UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Laptop Computer Accountability and Security

Report No. OIG-AMR-59-09-01

February 2009

INSPECTOR GENERAL

NATIONAL LABOR RELATIONS BOARD

WASHINGTON, DC 20570

February 27, 2009

I hereby submit a review of Laptop Computer Accountability and Security, Report No. OIG-AMR-59-09-01. This audit was conducted to determine whether Agency-owned laptop computers are properly controlled and configured to protect sensitive data.

We found that the Agency's laptop computers are not properly controlled and not all of the laptop computers are configured to protect sensitive data. In general, the Office of the Chief Information Officer lacks a system of internal control for the Agency's laptop computers. As a result, there is a significant risk of loss of equipment and, therefore, the data stored on that equipment. Just as significant as the lack of internal control, we found that personnel who are responsible for managing the laptop computers as an Agency asset lacked an understanding of those duties.

In addition to the lack of internal control, during the course of the audit we identified 21 laptop computers as either being lost, stolen, or otherwise missing. We also found that two additional laptop computers had been improperly removed from the electronic inventory system. Information regarding these laptop computers was referred to the Office of Inspector General investigative staff.

In his comments to the draft report, the Chief Information Officer stated that 17 of the 21 laptop computers that were missing were considered excess equipment and ready for disposal. He also noted that the 17 laptop computers were purchased prior to the Office of the Chief Information Officer being relocated in the Agency's organizational structure. While both of those points may be accurate, our concern with that analysis is that management officials cannot demonstrate that the loss of any one of the 17 missing laptop computers occurred before the change in the organizational structure or after the computer's useful life.

We have attempted to make detailed recommendations that will assist the Chief Information Officer in creating a system within his organization that achieves an appropriate level of internal control. Given the level of lack of internal control that we observed during the audit process and the risk it poses to the Agency, we will assess the effectiveness of the Chief Information Officer's actions in implementing the recommendations.

The Chief Information Officer's written comments to our draft report are attached as an appendix. The Chief Information Officer generally agreed with the findings and recommendations made in our report. The written comments state that two of the six recommendations have been implemented and addresses plans to implement the four remaining recommendations.

David P. Berry
Inspector General

TABLE OF CONTENTS

BACKGROUND

The National Labor Relations Board (NLRB or Agency) administers the principal labor relations law of the United States, the National Labor Relations Act of 1935, as amended. To assist in achieving that mission, the Agency procured 1,037 laptop computers between October 2004 and September 2007, at a cost of approximately $1.4 million. The laptop computers have been deployed at the Agency's Headquarters and across the 51 field offices and 3 administrative law judges satellite offices.

Within the Office of the Chief Information Officer (OCIO), responsibility for the management of the laptop computers is assigned to the Associate Chief Information Officer (CIO) for Customer Support. The Associate CIO for Customer Support administers those duties by assignment of them to the contractor who provides the OCIO's Help Desk services. To track and record information about individual laptop computers throughout their life cycle at the Agency, the Help Desk contractor's employees use a system called HEAT Asset Tracker or "HAT." "HEAT" is an acronym for Helpdesk Expert Automation Tool.

Several high-profile incidents at other agencies have identified a lack of control over laptop computers and the sensitive data maintained on them. On June 23, 2006, the Office of Management and Budget (OMB) issued Memorandum 06-16, *Protection of Sensitive Agency Information*. The memorandum identified applicable National Institute of Standards and Technology criteria to be followed and recommended steps that agencies should take that included encrypting data on mobile computers and devices, use of two-factor authentication, using a time-out function, and logging computer-readable data extracts. Responsibility for the implementation of these procedures is assigned to the Associate CIO for Information Technology (IT) Security.

Once a laptop computer has reached the end of its useful life at the Agency, it is considered "excess" property and, at Headquarters, is transferred to the Procurement and Facilities Branch (PFB) to be disposed of in accordance with Government-wide procedures. Field offices dispose of excess property locally. At the NLRB, the general practice has been to donate the excess laptop computers to educational or charitable organizations.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether Agency-owned laptop computers are properly controlled and configured to protect sensitive data. Our scope was laptop computers purchased or disposed of between October 2003 and March 2008.

We reviewed Government-wide laws, regulations, and policy documents regarding property management and information security. We also reviewed Agency policies and procedures to identify operating procedures and for more detailed guidance of property management and information security practices. We interviewed employees in the OCIO, the PFB, and the Help Desk contractor to identify the operating procedures for the life cycle of laptop computers.

We obtained and reviewed accounting reports, requisition orders, purchase orders, packing slips, and invoices for laptop computers purchased by the Agency between October 1, 2003 and March 2008, to identify the universe of laptop computers purchased by the Agency. We contacted the vendors and shipping agents to obtain additional information regarding the laptop computers.

We evaluated controls over laptop computers from the initial purchase through disposal. We reconciled the Agency's inventory of laptop computers to the acquisition documentation. We also reviewed the Agency's implementation of the OMB memorandum regarding encryption and the standard security configuration.

We evaluated HAT to determine whether it meets the Financial System Integration Office, formerly known as the Joint Financial Management Improvement Program (JFMIP), Property Management System Requirements.

This audit was performed in accordance with generally accepted government auditing standards during the period June 2008 through January 2009. 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 conducted this audit at NLRB Headquarters in Washington, DC.

FINDINGS

The Agency's laptop computers are not properly controlled and not all of the laptop computers are configured to protect sensitive data. The OCIO is not able to account for all of the laptop computers that it has purchased. The process for receiving and deploying laptop computers is not documented in policy documents. The system to monitor the inventory of laptop computers is unreliable in that it lacks accuracy and is subject to improper manipulation. There is also a lack of segregation of duties among the employees of the contractor who operated the database that maintains the inventory of laptop computers. The system used by the Associate CIO for IT Security to ensure that laptop computers are encrypted is not reliable and the OCIO had not implemented the Commonly Accepted Security Configurations, as required by OMB.

LOST OR STOLEN LAPTOP COMPUTERS

Twenty-one laptop computers were identified as being either lost, stolen, or missing. The situations involving these laptop computers are detailed below:

- The Associate CIO for Customer Support identified two laptop computers that he believed were returned to the manufacturer for repair, but no records or supporting documentation exists to support that belief.

- The Associate CIO for Customer Support identified one laptop computer, from the OCIO loaner pool, that was temporarily issued to an employee in July 2006, who then left the Agency in June 2007. HAT records show that, in December 2007, the laptop computer was reassigned from that former employee to storage. The laptop computer is now missing.

- Inventories conducted in Regional Offices listed five laptop computers that were identified by Regional Office personnel as lost or missing.

- Twelve laptop computers were identified as either "Missing/Research" or "Loss/Stolen" in a document titled "Inventory of Donated/Scrapped Items" that is maintained by the contractor's database administrator.

- One laptop computer was on a list of serial numbers from the manufacturer used to input information into HAT, but this laptop computer was not in HAT. Based on a review of invoices and related payments, it appears that the Agency paid for this laptop computer.

The Agency's Administrative Policies and Procedures Manual (APPM) Chapter PRO-1(A), *Personal Property Management and Accountability*, requires that the

property custodian immediately notify the Chief, Security Branch, and the Property Management Section upon discovery or awareness of any loss, theft, or damage to Agency property. We could not locate any information that this requirement was fulfilled until well after the initiation of this audit. Independent of that action, information regarding these laptop computers is being reviewed for possible investigation.

In his comments to the draft report, the CIO stated that 17 of the 21 laptop computers that were missing were considered excess equipment and ready for disposal. The CIO also noted that the 17 laptop computers were purchased prior to the OCIO being relocated in the Agency's organizational structure. While both of those points may be accurate, our concern with that analysis is that management officials cannot demonstrate that the loss of any one of the 17 missing laptop computers occurred before the change in the organizational structure or after the computer's useful life.

CONTROLS OVER LAPTOP COMPUTERS

Internal control serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. It should not be thought of as a single event, but rather as a series of actions and activities that occur throughout the operation of the Agency and on an ongoing basis.

The Agency did not utilize written procedures for managing laptop computers throughout their life cycle. Because proper documentation was not maintained, acceptance and inspection of laptop computers could not be verified. Laptop computers were not stored in secured locations prior to deployment or issuance to individual employees. Information regarding individual laptop computers was not timely entered into HAT upon receiving the laptop computers from the vendor and HAT was not maintained in a manner that ensured an acceptable level of accuracy. The HAT database administrator had the ability to input, change, and remove records from HAT.

Written Procedures

Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. Documentation of internal control procedures should appear in management directives, administrative policies, or operating manuals. The auditor met with representatives from the OCIO, Help Desk contractor, and PFB between June 24 and July 9, 2008, to identify procedures related to inventory management throughout the laptop computer life cycle. On July 16, 2008, the auditor requested that the Associate CIO for Customer Support provide the standard operating procedures or desk manuals for this life cycle.

On July 29, 2008, the Associate CIO for Customer Support responded to the request for documentation of procedures by stating that there were no written procedures and that the unwritten procedures that were used varied over time based upon changing conditions.

On October 16, 2008, the Associate CIO for Customer Support provided the Office of Inspector General (OIG) with written procedures. At that time, he stated that an OCIO employee found an electronic copy of the procedures when she was reviewing their network drive that they use to store electronic documents. He also stated that he had not reviewed the document to determine whether it reflects their current practices.

Without written procedures that are properly issued, there is a complete lack of internal control and employees and contractors cannot be expected to know how to correctly perform their duties.

Receiving, Acceptance, and Inspection

The Federal Acquisition Regulation (FAR) requires that a Government employee inspect goods to ensure that they conform to the contract's requirements and to document the inspection and acceptance of the goods. The FAR also requires that an agency have procedures and instructions for this function. The Agency's APPM has a provision that addresses inspecting and using the Form NLRB-12 to note discrepancies and damage, but those procedures do not address noting acceptance. The Agency's record retention guidelines require that such records be maintained for 2 years after the end of the fiscal year (FY) that items were received.

Generally, computer shipments delivered to Headquarters were addressed to the warehouse foreman. Upon receiving a shipment of laptop computers, the warehouse employee contacted the OCIO to inform them of the delivery. The Associate CIO for Customer Support then told the warehouse employee where to deliver the equipment. No particular OCIO staff member was responsible for acceptance or confirmation of the laptop computers that were delivered to Headquarters and no documentation of the transfer between PFB and OCIO took place.

Occasionally, a laptop computer was shipped to the Agency by a method that resulted in delivery through the mailroom. Three deliveries of 15 laptop computers were received by the mailroom and had an acknowledgment of receipt.

Laptop computers delivered to field offices were either sent directly to the field offices by the vendor or sent to Headquarters, and then deployed. When laptop computers were sent directly from the vendor to the field office, personnel in

the field office either called or sent an e-mail message to the OCIO Customer Relations Manager to verify receipt. According to OCIO personnel, packing slips for these shipments were to be maintained in the field offices.
We reviewed the OCIO and Finance files to determine if inspections of the laptop computer shipments were conducted and how damage, discrepancies, and acceptance were recorded. We were not able to locate any Form NLRB-12s in those files. We did find, however, packing slips that had some indication of inspection and acceptance. This is a summary of our effort to verify proper inspections and acceptance:

- We could not locate any packing slips for the 230 Dell D610 laptop computers that were purchased at the end of September 2005 and received in FY 2006. The invoices identify Headquarters as the delivery location.

- During FY 2005, the OCIO purchased 11 other miscellaneous laptop computers and maintained the packing slips with notations for inspection and acceptance for each shipment.

- Finance and the OCIO were able to provide packing slips for 309 of the 614 Dell D820 laptop computers purchased at the end of FY 2006 and received in FY 2007. Some of these laptop computers were shipped to Headquarters and others were shipped directly to field offices. Only one packing slip for 39 laptop computers showed any evidence of inspection and acceptance, which was in the form of checkmarks on the document. The document did not identify the person receiving the goods or the date this occurred.

- Packing slips were located for all 182 Dell D830 laptop computers purchased at the end of FY 2007. The packing slips had some notation of acceptance for 176 of the 182 laptop computers. The notations consisted of checkmarks on the packing slip. The packing slips did not identify when or who performed the acceptance.

Because the OCIO is responsible for approving invoices for payment and maintaining the inventory of the laptop computers, it would appear to be reasonable that the documentation of acceptance and discrepancies should be maintained by that office. By doing so, the OCIO would instill accountability and have accurate and verifiable information to begin the process of controlling the laptop computer inventory.

Physical Control over Laptop Computers

Standards for Internal Control in the Federal Government state that an agency must establish physical control to secure and safeguard vulnerable assets. Examples of appropriate physical controls include limiting access to equipment

and inventories. It also includes the creation and maintenance of appropriate control records to which the inventories can be compared.

Storage of Laptop Computers

Keys used to gain access to computer storage areas at Headquarters were kept in an unsecure location. As a result, those areas were vulnerable to unauthorized access. During the audit field work, we brought this issue to the attention of OCIO staff and, because of the potential for loss, requested that they properly secure the keys to the laptop computer storage areas.

Field offices were not instructed to keep the laptop computers shipped to them in a locked area pending deployment. The Associate CIO for Customer Support stated that field offices were instructed to not open any of the boxes. In December 2006, OIG staff observed laptop computers awaiting deployment being stored in an unsecured Regional Office conference room.

Physical Inventory

APPM Chapter PRO-1(A), *Personal Property Management and Accountability*, states that property custodians are responsible for performing annual physical inventories as appropriate for assigned property.

An inventory of field office equipment was conducted by the contractor database administrator between March and July 2008. The inventory was conducted by the contractor database administrator sending spreadsheets generated from HAT listing the equipment assigned to the particular field offices. Field office employees were instructed to verify the information in the spreadsheet, identify changes that were needed, and send the spreadsheet back to the database administrator. There was no verification of the information provided by the field offices. Responses from six field offices could not be located and, therefore, were not available for our review.

We were unable to find any records of a comprehensive physical inventory of laptop computers that had been performed at Headquarters, and documentation was not maintained for the limited work that was claimed to be performed.

Control Records

Entering Laptop Computers in HAT

Information pertaining to the receipt of laptop computers was not recorded into HAT in a timely manner. Date of delivery information was available for 398 of the 1,037 laptop computers that were purchased between FY 2004 and March

31, 2008. We compared the date that the HAT record was created for an individual laptop computer to its delivery date. Based on the comparison, we found that most of the 398 laptop computers were entered into HAT more than a month after being received by the Agency. Details of our testing appear in the table below:

	Fiscal Year 2005 Dell D610		**Fiscal Year 2006 Dell D820**		**Fiscal Year 2007 Dell D830**	
Time to Record	**Number**	**Percent**	**Number**	**Percent**	**Number**	**Percent**
Within 1 day	6	2.93	0		22	12.16
Within 1 week	0		0		24	13.26
Within 1 month	8	3.90	1	8.33	73	40.33
More than 1 month	191	93.17	11	91.67	62	34.25
Total	205	100.00	12	100.00	181	100.00

Given the lack of physical security over the laptop computers and the failure to create and/or maintain evidence of acceptance and inspection, the failure to initiate a timely control record creates a significant risk of loss to the Agency.

Purchases Information

For the Hewlett Packard Business Notebooks and Dell model D610, D810, D820, and D830 laptop computers, we identified discrepancies between the data in HAT and the purchase orders, shipping documents, and invoices we reviewed. In all, we found 44 discrepancies. Because the Agency did not maintain appropriate control records, much of the information used to resolve these items was obtained directly from the manufacturer. The discrepancies are outlined below:

Description	**Number**
Serial numbers for laptop computers on an invoice that was paid were not in HAT. The manufacturer provided the OIG with information documenting that laptop computers with different serial numbers were shipped to the Agency. Agency records did not address the discrepancy.	24
Laptop computers replaced under warranty were removed from HAT and there was no notation that the new laptop computer was a replacement.	10

Excessed laptop computers removed from HAT.	3
Laptop computers purchased by the Agency that were not in HAT, but were identified as being logged into the Agency network.	2
Laptop computers retained by the Agency when they should have been returned to the vendor.	2
Laptop computers with no record showing they were received by the Agency, but for which a record of payment exists.	1

We also discovered that, in May 2008, an OCIO employee directed that a Dell D810 laptop computer that was in HAT be removed from HAT. The bar code sticker was removed from the laptop computer and it was given to a contractor's employee to be excessed or to do what he wanted with it. When we first made inquiries about the location of the laptop computer, the OCIO employee could not recall any information regarding the laptop computer. The next day, the OCIO employee informed us that the laptop computer had been found. At that time, no mention was made that it had been in HAT and was removed or that the bar code sticker had been removed. The OCIO employee did state that the laptop computer had been abandoned by the vendor, that it was an evaluation unit, and that he could do whatever he wanted with it. Those assertions were not correct in that the Agency paid for the laptop computer.

We later discovered misleading information related to the removal of the laptop computer that was recorded in the HEAT Help Desk "tickets." The information on the ticket states that the Dell D810 laptop computer was an evaluation unit that was removed from HAT and sent back to the vendor by the OCIO employee.

We found that another laptop computer, a Dell D820, was also removed from HAT after the OCIO employee again erroneously came to the determination that the Agency had not purchased it. This time, the OCIO employee stated that he was told that the vendor had no record of selling the laptop computer to the Agency. In August 2008, the laptop computer was identified in HAT as missing. After October 15, 2008, the record of the laptop computer was removed from HAT. When we made an inquiry about the status of the laptop computer in December 2008, the laptop computer was identified to us as one that was being used by the OCIO. The OCIO employee could not explain how or when this laptop computer ended up being used by the OCIO. The OCIO employee explained to us that someone told him that the Agency had not

purchased the laptop computer. He stated that the person had spoken to the vendor's representative and that the vendor had no record of selling the computer to the Agency. Based on our review of the invoices and payments, we determined that the Agency purchased and paid for this laptop computer.

Assignment Accuracy of HAT

A statistical sample of equipment in HAT as of August 22, 2008, was tested to determine the accuracy of the laptop computer inventory. The database contained 1,156 units. A 90 percent confidence rate resulted in a sample size of 75 items. The 90 percent confidence level is consistent with Government Accountability Office guidance and our expected deviation rate. The results of our test can be projected to the population.

We compared the items in the sample to Systems Management Server (SMS) reports that listed the laptop computers logged on to the Agency's network and received software updates. Items at Headquarters that were not on SMS scans were physically inspected. We verified the existence of laptop computers in field offices that were not in SMS scans with either office managers or employees assigned the laptop computers.

HAT records were not accurate for 5 of the 75 (7 percent) laptop computers tested. HAT showed one laptop computer assigned to an OCIO employee, but the laptop computer was actually in a loaner pool in a Regional Office. One laptop computer assigned to a Division of Judges loaner pool was permanently assigned to an employee. A Regional Office sent one laptop computer to Headquarters on May 14, 2008, to be excessed. HAT showed this laptop computer assigned to the Regional Office as of August 22, 2008. In another Regional Office, two laptop computers were transferred to another Government agency on June 10, 2008, yet still appeared in the Agency's inventory on August 22, 2008.

Other Assignment Errors Noted During the Audit

In addition to the errors found in the statistical sample, while reviewing records we found the following assignment errors:

- Three laptop computers were removed from HAT, but in fact had been reassigned to Agency personnel and a contractor's employee.

- Seven laptop computers that had been assigned to a Headquarters employee had in fact been distributed to seven field office employees.

Laptop Computers Removed from HAT

JFMIP-SR-00-4, *Property Management System Requirements*, states that property management systems must record beginning balances, acquisitions, and withdrawals. The system must also identify the type of transaction affecting the property item, e.g., initial acquisitions, change in location, and disposal.

The OCIO removed a laptop computer from HAT when it was excessed, when one was replaced under warranty, and when one could not be found. Removing equipment from HAT destroys the history of the transactions involving the laptop computer and prevents maintenance of a control record. The result is that there is no record in the inventory system that the Agency ever owned the laptop computer and it is not possible to reconcile the actual inventory of laptop computers to the expected inventory.

Segregation of Duties

Standards for Internal Control in the Federal Government state that key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets.

Regional Office inventories were coordinated by the Help Desk contractor's employee who is the HAT database administrator. By having the database administrator performing this function, a lack of segregation of duties exists because the same person that is processing and recording transactions is also reviewing them by performing the inventory.

The contractor's HAT database administrator also inputted new laptop computers into the HAT system and removed laptop computers from that system when they were excessed. We found no records that documented the review, verification, or approval of that action. The result is that this individual has the ability to input or remove any laptop computer without detection by the OCIO's staff.

Another of the Help Desk contractor's employees has the ability to process and record activity related to excess equipment in HAT and handles the related asset without the transaction being reviewed. There was no evidence that the list of excessed equipment created by the contractor's employee and provided to the database administrator so that the equipment can be removed from HAT was approved or verified by an OCIO employee.

Assignment of Accountable Property Officer

APPM Chapter PRO-1(A) states that the Accountable Property Officer is responsible for maintaining an unbroken audit trail for acquisition, receipt, issue, transfer, and disposal of Agency property. The appointment is to be in writing by the PFB Chief.

The Agency has not appointed an Accountable Property Officer for laptop computers in a formal appointment document. The position description for the Associate CIO for Customer Support, however, states that the person in that position "[d]evelops and maintains a system for collecting, tracking/reconciling, and updating a database of all IT resources (computers, peripherals, and software licensing)." This responsibility is for all NLRB locations. The position description is not a replacement for a written appointment.

INFORMATION SECURITY

Encryption

OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, was issued on June 23, 2006. This memorandum requires agencies, among other things, to encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive.

The Agency implemented this memorandum through APPM Chapter IT-4, *Protection of Sensitive Agency Information*, issued on July 31, 2007. This policy states that all Agency laptop computers will have encryption software installed, regardless of the sensitivity of the data stored on it.

Sixty-eight of the Agency's laptop computers that were identified as being "installed" were not encrypted. The Agency's inventory consisted of 1,159 laptop computers on October 15, 2008. Of that number, 73 were either in storage or in the process of being excessed. The list of encryption keys, which documents laptop computers with encryption, provided by the IT Security Office on October 9, 2008, included 1,018 laptop computers, leaving a balance of 68 in the Agency's inventory that were not encrypted. Of those 68 laptop computers, 6 laptop computers may have been issued an exemption by the OCIO from the encryption process.

We were unable to ascertain exactly which laptop computers were not encrypted because the encryption key report does not identify the serial number of the laptop computers. Instead, it uses the NetBIOS name as the identifier and the NetBIOS names are not captured in HAT.

The procedure used by the IT security personnel to determine whether the laptop computers being used are encrypted consists of obtaining a list of Dell

Models D610, D820, and D830 from the HAT database administrator and manually comparing this to a report provided by the encryption software vendor. The computer NetBIOS name is compared to the customer identification name. The weakness with this method is that it uses a manual process to compare the NetBIOS name and the customer identification field, and the two are not identical.

Another weakness with this process is that it relies on an incomplete inventory of the Agency's laptop computers. By May 15, 2008, any laptop computer that was designated as obsolete by the OCIO was to be removed from use by Agency personnel. Despite that directive, we found that 71 laptop computers that were designated as obsolete were listed in HAT and categorized as "installed." The procedures described by the IT Security Office to ensure that laptop computers were encrypted did not include reviewing reports that listed this obsolete, but "installed" equipment.

Commonly Accepted Security Configurations

OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, was issued on March 22, 2007. This memorandum required agencies that either operate and/or plan to upgrade to either Windows XP or Vista adopt the Commonly Accepted Security Configurations (CASC) by February 1, 2008.

The Agency had not fully implemented the CASC. In August 2008, the Associate CIO for IT Security said that a pilot project was being conducted at one Regional Office and one Headquarters office. On October 31, 2008, the Associate CIO for Customer Support identified an additional office that was selected as a pilot for this initiative. At that time, the Associate CIO for Customer Support said that the CASC have not been fully implemented. He stated that the OCIO wanted to comply with the memorandum, but many of the security settings do not allow some of the Agency applications to properly execute.

In his comments to the draft report, the CIO stated that all but 18 of the more than 600 security settings were implemented across the Agency in January 2009. The CIO also stated that the 18 security settings that were not implemented were reported as an exception to OMB. We will evaluate the implementation of these settings during the audit follow-up process.

DONATED COMPUTER EQUIPMENT

Executive Order 12999, issued on April 17, 1996, created a program that directs agencies to give educationally useful excess Federal equipment to

schools and nonprofit organizations. Agencies are either to give such excess equipment directly to a school or nonprofit group or to the General Services Administration for redistribution. This program has come to be known as "Computers for Learning."

Inconsistent Internal Documents and Records for Headquarters

When laptop computers are identified for disposition as excess equipment, a Help Desk contractor's employee prepares a schedule of this property and sends it via an e-mail message to another Help Desk contractor's employee to open a service ticket. That person also sends an e-mail message to PFB's warehouse unit with a list of equipment to be donated that is then to be used to compare to the property actually delivered to the warehouse.

The Help Desk contractor's employee who creates these schedules maintains copies of them, but does not save the related e-mail messages. The database administrator, also a Help Desk contractor's employee, accumulates and compiles the information from the service tickets on a spreadsheet and later removes the laptop computers from HAT either in a large group or once a month depending on the volume of activity. PFB maintains receipts from organizations that receive the excessed laptop computers from Headquarters. These three pieces of information should be in agreement.

We identified nine laptop computers that should have been included in the e-mail messages sent to the Help Desk that were not located in the records maintained by the database administrator. Six of these were in the records maintained by PFB. We identified 38 laptop computers that were in the database administrator's records that were not located in PFB records as donated. Seven of these were in the records maintained by the contractor's employee who identifies the equipment for disposition. We also identified 14 laptop computers that were in the PFB records that were not in the database administrator's records. Six of these were in the records maintained by the contractor's employee who identifies the equipment for disposition.

Ineligible Recipients

We identified two computer equipment recipients that were ineligible to participate in the Computers for Learning program. They were ineligible because they were either not non-profit organizations registered with the Internal Revenue Service or were not educational organizations.

Staff in PFB stated that it is difficult for them to find educational or non-profit groups willing to take excess computer equipment from Headquarters. It was their observation that schools in the metropolitan District of Columbia region

have access to an extensive amount of excess computer equipment and the Agency's equipment is not competitive.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Develop and maintain a system or process that will provide proper internal control over the Agency's laptop computers throughout their asset life cycle. This system should include written procedures and a method for ensuring that the procedures are followed. Additionally, the OCIO should consider obtaining inventory control software to assist in the process. At a minimum, the actions implementing this recommendation must conform to the Standards for Internal Control in the Federal Government and the JFMIP requirements.

2. Encrypt all laptop computers that are in use by Agency personnel.

3. Develop and maintain a system that will ensure that all laptop computers in use by Agency personnel are encrypted.

4. Implement Commonly Accepted Security Configurations in conformance with OMB Memorandum 07-11.

5. Obtain training on the Standards of Ethical Conduct for Employees of the Executive Branch for the OCIO personnel in the areas of the use of Government property and dealing with outside sources.

6. Obtain training on information technology asset control for the OCIO's Customer Support Section personnel.

ATTACHMENT

JFMIP REQUIREMENTS

The Financial Systems Integration Office, formerly known as the JFMIP, published the Property Management System Requirements (JFMIP-SR-00-4) in October 2000. This document identifies functional requirements for property management systems for data systems used to manage both capitalized and expensed property.

HAT does not meet 6 of the 10 applicable requirements. A table showing the JFMIP 12 mandatory requirements and whether HAT meets those requirements is shown below.

Requirement	**Meets Requirement**
1. Record beginning balances, acquisitions, and withdrawals and calculate ending balances expressed in values and physical units, except for heritage assets and stewardship land for which all end-of-period balances are expressed in physical units only.	No
2. Capture the condition of the asset for heritage assets, stewardship land, national defense property, plant and equipment (PP&E), and general PP&E for which a condition assessment was performed.	N/A
3. Provide edits (controls) to prevent duplication and reduce the likelihood of creating erroneous property documents and records to ensure the integrity of data recorded in the system.	Yes
4. Permit only authorized users to enter, modify, or otherwise alter property records.	No
5. Provide an audit trail for entries to a property record, including identification of individuals entering or approving information and data.	No
6. Identify the type of transaction affecting the property item, e.g., initial acquisition, change in location, and disposal.	No
7. Incorporate adequate security features that prevent unauthorized access to the property system by unauthorized individuals.	Yes
8. Enable the transfer of responsibility for property from one authorized manager to another authorized manager.	Yes

	Meets

Requirement	**Requirement**
9. Capture real property information for General Services Administration's worldwide inventory system as directed in Federal Property Management Regulation 102-84 (property management only).	N/A
10. Produce reports in accordance with user-defined criteria.	Yes
11. Capture the fact that an environmental or hazardous substance is located on or contained within a property item, in accordance with 41 CFR 101-42.202.	No
12. Distinguish between capitalized property and expensed property tracked in the property management system.	No

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of the Chief Information Officer

Memorandum

February 20, 2009

To: David P. Berry
Inspector General

From: Richard D. Westfield
Chief Information Officer

SUBJECT: Laptop Computer Accountability and Security Draft Report (OIG-AMR-59)

I have reviewed the draft report, dated January 16, 2009. In general, I concur with many of the findings and have taken or plan to take actions to correct them. I also want to state that I take property accountability very seriously and I will do everything I can to establish more effective internal controls and look at more efficient ways of managing our laptop inventory.

STOLEN OR LOST LAPTOP COMPUTERS

The report states that 21 laptops that were either lost, stolen or could not be found. We do not dispute this. Since the OCIO was re-delegated under the Board, 1,105 laptops have been purchased. Of this number, only 4 are missing[1]. The other 17 listed in the report were purchased prior to August 2003 and were considered excess and ready for disposal.

CONTROLS OVER LAPTOP COMPUTERS

Written Procedures

Although Customer Service does have draft procedures, they have been loosely followed. We agree on the need to have established, documented and repeatable procedures to ensure Customer Service employees and contractors understand roles, responsibilities and expectations. Developing procedures will also assist with establishing a good set of internal controls.

Receiving, Acceptance and Inspection

As part of our written procedures, we will require all laptops to be shipped to HQ first, where they will be received, inspected and accepted. All shipment documentation will be kept on file in accordance to the Agency records retention schedule.

---

[1] This number does not include the two laptops that were reported stolen from the Appellate Court Branch in December 2008

Physical Control over Laptop Computers

In October 2008, cipher locks were installed on the two exterior doors leading into the Helpdesk area on the 7th floor. The entire OCIO area on the 7th floor is secured from 6:00pm to approximately 7:00am during the weekday and on weekends.

In the past, we evaluated securing laptops with cable locks or laptop tie-down brackets, but still maintain the cost is excessive compared to the risk. As part of our review for a new and better asset tracking program, we will research "asset recovery" solutions.

Storage of Laptop Computers

Customer Support has purchased a wall mounted combination lockbox to secure storage area door keys that in the past were placed in a non-secure area in an office. The lockbox will be installed the week of February 23rd and will be accessible to only authorized Customer Support personnel.

Physical Inventory

Although Customer Support does perform an annual inventory, we believe performing a physical inventory in a geographically distributed environment will always be difficult to reconcile and complete with accuracy. It is our intention to purchase an asset management program that will automate most of the inventory collection work for us.

Control Records

The asset tracking program currently used is obsolete and asset tracking is still very much a manual process. All the handling that occurs between the vendors, HQ, the regions and Customer Support introduces errors. We believe that an automated program to assist in asset management will eliminate most data accuracy errors and some issues related to "segregation of duties."

Segregation of Duties

Customer Service will provide more oversight into asset management and this oversight will be reflected in the new procedures.

INFORMATION SECURITY

Encryption

We have 1,111 laptops "in use." Of this number, 26 laptops are in storage, 5 laptops have been given exemptions and 1,080 have been encrypted.

Security Controls and Settings

When the audit was started, we were piloting the government mandated FDCC (Federal Desktop Core Configuration) settings. In January 2009, we implemented the security settings across the entire Agency, with the exception of 18 (out of 600+) settings that were identified during the pilot as problematic. These exceptions were reported to OMB.

RECOMMENDATIONS

1. This will require the purchase of a more robust asset management system for life cycle management. Budget permitting, we will put this into our FY09 work plan. In addition we agree on the need to review and update our procedures. Finally, we will take into consideration JFMIP requirements when evaluating a new asset management product.

2. Completed with the exception of those in storage and those that have been given an exemption.

3. There are no quick and easy answers to reconcile the physical laptop inventory with the encryption process. They use different identifiers, the encryption software has no centralized management features and the asset tracking system is obsolete. Matching the two up is labor intensive and prone to error. As part of a longer term solution, the OCIO will begin using a common identifier when deploying laptops. In addition, ensuring laptops are encrypted will be part of the written procedures. Finally, a new automated asset management system should make it easier to determine if a laptop is encrypted.

4. Completed with the exception of the 18 settings that were reported to OMB.

5. The OCIO will work with the Agency's DAEO to obtain training in the areas of government property management and dealing with outside sources for all areas of the OCIO.

6. The OCIO will ensure that Customer Support receives A-123 and asset management training in the future.

Cc: The Board
General Counsel
Director of Administration