July 9, 2008

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Protection of Sensitive Equipment at Selected Postal Service Information Technology Facilities (Report Number IS-AR-08-013)

This report presents the results of our audit of sensitive equipment at selected information technology (IT) facilities (Project Number 07BD001IS003). Our objective was to determine whether controls were in place to ensure the Postal Service adequately protected information technology equipment from accidental or intentional loss or damage. Specifically, we reviewed the inventories for laptop and BlackBerry® devices assigned to employees and contractors at six IT facilities to determine if accountability controls adequately protected this equipment and any data stored on these devices. We performed this review as part of the fiscal year (FY) 2007 information systems audit of general controls at the Postal Service's Information Technology and Accounting Service Centers (IT/ASCs). Click here to go to Appendix A for additional information about this audit.

Conclusion

In most locations tested, the Postal Service had effective controls in place to ensure their sensitive information technology physical resources were adequately protected from accidental or intentional loss or damage. Specifically, we found controls were in place for tracking inventories of sensitive computer equipment at five of the six sites visited. However, management could strengthen accountability controls by ensuring they make inventory staff aware of and follow all steps related to safeguarding the inventory of information technology assets and any data stored on those devices from accidental or intentional loss or damage. In addition, management could improve the data integrity in the [redacted] by periodically reconciling the data.

Laptop Computer Inventories

Out of our audit sample of 235 devices, we could not locate 30[1] of 107 laptops from headquarters,[2] thus, we projected an inability to locate 836 of 2,982 laptops from the headquarters offices. Additionally, we were unable to locate three of 54 laptops from the [redacted] Information Technology Service Center (ITSC) and one laptop of 11 from the [redacted] IT/ASC. At the three remaining IT facilities, we located all laptops identified in our sample. This occurred because inventory staff[3] did not always follow, or were not aware of, policies,[4] procedures,[5] and processes for documenting and certifying inventory results and recording the information in [redacted].

We quantified the risk associated with 836[6] missing headquarters laptops and the potentially compromised laptop data. The total projected estimate associated with these laptops was $1,901,900. We based this figure [redacted][7]. Additionally, we used a conservative estimate of 10 records on each laptop and the associated cost of a potential data breach at $83 per record to calculate a potential cost of data disclosure of $693,880. (Click here to go to Appendix C for details of the calculation.) These laptops and potential data disclosure could affect customer trust in the Postal Service brand. We will report $1,901,900 of non-monetary impact for physical assets at risk, safeguarding data, and goodwill branding in our *Semiannual Report to Congress.* Click here to go to Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the managers at the [redacted] Information Technology facilities; and the Headquarters Computing Infrastructure Services to:

1. Ensure Material Accountability Officers and Assistants are aware of and follow all policies and procedures for inventory control of sensitive equipment including report certification by their functional managers.

---

[1] We completed our inventory work as of July 5, 2007, and 40 laptops were not located. Since that time, headquarters staff performed additional research and as of June 10, 2008, located 10 of the laptops.
[2] The headquarters category within the [redacted] includes the offices located at L'Enfant Plaza, the William F. Bolger Center for Leadership Development located in Potomac, Maryland, offices located in Merrifield and Arlington, Virginia, and headquarters staff located at field sites across the nation serving in a headquarters-related job function.
[3] Postal Service policy gives primary responsibility of physical inventory and reconciliation of sensitive property records to the Material Accountability Officer and optional Material Accountability Assistant.
[4] Handbook AS-701, *Material Management*, June 2005 (updated with *Postal Bulletin* revisions through November 9, 2006), Chapter 5 – Asset Accountability and Chapter 6 – Asset Recovery, Redistribution, Recycling, and Disposal; Handbook AS-805, *Information Security*, March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006), Chapter 7 – Physical and Environmental Security.
[5] *IT Facilities Inventory Processes & Procedures Document*, Version 9, December 4, 2006.
[6] We did not include the four laptops we could not locate at the other IT locations in our projections because they were not statistically significant.
[7] [redacted]

BlackBerry Device Inventories

We sampled 208 of 1,909 BlackBerry devices assigned to employees and contractors at the six IT facilities. We located all BlackBerry devices in our sample, verifying that the Postal Service had effective controls in place to ensure management adequately protected BlackBerry devices from accidental or intentional loss or damage.

[redacted] did not always reflect the current custodian, location, or status of the Postal Service's sensitive laptop and BlackBerry device inventory. From a random sample of these sensitive equipment records, we projected that 24 percent of the laptop and almost 40 percent of the BlackBerry device records would contain at least one discrepancy.[8] Although mandated by Postal Service policies[9] and procedures,[10] some inventory staff did not reconcile the physical inventories with [redacted]. Additionally, the automated interface between the databases feeding laptop and BlackBerry device data to [redacted] has transmitted incorrect historical data. During our search for these devices, we identified cases where one or more of the 19 databases feeding [redacted] contributed to perpetuated data record errors and, in at least one instance, a manual override could not correct the error. An accurate [redacted] inventory helps ensure the ability to locate all sensitive laptop and BlackBerry equipment. Click here to go to Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the managers at the [redacted] information technology facilities; and the Headquarters Computing Infrastructure Services to:

2. Conduct quarterly comprehensive reconciliations of the [redacted] to resolve discrepancies for sensitive equipment.

3. Develop a procedure to require individuals to semiannually validate and report inventory results for laptops, BlackBerry devices, or other sensitive equipment in their possession.

4. Establish a plan with milestones to correct data interface issues to promote data accuracy in the [redacted].

[8] We classified a record as a discrepancy when the actual custodian, equipment status (active vs. retired), or location differed from the data element recorded in the [redacted].
[9] See footnote 4.
[10] See footnote 5.

Management's Comments

Management agreed with all four recommendations. Regarding recommendation 1, management stated Information Technology (IT) facility managers will review applicable policies with responsible personnel each year. The managers will emphasize that the actual custodian, equipment status, and equipment location must be accurate for sensitive equipment. At individual facilities, responsible personnel will provide signed verification that they reviewed, understood, and will comply with applicable policies. In addition, each IT facility will audit a sampling of both the quarterly sensitive reconciliation and semiannual individual sensitive equipment validation performed by the responsible personnel to ensure compliance with applicable policies. Each IT facility manager will provide report certification that the audit samples reviewed are in compliance. Management will complete their corrective action by August 29, 2008.

For recommendation 2, management stated all IT facilities would conduct quarterly reconciliations with [redacted] starting by December 31, 2008, to resolve discrepancies for sensitive equipment allocated to employees. Each quarterly review will include an audited sample and the facility manager will certify that samples comply with procedures.

In conjunction with recommendation 3, management will develop a process by September 30, 2008, to require individuals to semiannually validate and report sensitive equipment in their possession. They will complete the initial semiannual validation by March 31, 2009. Management also stated that they have controls in place for assignment of sensitive equipment and they plan to implement encryption on 4,600 laptops by the end of this fiscal year.

Regarding recommendation 4, management stated that enhanced tracking procedures are in place to verify receipt of shipped equipment, report new equipment installations in a weekly status report to upper management, and ensure the equipment remains active on the network. Management stated that implementing recommendations 1-3 would correct the manual or automated feeds causing some situations of incorrect data within the [redacted]. They also stated that responsible personnel will correct equipment status information and ensure they enter cancellation requests into [redacted] for equipment no longer needed. Finally, management will review current data feeds to the [redacted] and correct data interface issues by June 30, 2009.

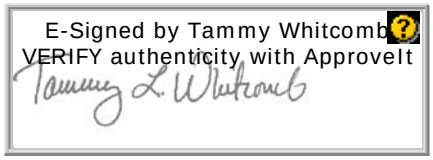
We received additional information subsequent to the receipt of written comments. Management provided a list of milestones and related completion dates and informed us that they planned to complete all activities by June 30, 2009, rather than September 30, 2009, as originally reported. They also stated that they agreed with the non-monetary impact described in the report. Click here to go to Appendix D to view management's comments.

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations, and their corrective actions should resolve the issues identified in the report.

The OIG considers recommendation 1 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. This recommendation should not be closed in the follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Gary C. Rippie, Director, Information Systems, or me at (703) 248-2100.



Tammy L. Whitcomb
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Ross Philo
Harold E. Stark
Deborah J. Judy
John P. Byrne
Joseph G. Gabris
Michael E Goldman
Terrance P. Moran
G. Dean Larrabee
Emily M. Andrew
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The [redacted] is the official central repository for tracking all IT assets. The system automates the collection of data about most IT assets such as workstations, laptops, and servers. [redacted] allows users to query the asset database using a variety of search methods to review, analyze, and maintain networked and non-networked asset inventory, as their assigned authority level allows. The major ongoing tasks of [redacted] are to:

- Provide a common, web-accessible view of all computing devices in the Postal Service.
- Ensure management, data owners, and device owners have the necessary information to make informed decisions.
- Ensure the consolidated information can interface with other systems, reducing data redundancy.
- Continue to develop methods to ensure data accuracy.
- Continue to discover data sources that will give a broader picture of the Postal Computing Environment.

[redacted] categorizes both headquarters and headquarters-related offices in the Washington, D.C. metropolitan area as “headquarters” for generating reports. Reports generated for this category include inventory for offices located at L’Enfant Plaza, the Virginia offices of Merrifield and Arlington, and the William F. Bolger Center for Leadership Development in Potomac, Maryland. Additionally, reports include inventory for Postal Service staff assigned to headquarters-related job functions at numerous field sites across the nation.

[redacted] receives automated data feeds from 19 databases and a number of manual sources to assist in maintaining an accurate inventory of workstation and portable equipment, including laptop computers and BlackBerry devices. The chart below depicts those automated and manual sources.

Redacted

Redacted

In July 2006, the Postal Service began an initiative in response to a presidential directive to improve data security related to breaches of sensitive information. To support this effort, the IT Corporate Information Security Office (CISO) and the Privacy Office jointly developed user procedures for reporting equipment loss and security breaches of Postal Service computing equipment, including laptop computers, BlackBerry devices, and other portable equipment. The Privacy Office included factual case studies in its online privacy training program, focusing on specific principles and a variety of data breaches that impacted well-known companies. Both organizations also issued a series of online articles in the USPS News Link beginning in April 2007, emphasizing mobile device security, including encrypting sensitive data. Additionally, the CISO placed a policy on its new IT website[11] requiring that all laptops implement hard disk encryption.

After completion of our fieldwork, the reporting structure changed for Information Technology. Previously, Information Technology reported to the Vice President, Chief Technology Officer, who reported to Executive Vice President, Chief Financial Officer. As of February 25, 2008, Information Technology now reports through the Executive Vice President, Chief Information Officer, to the Postmaster General.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether controls were in place to ensure the Postal Service adequately protected sensitive Postal Service information technology equipment from accidental or intentional loss or damage. Specifically, we reviewed the inventories for laptop and BlackBerry devices assigned to employees and contractors at six IT facilities to determine if accountability controls adequately protected this equipment and any data stored on these devices. We performed this review as part of the FY 2007 information systems audit of general controls at the Postal Service's IT/ASCs.

We limited the scope of our review to a stratified sample of laptops and BlackBerry devices identified in [redacted] as located at the [redacted] IT/ASCs; the ITSC in [redacted]; Postal Service Headquarters in Washington, D.C.; and the Integrated Business Systems Service Center in [redacted].

To meet our objective, we obtained inventory data for laptops and BlackBerry devices from the [redacted] database for the sites in our sample. We used the "Custom Query" report in [redacted] to identify the universe of laptops and BlackBerry devices. We used manual and automated techniques to separate the laptop records from the other types of computer equipment records. We worked with inventory support staff for [redacted] at the [redacted] ITSC to confirm that we had properly selected [redacted] records for sampling. We also interviewed inventory staff to determine the process they used to address

[11] [redacted].

damaged laptops. Specifically, we drew a statistically valid stratified random sample for each location. The audit universe consisted of 4,139 laptops and 1,909 BlackBerry devices assigned to the headquarters, [redacted] IT facilities. The audit team obtained the universe information from the January 2007 [redacted] database.

Using the sample results, we projected the number of laptops that could not be located and the number of laptop and BlackBerry devices that were located but had discrepancies associated with the [redacted] record. We classified a record as a discrepancy when the actual custodian, equipment status (active versus retired), or location differed from the data element recorded in [redacted]. Additionally, we reviewed documents regarding physical security policies and practices and interviewed key Postal Service managers about current inventory practices.

We conducted this performance audit from January through September 2007 and March through July 2008[12] in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Even though some data in our sample records were incomplete or inaccurate, [redacted] is the only comprehensive database available for the IT facilities that we visited; therefore, we found this system sufficiently reliable for selecting our samples. We discussed our observations and conclusions with management officials during the audit and on June 5, 2008, and included their comments where appropriate.

PRIOR AUDIT COVERAGE

In July 2005, the U.S. Postal Service Office of Inspector General reported[13] two issues related to managing sensitive equipment. The [redacted] IT/ASCs relied on local procedures to manage capital and sensitive equipment, which were inconsistent with corporate-wide policy. Additionally, some capital and sensitive equipment either could not be located, had been moved, or was improperly documented in the locally managed equipment databases. We recommended that managers at the [redacted] data centers complete local implementation of [redacted] within 90 days of report issuance. Management agreed with the recommendation and implemented [redacted] at all three sites in December 2005.

[12] We did not work on this audit from October 2007 through February 2008 due to the unavailability of resources.
[13] *Physical Security Controls at the* [redacted] *Information Technology and Accounting Service Centers* (Report Number IS-AR-05-012, dated July 26, 2005).

APPENDIX B: DETAILED ANALYSIS

Laptop Computer Inventories

Based on a random sample of laptop computer records from [redacted], we could not locate 30 laptops[14] from headquarters, three from the [redacted] ITSC, and one from the [redacted] IT/ASC. Using these tests, we calculated the overall results displayed in Table 1. Based on our sampling, we projected an inability to locate 836 laptops from the headquarters offices. Using a replacement cost of [redacted][15] for physical assets at risk. Additionally, the non-monetary impact associated with cost of a potential data breach conservatively computed to $693,880 for the 836 laptops. Click here to go to Appendix C for details of our calculation for the non-monetary impact associated with potential data breaches.

Table 1: Results of Laptop Equipment Inventory Review

Location	Universe	Statistical Sample Size	Items Not Found	Projected Items Not Found	Percent of Not Found
Headquarters	2,982	107	30	836	28.0
All Other Sites	1,157	128	4(1)	36	3.1(1)
Total	4,139	235	34	872	21.1(2)

[1] The four laptops we could not locate at the other IT facilities were not statistically significant.
[2] We based the totals for projected items not found and percent not found on the overall point estimate of the statistical sample.

Inventory staff[16] at five of the six IT facilities all confirmed they were using a common set of procedures,[17] which included using PS Form 7340-B, Property Transfer Request Worksheet; PS Form 2880, Physical Inventory Certification/Adjustments; and PS Form 969, Material Recycling and Disposal, for managing inventory for sensitive equipment.

This situation occurred at headquarters because inventory staff did not always follow, or were not always aware of, policies,[18] procedures,[19] and processes for accurately recording key data such as custodian and location; sending or retaining documentation regarding disposal of computer laptops; and reconciling the results of the physical inventories of laptop equipment with [redacted]. Additionally, the functional manager in charge of the inventory staff had not certified the correctness of inventories performed.

During the review, we also confirmed the Postal Service did not have an enterprise-wide solution implemented to encrypt laptop computers during our audit fieldwork period of January through September 2007. Therefore, there is a potential that sensitive data contained on laptops we could not locate is vulnerable to data breach.

[14] We attempted to identify the job functions of the last known custodians for the laptops we could not locate. These included managers, miscellaneous staff positions, and several individuals who are no longer with the Postal Service.
[15] [redacted]
[16] See footnote 3.
[17] See footnote 5.
[18] See footnote 4.
[19] See footnote 5.

Corrective Actions Taken

Management has begun a project designed to enhance laptop accountability. The Laptop/Mobile Media Project:[20]

- Requires the employee to complete a handwritten PS Form 1357-D, Data Accountability, and include serial number, make or model, and manufacturer.
- Requires an Executive Administrative Service or Postal Career Executive Service manager's signature.
- Makes the employee personally responsible for the equipment and acknowledges the employee will abide by security practices, including travel procedures, using encryption technology and procedures to report lost or stolen equipment.
- Requires the employee to request access in the [redacted] test environment, including a step where the user uploads an automated copy of the signed document.

Additionally, Corporate IT began implementing their encryption program, which will mitigate the risk associated with sensitive data stored on equipment. They will transmit encryption software directly to compatible laptops using the Systems Management Server system. Management plans to implement encryption on approximately 4,600 laptops by the end of the fiscal year.

[redacted]

[redacted] data did not always reflect the current custodian, location, or status of the Postal Service's sensitive laptop and BlackBerry device inventory. From a random sample of laptops and BlackBerry devices, we projected that 24 percent of the laptop and 40 percent of the BlackBerry records would contain at least one discrepancy.[21] We listed overall results in the tables below. We also projected that 20.6 percent of the laptop and 43.9 percent of the BlackBerry records for headquarters and 32 percent of the laptop and 22.5 percent of the BlackBerry records for all other IT/ASC sites would have at least one discrepancy in [redacted].

As demonstrated in Table 2, based on our projections, 24 percent of the laptop records (984 of 4,139) would contain at least one discrepancy.

[20] The project began April 25, 2008, at headquarters and a limited number of field groups, but management has not established a date when all users will follow these new procedures.
[21] See footnote 8.

Table 2: Results of [redacted] Data Review for Laptops

Location	Universe	Statistical Sample Size	Number of Record Errors	Projected Record Errors	Percentage of Record Errors
Headquarters	2,982	107	22	613	20.6
All Other Sites	1,157	128	41	371	32.0
Total	4,139	235	63	984	23.8[(1)]

[1] We based the totals for projected items not found and percentage of records in error on the overall point estimate of the statistical sample.

As demonstrated in Table 3, based on our projections, almost 40 percent of BlackBerry records (754 of 1,909) would contain at least one discrepancy.

Table 3: Results of [redacted] Data Review for BlackBerry Devices

Location	Universe	Statistical Sample Size	Number of Record Errors	Projected Record Errors	Percentage of Record Errors
Headquarters	1,518	57	25	666	43.9
All Other Sites	391	151	34	88	22.5
Total	1,909	208	59	754	39.5[(1)]

[1] We based the totals for projected items not found and percentage of records in error on the overall point estimate of the statistical sample.

During our search for these devices, we identified cases where one or more of the 19 databases feeding [redacted] contributed to or perpetuated data record errors and, in at least one instance, a manual override could not correct the error. For example, during our review of the sensitive equipment inventory at the [redacted] IT/ASC, neither we nor the inventory staff could locate one laptop. We identified automated and manual feeds that affected data elements of custodian, status, or location.[22] The inventory staff confirmed that all three data elements for the laptop record were incorrect. Since we could not locate the laptop, the inventory staff initiated procedures to submit a "Lost/Theft" report and PS Form 2880, Physical Inventory Certification - Adjustments.

While we confirmed the existence of a collection of headquarters laptops, we had to rely on a fragmented process involving the equipment's "Configuration" and "Last User Logon ID" in [redacted]. With these data elements and a discussion with a network systems analyst, we determined five laptops did not belong to a permanent custodian but to users training at the William F. Bolger Center for Leadership Development. By identifying these laptops as associated with the Bolger Center, it would make future inventory efforts more efficient and alleviate concerns that they were lost or stolen. In another case, we confirmed the existence of a laptop, but only after going through a lengthy process to ascertain that [redacted] had duplicate records for the laptop. We determined that a manual override in [redacted] would not correct the problem until repair

[22] [redacted]

technicians ran a utility disk on the laptop's Basic Input/Output System (BIOS)[23] to recognize a new hard drive they had installed.

Corrective Actions Taken

During our audit, management also made changes to correct problems occurring with two [redacted] interfaces. During February 2008, management completed changes, which corrected a problem with the interface between [redacted] and the PS Form 969, Material Recycling and Disposal, web application (969 system). The migration of the 969 system from older to newer computer equipment caused the interface between the systems to fail. The corrected interface allows the data entered in the 969 system interface to reconcile with [redacted] data. Additionally, from November 19 to December 24, 2007, management reviewed and corrected an automated interface between [redacted] and the BlackBerry Enterprise Server. This effort fixed incorrectly recorded BlackBerry device data in [redacted].

[23] BIOS refers to the firmware code run by an International Business Machines Personal Computer (PC) when first powered on. The primary function of the BIOS is to identify and initiate component hardware (such as hard disk, floppy, and optical disk drives). This is to prepare the machine so other software programs stored on various media can load, execute, and assume control of the PC.

APPENDIX C: ESTIMATED COST OF A SENSITIVE DATA COMPROMISE

The following describes the methodology we used to calculate non-monetary impact for safeguarding assets associated with potential data breaches involving 836 laptops.

We used the Ponemon Institute's November 2007 study[24] as a benchmark to identify the cost of a data breach. The Ponemon Institute classified the total cost of $198 per record using detection and escalation costs of $9, notification costs of $15, ex-post response costs of $46, and lost business costs of $128, as displayed in the table below.

Cost Category	Costs per Record as Reported by Ponemon Institute	Amount Applicable to the Postal Service
Detection and Escalation		
Internal Investigation, Legal, Audit, and Consulting	$9	$9
Notification		
Letters, Emails, Telephone, Published Media, and Website	15	15
Ex-Post Response		
Mail, Email, Telephone (to Internal Call Center), Telephone (to Outsourced Call Center), Legal Defense, Criminal Investigations (forensics), Public or Investor Relations, Free or Discounted Services	46	46
Lost Business		
Cost of Turnover, Cost of Fewer New Customers	128	13[25]
Total	**$198**	**$83**

[redacted] The number of records stored on the seven stolen computers ranged from four to 40,000, so we based our calculation on a conservative 10 records per laptop. We calculated a total non-monetary impact of $693,880 based on $83.00 per record for the projected 836 laptops (10 records each) which we could not locate at the headquarters offices.

[24] Ponemon Institute, LLC, *2007 Annual Study: U.S. Cost of a Data Breach*, dated November 2007, page 9.
[25] The $128 estimated cost per record listed by the Ponemon Institute in the Lost Business category does not represent a reasonable estimate for the Postal Service. We believe Postal Service customers have few alternatives in the market for delivery of letters and packages at comparable, competitive rates so we estimate the actual loss of business would be much less. Therefore, we elected to reduce the lost business estimate of $128 by 90 percent (from $128 to $13).

APPENDIX D. MANAGEMENT'S COMMENTS

GEORGE W. WRIGHT
VICE PRESIDENT
INFORMATION TECHNOLOGY OPERATIONS

UNITED STATES POSTAL SERVICE

July 1, 2008

Lucine Willis
Director, Audit Operations
Office of Inspector General
1735 North Lynn Street
Room 11044
Arlington, VA 22209-2020

SUBJECT: Management Response – Protection of Sensitive Equipment at Selected Postal Service Information Technology Facilities (Report Number IS-AR-08-DRAFT)

We are pleased to provide the attached response to the recommendations described in the subject audit report. We are in agreement with all recommendations of the audit findings.

Corrective actions will be taken to address all requirements as detailed in this audit, which we expect to complete by September 30, 2009.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the United States Postal Service. The Manager of Corporate Information Security will work with you to determine what portions of this report should be considered as classified and restricted, and exempt from disclosure under the Freedom of Information Act (FOIA).

If you have any questions or comments regarding this response please contact Shawn D. Harris at 202-268–6802, CTO Audit Response Management.

George W. Wright

cc: Ross Philo
Joseph J. Gabris
John T. Edgar
Tim W. Knox
G. Dean Larrabee
Cliff M. Biram
Gregory G. Wallace
Kathleen A. Warnaar
Katherine S. Banks
audittracking@uspsoig.gov

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-2764
FAX 202-268-4492
GEORGE.W.WRIGHT@USPS.GOV
WWW.USPS.COM

Protection of Sensitive Equipment at Selected Postal Service Information Technology Facilities (Report Number IS-AR-08-DRAFT, dated June 16, 2008)

We recommend the Vice President, Information Technology Operations, direct the managers at [redacted] Infrastructure Services to:

Recommendation 1: Ensure Material Accountability Officers and Assistants are aware of and follow all policies and procedures for inventory control of sensitive equipment including report certification by their functional managers.

Management Response: Management agrees and will take the following corrective actions:

A. Each of the 6 IT Facility Managers (or designee) will hold a review session on a yearly basis with the local Functional Managers, MAOs and MAAs to review: Handbook AS-701, Material Management, June 2005 (updated with Postal Bulletin revisions through November 9, 2006), Chapter 5 – Asset Accountability and Chapter 6 – Asset Recovery, Redistribution, Recycling, and Disposal Handbook AS-805, Information Security, March 2002 (updated with Postal Bulletin revisions through November 23, 2006), Chapter 7 – Physical and Environmental Security IT Facilities Inventory Processes & Procedures Document, Version 9, December 4, 2006 for sensitive equipment in [redacted]
B. In these sessions the IT Facility Managers (or designee) will emphasize that the actual custodian, equipment status (active vs. retired), and equipment location must be accurate for sensitive equipment.
C. Each IT Facility Manager, Functional Manager, MAA, and MAO will provide signed report certification that he or she reviewed, understood, and will comply with the AS-701, AS-805, and IT Facilities Inventory Processes & Procedure Document.
D. Each IT Facility MAO will audit a sampling of each quarterly sensitive reconciliation performed by their MAAs to ensure that the MAAs are in compliance as outlined in Handbook AS-701, Material Management, June 2005 (updated with Postal Bulletin revisions through November 9, 2006), Chapter 5 – Asset Accountability section 541 Assignment of the MAO. Each IT Facility Manager will provide report certification that the audit samples are in compliance.
E. Each IT Facility MAO will audit a sampling of each semiannual individual sensitive equipment validation performed by their MAAs to ensure that the MAAs are in compliance as outlined in Handbook AS-701, Material Management, June 2005 (updated with Postal Bulletin revisions through November 9, 2006), Chapter 5 – Asset Accountability section 541 Assignment of the MAO. Each IT Facility Manager will provide report certification that the audit samples are in compliance as outlined.

Scheduled Completion Date: August 29, 2008

Recommendation 2: Conduct quarterly comprehensive reconciliations of the [redacted] to resolve discrepancies for sensitive equipment.

Management Response: Management agrees. All IT Facilities will conduct quarterly reconciliations with [redacted] to resolve discrepancies for employee allocated equipment identified as sensitive (e.g. BlackBerry and Laptops). Each IT Facility manager, Functional manager, MAA, and MAO will provide signed report certification that he or she complied in accordance with the AS-701, AS-805, and IT Facilities Inventory Processes & Procedure Document as outlined in the USPS Information Technology's response to the OIG Audit recommendation number 1. Each IT Facility MAO will audit a sampling of each quarterly sensitive reconciliation performed by their MAAs to ensure that the MAAs are in compliance as outlined in Handbook AS-701, Material Management, June 2005 (updated with Postal Bulletin revisions through November 9,2006), Chapter 5 – Asset Accountability section 541 Assignment of the MAO. Each IT Facility Manager will provide report certification that the audit samples are in compliance.

Scheduled Completion Date: December 31, 2008

Recommendation 3: Develop a procedure to require individuals to semiannually validate and report inventory results for laptops, BlackBerry devices, or other sensitive equipment in their possession.

Management Response: Management agrees.

A. For existing employee allocated equipment identified as sensitive (e.g. BlackBerry and Laptops), USPS IT will develop a process to require individuals to semiannually validate and report sensitive equipment in their possession [redacted] The initial semiannual execution of the new process with individual validation will be complete by March 31st, 2009. Each IT Facility MAO will audit a sampling of each semiannual individual sensitive equipment validation performed by their MAAs to ensure that the MAAs are in compliance as outlined in Handbook AS-701, Material Management, June 2005 (updated with Postal Bulletin revisions through November 9,2006), Chapter 5 – Asset Accountability section 541 Assignment of the MAO. Each IT Facility Manager will provide report certification that the audit samples are in compliance as outlined.

B. As mentioned on page 9 under the OIG Audit Report Laptop Computer Inventories/Corrective Actions section, the Laptop/Mobile Media Project is underway. Information Technology is also in the process of refreshing laptops via the [redacted] program. [redacted]

[redacted]

As part of the Laptop/Mobile Media Project, Information Technology has begun implementing its encryption program, which will mitigate the risk associated with sensitive data stored on Laptops. Information Technology will transmit encryption software directly to compatible laptops using the Systems Management Server system. Current plans call for implementation of encryption on approximately 4,600 laptops by the end of this fiscal year.

C. A process currently exists for the allocation of BlackBerrys, issued to IT employees. This process involves the use of [redacted] and is documented on the IT Web page.

Scheduled Completion Date: March 31, 2009

Recommendation 4: Establish a plan with milestones to correct data interface issues to promote data accuracy in the [redacted].

Management Response: Management Agrees.

A. During our review of the sensitive equipment inventory at the [redacted] IT/ASC, neither we nor the inventory staff could locate one laptop. We identified automated and manual feeds that affected data elements of custodian, status, or location. Footnote 22: The inventory staff confirmed that all three data elements for the laptop record were incorrect. Footnote 23: Three [redacted]

- OIG Audit Recommendations 1, 2, and 3 will correct this issue. (OIG Audit Report, 2008, p. 2-3). Information on Laptops and Blackberries no longer in use, must be updated by the MAAs in accordance with the USPS Information Technology's response to the OIG Audit recommendation number 1. In addition we have put enhanced tracking procedures in place as part of the [redacted] refresh of hardware to validate that equipment which has been shipped is received at the destination offices, reported in the weekly status report to upper management as having been installed, and monitored continuously to determine that the equipment is still active on the network. Equipment that is being retired also now has multiple check points to validate receipt at the disposal facility and to automatically feed between the [redacted]
- For Laptops, the MAAs must enter the correct status if the equipment is no longer active (e.g. Stored, Retired, and Stolen). MAAs must always update [redacted] with the accurate Custodian/User, Finance # (Office), "Building Name", and "Facility Database ID". If the equipment is lost or stolen, the MAAs must fill out the proper paperwork and update [redacted] with the appropriate information. The [redacted] system will show the last time it received an active feed on this asset until the Laptop information is accurately updated by the MAAs in accordance with the USPS Information Technology's response to the OIG Audit recommendation number 1.
- For Blackberries, the MAAs will ensure that an employee goes into [redacted] and creates a cancellation request if the equipment is no longer needed. The BlackBerry Enterprise Server will provide this updated information to [redacted]

B. "In another case, we confirmed the existence of a laptop, but only after going through a lengthy process to ascertain that [redacted] had duplicate records for the laptop. We determined that a manual override in [redacted] would not correct the problem until repair technicians ran a utility disk on the laptop's Basic Input/Output System (BIOS) to recognize a new hard drive they had installed."

- In some instances HP failed to properly update the device's BIOS with the serial number, make, and model number. In other cases there was a bug in HP's BIOS software. Since HP is unable to locate the devices with this issue, when discovered a technician must locate the device and run a Utility to correct this issue. In [redacted], the BIOS issues are reflected as a serial number with multiple entries or a message that the make/model is broken.

- OIG Audit Recommendations 1, 2, and 3 will assist the MAA and technician with locating the equipment and correcting any [redacted] discrepancy.

C. As noted under the [redacted] Data/Corrective Actions Taken section on page 11, issues were discovered with the BlackBerry Enterprise Server and 969 systems. Both systems were corrected during the audit and this fully addresses the OIG finding. OIG Audit Recommendations 1 and 2 will uncover [redacted] data issues which could immediately be corrected.