 (lower limit) and 10 (upper limit) for the NYRO.

[24] According to the Department of Homeland Security, when an individual gains logical or physical access, without permission, to a Federal agency network, system, application, data, or other resource (i.e., a laptop) the Department must be notified within 1 hour of discovery or detection. Agencies notify the Department of Homeland Security through the United States Computer Emergency Readiness Team's web-based system.

To verify internal reporting to the AMB, we requested a list of lost or stolen items reported to the CSIRC between October 1, 2011, and March 31, 2014. Eighteen of the reported incidents involved laptops. AMB staff confirmed that they were notified of the 18 incidents; however, they could not determine whether 14 of the 18 laptops had been recovered because CSIRC personnel did not provide an updated status of the laptops. Additionally, AMB staff stated that they can flag an asset in the ITSM system as lost or stolen, but they do not know if a regional office user has been issued a new laptop. We concluded that CSIRC and AMB personnel do not always share information or periodically reconcile their separate inventories to ensure that (1) all responsible parties know the status of laptops that are reported as lost or stolen, and (2) the IT inventory is as accurate as possible.

### Lack of Clear Roles and Responsibilities, Adequate Policies and Procedures, and Effective Communication of the Agency's Approach to IT Inventory Management

The weaknesses that we observed existed, in part, because the OIT's policies and procedures did not clearly define roles and responsibilities to ensure that the laptop inventory (or the IT inventory in general) is consistently updated with current and correct information. Further, OIT policies and procedures had not been effectively communicated to the responsible parties, including staff located in the regional offices, and are not consistently followed throughout each asset's lifecycle.

While the SEC's policies and procedures identify roles and responsibilities for laptop inventory management, our fieldwork found inconsistencies with SEC Administrative Regulation, SECR 09-02. This regulation states that accountability for laptops is delegated to directors and office heads with the AMB providing general oversight. However, we found that accountability for laptops is centralized within the AMB, with the Service Desk and IT Specialists supporting the AMB's accountability efforts. Additionally, although the AMB has developed 11 different operating procedures about accountability for IT assets (including laptops),[25] only 6 of the 11 procedures contain guidance on roles and responsibilities for updating the ITSM system, and we determined that such guidance was often unclear. For example, the *Maintenance, Repair, and Return Material Authorization Procedure* does not specifically describe the objective of the AMB or state the fields within the ITSM system that should be updated.

To gain a complete understanding of the SEC's roles and responsibilities for updating the agency's IT inventory, we interviewed personnel from the AMB, the Service Desk, the CSIRC, directors and office heads, and the IT Specialists located at the SEC's headquarters and regional offices. These discussions were necessary because the agency's written operating procedures did not sufficiently establish the roles and responsibilities in practice across the agency.

In addition, during our visits to the ARO, DRO, and NYRO, we inquired about the policies and procedures that the regional office IT Specialists use to account for assets

[25] See Appendix II. Federal Laws and Guidance and SEC Administrative Regulations, Policies, and Procedures.

and to maintain control over their office's laptop inventory. None of the five IT Specialists in the three regional offices that we visited were aware of the agency's written requirements for IT asset management or inventory control, including SECR 09-02. Although we were informed by OIT staff at the SEC's headquarters that regional IT Specialists are responsible to know and adhere to these policies and procedures, the Specialists informed us that they follow their own procedures for tracking laptops throughout their lifecycles. Finally, although regional IT Specialists manage their office's IT asset inventories, they are primarily concerned with minimizing down-time for local users. Two of the regional IT Specialists that we interviewed said they never updated the ITSM system. The remaining three regional IT Specialists that we interviewed informed us that they updated the system only when an asset's status change was permanent (i.e., when an individual was issued a new laptop). We also found that regional IT Specialists performed local inventories and maintained their own sets of records that reflected changes in laptops' locations and end users. However, they did not report such changes to AMB staff or ensure that the ITSM system was updated.

## Conclusion

Although the SEC addressed the OIG's prior recommendations about laptop accountability and has policies and procedures for safeguarding laptops throughout their lifecycles, we identified needed improvements in both its IT inventory program and its controls over laptops. Inaccurate inventory records required personnel to engage in time-consuming and extraordinary efforts to locate or account for the SEC's assets. Staff had to examine local inventory records, search through boxes and storage areas containing laptops scheduled for disposal, and request tracking using RF Code™ and Computrace®. While most laptops we reviewed were found, not all were accounted for. In addition, we found that the ITSM system did not reflect the correct status of several laptops, and several laptops were not included in the ITSM system or were incorrectly identified in the system. As a result of our testing, we questioned the reliability of the SEC's IT inventory and estimated that the inventory reflected incorrect location and/or user information for over 1,000 laptops, or nearly one-third of the 3,601 assets assigned to the locations we reviewed. Furthermore, we estimated that as many as 202 laptops assigned to the locations we reviewed may be unaccounted for. The IT inventory was also unreliable because of inadequate follow-through and sharing of information about lost or stolen laptops. Specifically, AMB staff were unable to provide the current status of certain laptops because of a lack of information from CSIRC personnel.

By not ensuring that inventory records are accurate and that all laptops are accounted-for, the SEC is not consistently safeguarding sensitive assets and may be unaware of laptops that have been lost or stolen. In addition to losing the asset itself, lost, stolen, or otherwise unaccounted-for laptops that are not protected by encryption software create a risk for unauthorized release of sensitive, nonpublic information. As we reported in our May 2014 *Review of the SEC's Practices for Sanitizing Digital*

*Information System Media* (Report No. 521),[26] laptop hard drives that were in use between 2010 and 2013 – after the agency began requiring full disk encryption[27] – were not encrypted and, in some cases, contained large amounts of nonpublic information, including personally identifiable information. Consequently, some of the laptops that are currently unaccounted for may have unencrypted hard drives. If they have been lost or stolen, the SEC's nonpublic information could be compromised.

The OIT is undertaking an agencywide IT inventory, which includes laptops, and expects to complete the inventory by the end of 2014. While this is a good first step, additional actions are needed to address the control weaknesses we observed and to ensure that the SEC maintains an accurate laptop inventory in the future.

## Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's controls over laptops, the Office of Information Technology should implement the following recommendations:

**Recommendation 1:** Revise and communicate to all responsible parties, including regional office personnel, comprehensive procedures for maintaining inventories of laptop computers, to include (a) clearly defined roles and responsibilities, (b) management's expectations for maintaining an accurate inventory, and (c) guidance on when inventory updates are required.

**Management's Response.** The Office of Information Technology concurred with the recommendation and will review, revise as appropriate, and disseminate enhanced policy and comprehensive procedures on property accountability and reporting, with specific emphasis on controls associated with laptop computers. Further, the Office will train responsible parties, including regional office personnel, on property management recordkeeping requirements, timeframes, and procedures. In addition, OIT will communicate expectations to all stakeholders regarding maintaining accurate inventory records, and will conduct "spot check" reconciliations of property records to laptop assets to assess compliance. Management's complete response is reprinted in Appendix III.

**OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

[26] U.S. Securities and Exchange Commission, Office of Inspector General, Report No. 521, *Review of the SEC's Practices for Sanitizing Digital Information System Media*, May 30, 2014. The report's executive summary can be accessed at: http://www.sec.gov/oig/reportspubs/521.pdf.

[27] According to SEC OIT Implementing Instruction II 24-04.04.05 (01.1), *Information Encryption within the SEC,* April 6, 2010, the SEC requires full disk encryption on all laptop computers before they are issued to end users.

**Recommendation 2:** Ensure that personnel in the Computer Security Incident Response Center have the ability to search for and track unaccounted-for laptops using available resources such as RF Code™ and Computrace® and that they provide to the Office of Information Technology Asset Management Branch personnel periodic status updates on laptops that have been reported lost or stolen so that the inventory can be updated as necessary.

**Management's Response.** The Office of Information Technology concurred with the recommendation and will address the theme of the recommendation as a component of the corrective actions to address Recommendation 1. The Office recognizes the need for more systematic information-sharing among appropriate parties (such as the Computer Security Incident Response Center, Office of Information Technology Asset Management Branch, Office of Support Operations' Office of Security Services, and OIG Office of Investigations) in the case of potentially lost or stolen laptops. Management's complete response is reprinted in Appendix III.

**OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

**Recommendation 3:** Complete its ongoing agencywide inventory. Based on the result of the agencywide inventory, promptly update its inventory system to ensure that all assets are included in the system accurately, and report to the Office of Information Technology's Computer Security Incident Response Center unaccounted-for laptops.

**Management's Response.** The Office of Information Technology concurred with the recommendation and, upon completion of the "wall-to-wall" inventory in October 2014, will update the inventory system as appropriate. Management's complete response is reprinted in Appendix III.

**OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

# Finding 2: Lack of Segregation of Duties and Compensating Controls in the ITSM System

To help prevent misappropriation of Federal assets, OMB Circular A-123 requires Federal managers to establish effective controls, such as segregation of duties.[28] Contrary to this principle, at least 88 AMB employees and contractors that have access to and custody of laptops also have the ability to delete asset records from the ITSM inventory database.

During our audit, we requested a list of user accounts and permissions for RF Code™, Computrace®, and the ITSM system. We determined that RF Code™ has one user and Computrace® had two users with permissions to add or delete assets from the systems. Furthermore, both systems included audit trails that record the activities of each user. However, we found that at least 88 AMB employees and contractors have the ability to delete records from the ITSM system and have physical access to laptops. Additionally, the ITSM system does not have an audit trail that tracks when an employee adds or deletes an asset from the inventory database or otherwise modifies its status.

According to AMB staff, the ITSM system automatically assigns delete rights to all users designated as system administrators and members of the AMB. AMB officials stated that updating the system to reduce the number of users who can delete inventory records would not be practical since the OIT plans to replace the system in fiscal year 2015.

## Conclusion

The lack of segregation of duties and compensating controls in the ITSM system creates opportunities for laptops to be misappropriated. For example, OIT personnel who have permissions to delete assets from the ITSM system also have access to areas where laptops are stored. These individuals could simply take a laptop and delete it from the inventory, without the knowledge of OIT management.

## Recommendation, Management's Response, and Evaluation of Management's Response

To improve controls over the SEC's information technology inventory, the Office of Information Technology should implement the following recommendation:

**Recommendation 4.** Ensure that the system selected to replace the SEC's Information Technology Service Management system includes segregation of duty controls, minimizes the number of user accounts that have permission to delete assets from the inventory, and includes an audit trail.

[28] OMB Circular A-123, p. 8.

**Management's Response.** The Office of Information Technology concurred with the recommendation and is working with the Office of Acquisitions to procure an equipment management tool. OIT expects to begin implementing the new system early in fiscal year 2015. As the new tool is implemented, the Office of Information Technology will ensure that it is configured to appropriately segregate duties, limit ability to delete asset records to the minimal number of personnel required to maintain accurate inventory records, and maintain an electronic audit trail of all changes to property records. Management's complete response is reprinted in Appendix III.

**OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

# Appendix I. Scope and Methodology

We conducted this performance audit from April through September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**Scope.** The audit covered the period of October 1, 2011, to April 1, 2014, and consisted of reviewing the SEC's laptop inventory, including samples of laptops assigned to the SEC's headquarters, the ARO, the DRO, and the NYRO. The scope also included an assessment of the SEC's processes and selected supporting documentation. Specifically, the audit included a review of

- Federal guidance and agency policies and procedures for laptop computer inventorying and accountability;
- relevant internal controls;
- the SEC's laptop inventory processes and organizational roles and responsibilities;
- the accuracy and completeness of the agency's laptop inventory; and
- procedures for reporting and accounting for lost or stolen laptops.

**Methodology.** To determine whether the OIT had established policies, procedures, and supporting documentation to properly identify, track, and safeguard the SEC's laptops throughout their lifecycles, we obtained and reviewed relevant asset management and information security laws, regulations, policies, and procedures. In addition, we conducted interviews with responsible officials at each location we reviewed to gain an understanding of the OIT's processes for maintaining control of laptop computers.

To evaluate the SEC's procedures for receiving laptops and adding them to the IT inventory, we interviewed OIT personnel who were responsible for overseeing laptops. We also toured the SEC headquarters' mailroom and loading dock areas where all SEC laptops are received. Finally, we selected a judgmental sample of 30 laptops received as recorded in the AMB's receiving log and compared supporting information to the ITSM inventory.

To evaluate the SEC's procedures for updating the status of laptops in the IT inventory and to assess the IT controls over information systems used to track laptops, we performed existence and completeness testing[29] of the laptops distributed to the SEC's headquarters, the ARO, the DRO, and NYRO. We developed and tested statistical and judgmental samples using data from the ITSM system and our observations during fieldwork performed at the locations included in the audit. We also selected a judgmental sample of 11 laptops and reviewed the historical activity in ITSM associated with each laptop.

To further meet our audit objectives, we evaluated the SEC's procedures for reporting lost or stolen laptops. We interviewed OIT staff responsible for tracking laptops reported as lost or stolen and determined the disposition of assets reported missing during the scope of the audit.

To determine whether the SEC effectively addressed prior recommendations for corrective action from the OIG's Inspection Report No. 441, *Controls Over Laptops* (March 31, 2008), we reviewed recommendation closeout memoranda and discussed the recommendations with OIT staff. We concluded that the OIG concurred with the actions taken and closed all recommendations during fiscal year 2009.

**Internal Controls.** We obtained an understanding of the OIT's internal controls over laptops and assessed the internal controls in accordance with the "[Committee of Sponsoring Organizations] Model of Internal Control." For our review of internal controls, we considered the following:

- *Control Environment* – We evaluated the SEC's control environment related to laptops and determined that personnel at the ARO, the DRO, and NYRO did not receive the agency's asset management and ITSM system training beyond the introductory sessions.

- *Risk Assessment* – We determined that a risk assessment of laptop inventory processes had not been conducted at the regional offices we visited. In addition, we observed that the regional office IT Specialists were primarily concerned with minimizing down-time for local users and not necessarily inventory management.

- *Monitoring* – We assessed the SEC's relevant monitoring activities and determined that regional office IT Specialists periodically validated their own laptop inventory. However, the regional office IT Specialists provided their inventory listings to headquarters personnel only if requested.

- *Control Activities* – We reviewed the SEC's control activities related to laptops and found that regional laptops were properly secured. Unissued laptops were either stored in locked closets or IT work rooms with card reader access.

[29] "Existence testing" verified that a laptop included in the ITSM system actually existed and was in the possession of the person and at the location identified in the ITSM system. "Completeness testing" verified that a laptop found in the possession of a person at a particular location was correctly recorded in the ITSM system.

- *Information and Communication* – We evaluated the SEC's information and communication activities regarding controls over laptops and determined that regional office IT staff were unfamiliar with OIT guidance concerning asset management. Rather, they followed their own policies, which included creating and maintaining local inventories instead of using the agency's ITSM system.

Overall, we determined that the OIT's IT inventory program and controls over its laptops need improving, as discussed in this report.

**Computer-processed Data.** The Government Accountability Office's (GAO) *Assessing the Reliability of Computer-Processed Data* (GAO-09-680G, July 2009) states that "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing." Furthermore, GAO-09-680G provides definitions for "reliability," "completeness," and "accuracy."

- "Reliability" means that data are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.

- "Accuracy" refers to the extent that recorded data reflect the actual underlying information.

- "Completeness" refers to the extent that relevant records are present and the fields in each record are populated appropriately.

We used computer-processed data extracted from the ITSM system. Testing performed on the data helped us determine the data's completeness and accuracy. By testing the laptop receiving log and interviewing AMB receiving staff, we determined that laptops were added to the ITSM system as they were received; therefore, the inventory was complete. However, through testing of the laptop inventory, we determined that the user and location information in the ITSM system was inaccurate, as discussed in this report.

Using GAO's definition of "reliability" and the results of our testing, we concluded that laptop location and end user information in the ITSM system was inaccurate and, therefore, unreliable. Our results demonstrate that OIT staff did not consistently update within the ITSM system each asset's assigned SEC facility, user, user location, and current status (i.e., lost, stolen, or disposed).

**Sampling Methodology.** To accomplish our objectives, we selected from the SEC's IT inventory a statistical sample of 244 laptops. We also selected a judgmental sample of an additional 244 laptops, for a total of 488 laptops reviewed. We chose to select assets assigned to the SEC's headquarters and the NYRO because the majority of SEC laptops were assigned to these facilities. In addition, we chose to include laptops assigned to the ARO and the DRO to ensure that representative regional office operations and activities were included in our review. According to the ITSM system, as of April 1, 2014, about 65 percent of the SEC's total population of 5,525 laptops were assigned to the locations selected for review.

*Statistical Sampling.* Using the data included in the ITSM system as of April 1, 2014, we developed a stratified statistical sample for the locations we reviewed. The sample size for each location was determined using the following parameters and EZ-Quant statistical software[30]:

a) a presumed error rate of 5 percent;

b) a desired maximum precision range of 10 percent; and

c) a desired confidence level of 90 percent.

After the sample size was determined, we selected items from the inventory for testing using EZ-Quant's random number generator. The total population at the locations reviewed was 3,601 laptops. A statistical sample of 244 laptops from the SEC's IT inventory records was selected to test as follows:

- 74 of the 2,795 laptops assigned to the SEC's headquarters;[31]
- 56 of the 120 laptops assigned to the ARO;
- 52 of the 118 laptops assigned to the DRO; and
- 62 of the 568 laptops assigned to the NYRO.

We visited the locations selected to verify each asset's existence and the accuracy of the information recorded in the inventory (referred to as existence testing). As discussed in this report, we projected the results of our tests to the laptop populations at each location we visited to determine how many errors could be anticipated. We also used GAO guidance on statistical sampling to calculate the sampling error for each projection.[32]

*Judgmental Sampling.* While performing existence testing, we judgmentally selected laptops found on-site and traced them back to the inventory records to determine

[30] EZ-Quant is a suite of three statistical applications for performing statistical sampling, regression analysis, and improvement curve analysis. The Defense Contract Audit Agency developed and tested it for use in its audit processes.

[31] Initially, our headquarters sample included 21 laptops from the Operations Center. However, since OIT had not updated the location information for any of the laptops assigned to the Operations Center, we removed these assets from our sample and select 21 additional laptops from the SEC's headquarters population using the inventory dated April 1, 2014. We used EZ-Quant to verify that the sample size did not change, even though the tested population was reduced. The sampling parameters and our methodology for using EZ-Quant's random number generator for sample selection, verifying the existence of the laptops, and projecting our results to the population remained unchanged.

[32] GAO, *Using Statistical Sampling*, GAO/PEMD-10.1.6, Revised May 1992.

whether the records were accurate and complete (referred to as completeness testing). Specifically, we judgmentally selected an additional 74, 56, 52, and 62 laptops (for a total of 244) found at the SEC's headquarters, the ARO, the DRO, and the NYRO, respectively.

**Prior Coverage.** In March 2008, the Office of Inspector General issued the inspection report *Controls over Laptops,* Report No. 441.[33] The report contained three findings related to the SEC's policy, inventory, and accountability for laptops. Specifically, we found that the SEC had not identified laptops as sensitive property and annual inventories of sensitive property were not performed. Also, we could not determine the total number of laptops within the SEC and determined that OIT's AMB did not have appropriate controls over laptops and was unable to trace ownership to specific SEC employees. The OIG attributed this issue to the AMB's failure to consistently complete supporting property transaction forms.

We made five recommendations for corrective action, which are summarized below:

A – Revise draft policy to identify sensitive property.

B – Develop a method of accountability for sensitive property that would ensure an accurate accounting of laptops.

C – Complete a full inventory of laptops to establish a baseline.

D – Establish clear accountability for laptops including documenting the SEC employees who are issued and who receive equipment.

E – Create a form to account for sensitive property.

Although the OIG concurred with the actions taken to address the recommendations and closed the recommendations during fiscal year 2009, we determined that the SEC's inventory over laptops is still inaccurate, as stated in this report.

[33] U.S. Securities and Exchange Commission, Office of Inspector General, Inspection Report No. 441, *Controls Over Laptops*, March 31, 2008. The report can be accessed at: http://www.sec.gov/oig/reportspubs/ir441.pdf.

# Appendix II. Federal Laws and Guidance and SEC Administrative Regulations, Policies, and Procedures

We reviewed the following documents during the course of our fieldwork:

**Federal Laws and Guidance:**

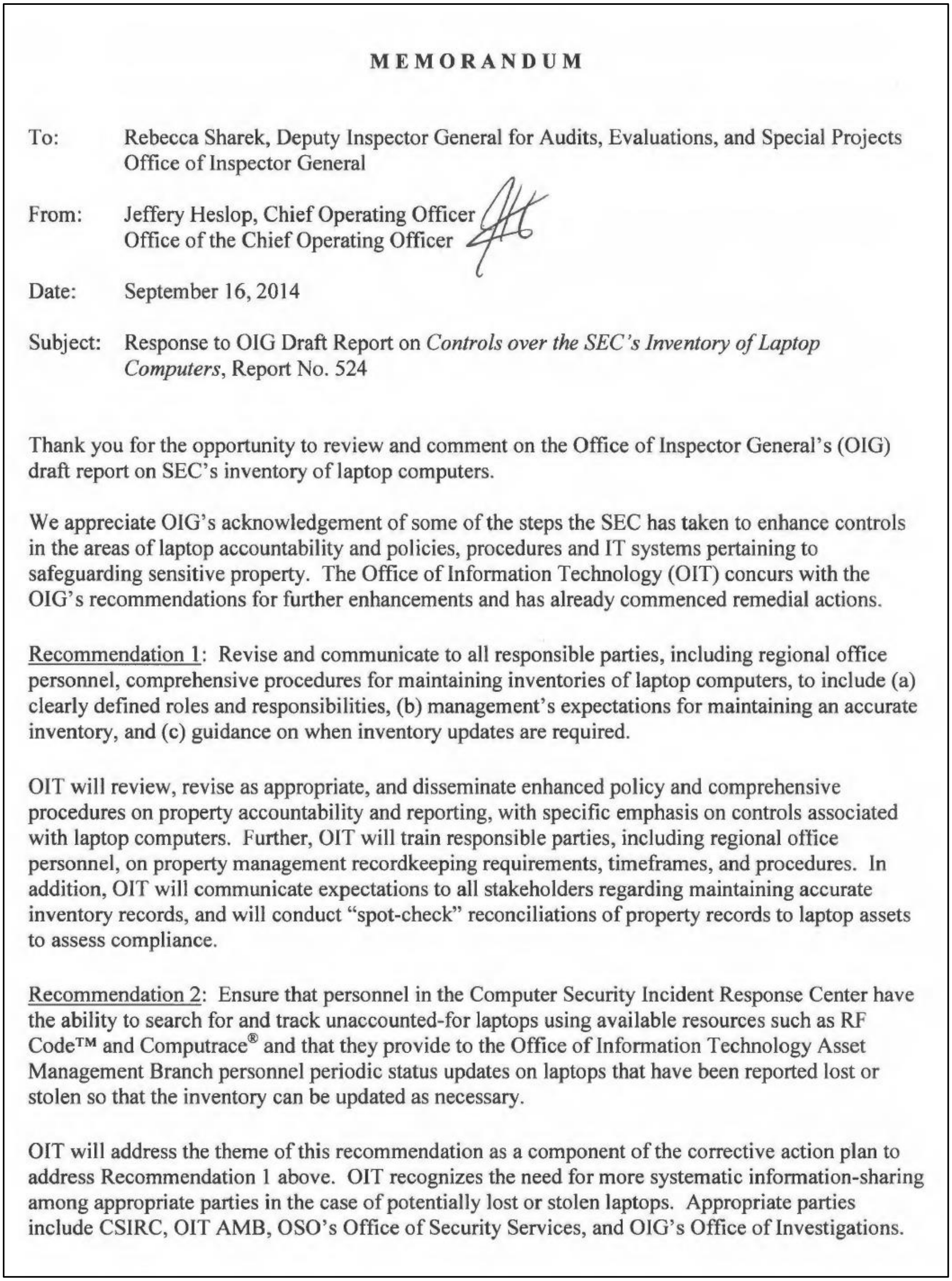
- Federal Manager's Financial Integrity Act of 1982, Pub. L. 97-255.
- GAO, *Using Statistical Sampling*, GAO/PEMD-10.1.6, Revised May 1992.
- GAO, *Assessing the Reliability of Computer-Processed Data*, GAO-09-680G, July 2009.
- OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, December 21, 2004.
- OMB Circular A-130 Revised, Transmittal Memorandum #4, Management of Federal Information Resources, November 28, 2000.

**SEC Administrative Regulations, Policies, and Procedures:**

- SEC Administrative Regulation SECR 09-02, Rev. 1, *Property Management Program*, September 11, 2012.
- SEC Administrative Regulation SECR 09-03, *Report of Survey Program*, March 18, 1996.
- SEC Administrative Regulation SECR 23-2a, *Safeguarding Nonpublic Information*, January 21, 2000.
- SEC SOP-206-1309, *AMB Reconciliation of Delphi-RF Code and Delphi-ITSM Standard Operating Procedure*, June 12, 2013.
- SEC AMB, *AMB Ship Hardware Procedure* (Draft), July 31, 2013.
- SEC AMB WI, *Auditing IMACs with CoR*, November 8, 2013.
- SEC AMB WI, *Conducting Spot Inventories*, November 8, 2013.
- SEC ISS-AM-PD-0018, *Release IT Hardware Asset Procedure*, July 31, 2013.
- SEC ISS-AM-PD-0022, *AMB Receiving Procedure* (Draft), July 12, 2013.

- SEC ISS-AM-PD-0022*, Maintenance, Repair, and Return Material Authorization Procedure* (Draft), July 29, 2013.
- SEC ISS-AM-PD-0025, *Retire IT Hardware Asset Procedure*, July 31, 2013.
- SEC ISS-AM-PD-0036, *Perform Inventory Audit Procedure*, February 5, 2010.
- SEC ISS-AM-PD-0038, *Manage Stock Levels Procedure*, March 23, 2010.
- SEC ISS-PM-WI-0002 v.0.2, *Manage Asset Record*, September 14, 2010.
- Securities and Exchange Commission, Office of Information Technology, Security Operations, *SEC Incident Response Capability Handbook*, April 2014.

# Appendix III. Management Comments



## MEMORANDUM

To: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects
Office of Inspector General

From: Jeffery Heslop, Chief Operating Officer
Office of the Chief Operating Officer

Date: September 16, 2014

Subject: Response to OIG Draft Report on *Controls over the SEC's Inventory of Laptop Computers*, Report No. 524

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on SEC's inventory of laptop computers.

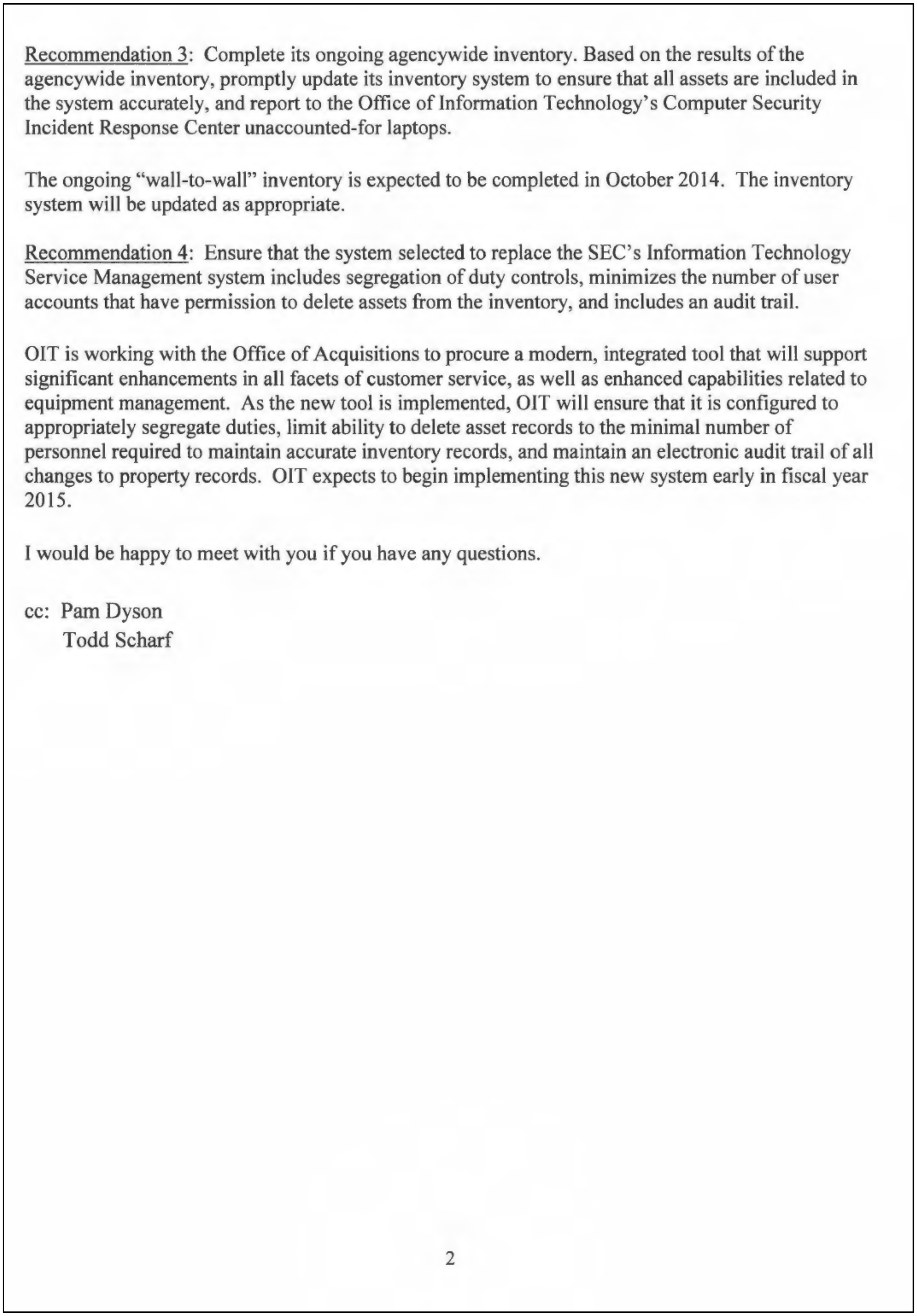
We appreciate OIG's acknowledgement of some of the steps the SEC has taken to enhance controls in the areas of laptop accountability and policies, procedures and IT systems pertaining to safeguarding sensitive property. The Office of Information Technology (OIT) concurs with the OIG's recommendations for further enhancements and has already commenced remedial actions.

Recommendation 1: Revise and communicate to all responsible parties, including regional office personnel, comprehensive procedures for maintaining inventories of laptop computers, to include (a) clearly defined roles and responsibilities, (b) management's expectations for maintaining an accurate inventory, and (c) guidance on when inventory updates are required.

OIT will review, revise as appropriate, and disseminate enhanced policy and comprehensive procedures on property accountability and reporting, with specific emphasis on controls associated with laptop computers. Further, OIT will train responsible parties, including regional office personnel, on property management recordkeeping requirements, timeframes, and procedures. In addition, OIT will communicate expectations to all stakeholders regarding maintaining accurate inventory records, and will conduct "spot-check" reconciliations of property records to laptop assets to assess compliance.

Recommendation 2: Ensure that personnel in the Computer Security Incident Response Center have the ability to search for and track unaccounted-for laptops using available resources such as RF Code™ and Computrace® and that they provide to the Office of Information Technology Asset Management Branch personnel periodic status updates on laptops that have been reported lost or stolen so that the inventory can be updated as necessary.

OIT will address the theme of this recommendation as a component of the corrective action plan to address Recommendation 1 above. OIT recognizes the need for more systematic information-sharing among appropriate parties in the case of potentially lost or stolen laptops. Appropriate parties include CSIRC, OIT AMB, OSO's Office of Security Services, and OIG's Office of Investigations.



Recommendation 3: Complete its ongoing agencywide inventory. Based on the results of the agencywide inventory, promptly update its inventory system to ensure that all assets are included in the system accurately, and report to the Office of Information Technology's Computer Security Incident Response Center unaccounted-for laptops.

The ongoing "wall-to-wall" inventory is expected to be completed in October 2014. The inventory system will be updated as appropriate.

Recommendation 4: Ensure that the system selected to replace the SEC's Information Technology Service Management system includes segregation of duty controls, minimizes the number of user accounts that have permission to delete assets from the inventory, and includes an audit trail.

OIT is working with the Office of Acquisitions to procure a modern, integrated tool that will support significant enhancements in all facets of customer service, as well as enhanced capabilities related to equipment management. As the new tool is implemented, OIT will ensure that it is configured to appropriately segregate duties, limit ability to delete asset records to the minimal number of personnel required to maintain accurate inventory records, and maintain an electronic audit trail of all changes to property records. OIT expects to begin implementing this new system early in fiscal year 2015.

I would be happy to meet with you if you have any questions.

cc: Pam Dyson
Todd Scharf

# Appendix IV. OIG Response to Management Comments

We are pleased that the OIT concurred with all four recommendations for corrective action. Management's proposed actions are responsive to the recommendations; therefore, the recommendations are resolved and will be closed upon completion and verification of appropriate corrective action. Full implementation of our recommendations should strengthen the SEC's inventory controls over its laptop computers.

## To Report Fraud, Waste, or Abuse, Please Contact:

| | |
|---|---|
| Web: | www.reportlineweb.com/sec_oig |
| E-mail: | oig@sec.gov |
| Telephone: | (877) 442-0854 |
| Fax: | (202) 772-9265 |
| Address: | U.S. Securities and Exchange Commission<br>Office of Inspector General<br>100 F Street, N.E.<br>Washington, DC  20549-2736 |

## Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6061. Comments, suggestions, and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.