



**OFFICE OF  
INSPECTOR GENERAL**  
UNITED STATES POSTAL SERVICE

AUDIT REPORT

# Topeka, KS, Material Distribution Center – Information Technology General Controls

June 11, 2014



Report Number IT-AR-14-006



June 11, 2014

**Topeka, KS, Material Distribution Center –  
Information Technology General Controls**  
Report Number IT-AR-14-006

***BACKGROUND:***

In June 2013, the U.S. Postal Service completed consolidation of all print operations into the National Print Center in the administrative building at the Topeka, KS, Material Distribution Center. As a result of this cost-cutting measure, the National Print Center now processes about 192,000 payroll checks and 107,000 vendor checks per month (totaling about \$468 million), as well as earnings and Express Mail corporate account statements.

In addition to the print operations, the Material Distribution Center's administrative building maintains a computer server room that supports systems that manage vehicles, warehousing, inventory, and equipment.

Our objective was to determine whether general security controls pertaining to physical access, contingency planning, security management, and segregation of duties at the center's administrative building provide reasonable assurance that computer assets, processed payroll data, and vendor data are secure.

***WHAT THE OIG FOUND:***

Contingency planning and segregation of duties were adequate; however, security controls related to physical access and security management were not in place to protect computer assets and data at the center's administrative building. Specifically, management did not conduct physical key reviews or maintain a key inventory as required.

Additionally, management did not use a reliable badge system for accessing the administrative building, monitor personnel access privileges, or put alarms on emergency doors that provide access to computer assets in the building's warehouse area. In addition, management did not have procedures in place for granting and monitoring employee access to the check printing system or provide security training for employees with access to the system.

Management considered the key inventory and alarms on the emergency doors to be low priorities. Also, officials were unaware of procedures related to user access reviews and security training. Not adhering to information security controls increases the risk of unauthorized individuals accessing sensitive information, including employees' names, addresses, and identification numbers.

***WHAT THE OIG RECOMMENDED:***

We recommended management complete a physical key review, rekey certain areas, and better restrict access to the administrative building. Further, we recommended management periodically review employee access to the server room and check printing system. Finally, we recommended management provide information security training to all employees with access to computer assets and data.

[\*Link to review the entire report\*](#)



June 11, 2014

**MEMORANDUM FOR:** JOHN T. EDGAR  
VICE PRESIDENT, INFORMATION TECHNOLOGY

SUSAN M. BROWNELL  
VICE PRESIDENT, SUPPLY MANAGEMENT

A rectangular box containing a handwritten signature in black ink that reads "John E. Cihota". There is a small black dot in the upper right corner of the box.

**FROM:** John E. Cihota  
Deputy Assistant Inspector General  
for Finance and Supply Management

**SUBJECT:** Audit Report – Topeka, KS, Material Distribution  
Center – Information Technology General Controls  
(Report Number IT-AR-14-006)

This report presents the results of our audit of the Topeka, KS, Material Distribution Center's Information Technology General Controls (Project Number 14BG002IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean D. Balduff, acting director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

## TABLE OF CONTENTS

Introduction .....	1
Conclusion .....	1
Physical Security .....	2
Logical Access Security .....	4
Information Security Training .....	4
Recommendations .....	4
Management’s Comments .....	5
Evaluation of Management’s Comments.....	6
Appendix A: Additional Information .....	7
Background .....	7
Objective, Scope, and Methodology .....	7
Prior Audit Coverage .....	8
Appendix B: Management's Comments .....	9

## Introduction

This report presents the results of our self-initiated audit of the Topeka, KS, Material Distribution Center (MDC) – Information Technology (IT) General Controls (Project Number 14BG002IT000). Our objective was to determine whether general controls pertaining to physical access, security management, contingency planning, and segregation of duties at the MDC’s administrative building<sup>1</sup> provide reasonable assurance that computer assets<sup>2</sup> and processed payroll and vendor data are secure. See [Appendix A](#) for additional information about this audit.

The Topeka MDC provides parts, equipment, and supplies to all U.S. Postal Service facilities. In 1975, the Postal Service added the Label Printing Center (LPC) to the Topeka MDC and, in June 2013, changed the name from the LPC to the NPC to reflect the consolidation of all print operations into the new center. The NPC now carries out all print functions, such as processing payroll and vendor checks, earning statements, and Express Mail corporate account (EMCA) statements using the Ricoh Process Director (RPD or check printing) system.<sup>3</sup> The 35 employees working at the NPC process about 192,000 payroll checks and 107,000 vendor checks per month, totaling about \$468 million.

In addition to print operations, the MDC’s administrative building maintains a computer server room that supports the Material Distribution and Inventory Management System (MDIMS)<sup>4</sup> and the Solution for Enterprise Asset Management (SEAM).<sup>5</sup>

The U.S. Postal Inspection Service performs site reviews to address physical security controls at Postal Service facilities. The Postal Inspection Service last reviewed security controls at the Topeka MDC in March 2012.

## Conclusion

Contingency planning and segregation of duties were adequate; however, security controls related to physical access and security management were not in place to protect computer assets and data at the MDC’s administrative building. Specifically, management did not conduct physical key reviews or maintain a key inventory as required. Additionally, management did not use a reliable badge system for accessing the administrative building, monitor personnel access privileges, or put alarms on

---

<sup>1</sup> The administrative building contains the administrative offices, the National Print Center (NPC), and the center’s computer server room.

<sup>2</sup> Computer assets include desktop and laptop computers, printers, and servers.

<sup>3</sup> The RPD system automates the printing function for multiple types of documents such as employee and vendor checks, employee earning statements, and EMCA statements.

<sup>4</sup> MDIMS is used to perform material distribution, warehousing, and inventory management business functions for the Postal Service. MDIMS helps manage inventory for a catalog of items and provides material support for customers.

<sup>5</sup> SEAM provides inventory management and supply chain planning, and manages and services installed equipment and deployed vehicles.

emergency doors that provide access to computer assets in the building's warehouse area.

Management officials did not take these security precautions because they considered conducting the physical key inventory and installing alarms on the emergency doors to be low priorities. Further, management officials were unaware of specific procedures related to user access reviews and security training. Not adhering to information security controls increases the risk unauthorized individuals will access Postal Service IT assets and information, including employees' names, addresses, and identification numbers.

## Physical Security

We identified the following areas where physical access controls were not established or were not functioning as intended:

- Management had no record of conducting a physical key review and did not maintain a current physical key inventory. Instead, management kept all of the spare building keys in a coffee can and a plastic tub. This occurred because management considered conducting the physical key inventory to be a low priority. Postal Service policy<sup>6</sup> requires management to conduct a semiannual review of all physical keys and maintain an accurate inventory. During our audit, we observed management initiating the process to identify and account for the center's spare keys.
- Management uses an obsolete and unreliable badge system to restrict physical access to the facility, including areas where computer assets are stored. Specifically:
  - The badge system is running on a computer using an operating system the vendor no longer supports. In addition, management could not find new parts for the system when repairs were needed and purchased used replacement parts from eBay.
  - Periodically, management relies on a spreadsheet to verify access lists because accounts were lost during a power interruption.

Budget constraints prevented management from updating or replacing the current badge system and managers did not document their acceptance of risk for using an outdated access system.

- Management did not review the access control list for individuals with physical access to the computer server room, as required. The current IT manager was

---

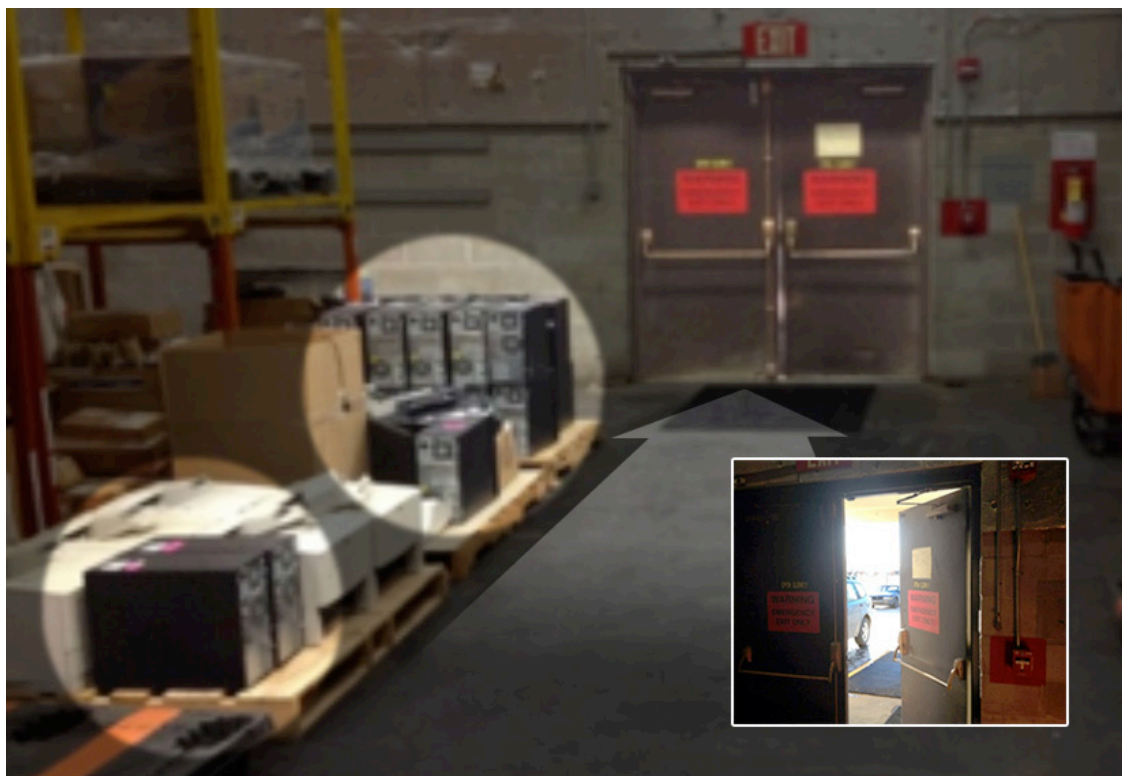
<sup>6</sup> *Administrative Support Manual 13*, Section 273.461, Key and Access Control Device Accountability, and Section 464, Key Survey, updated November 28, 2013.



unaware that Postal Service policy<sup>7</sup> requires designated IT managers to review access control lists quarterly.

- Management did not install alarms on three emergency exit doors that provide access to those administrative building warehouse areas containing IT assets. Figure 1 shows computers and printers near emergency exit doors that lead to a public parking lot. Management did not think this represented an immediate threat or vulnerability. Postal Service policy<sup>8</sup> states that it must protect its information resources<sup>9</sup> against damage, unauthorized access, and theft in the Postal Service environment. During our audit, management placed an order for new alarm systems and installed them on the emergency doors on January 16, 2014; therefore, we are not making a recommendation related to this issue.

**Figure 1. IT Assets at Risk**



Source: U.S. Postal Service Office of Inspector General (OIG) photographs taken December 17, 2013.

The Postal Inspection Service also identified these physical security issues during a March 2012 site review. When management officials do not adhere to physical access control policies, there is an increased risk that unauthorized individuals may obtain access to Postal Service assets.

<sup>7</sup> Handbook AS-805, *Information Security*, Section 7-2.4, Establishment of Access Control Lists, dated March 2014.

<sup>8</sup> Handbook AS-805, Section 7-3, Physical Protection of Information Resources.

<sup>9</sup> Information resources are all Postal Service information assets, including information systems, hardware, software, data, applications, telecommunications networks, computer-controlled mail processing equipment, and related resources and the information they contain.

## Logical Access Security

Management did not periodically review user access to the RPD system. The RPD system is not part of the eAccess System;<sup>10</sup> therefore, managers did not receive notification to perform the periodic access review. Postal Service policy<sup>11</sup> states that managers must review access granted to personnel under their supervision to ensure they still need the access to perform their duties. When there is no formal process for reviewing user access to Postal Service systems, there is an increased risk that unauthorized individuals may have access to sensitive information, such as an employee's name, address, and identification number.

During our audit, management began reviewing user access by taking steps to add the RPD system to the eAccess system. We reviewed the RPD user list on February 12, 2014, and determined management removed 26 inactive accounts.

## Information Security Training

Management did not always provide information security training to employees with access to sensitive Postal Service information resources. Specifically, none of the nine employees with "operator"<sup>12</sup> access to the RPD system received information security training because the MDC manager thought only managers needed this training. Postal Service policy<sup>13</sup> states that all personnel with access to Postal Service information resources must participate in annual information security training. Users who do not receive this training may not be aware of their responsibilities or the actions they can take to protect the Postal Service's information.

## Recommendations

We recommend the vice president, Supply Management, direct the manager, Operating Asset Fulfillment, to:

1. Perform a physical key review and maintain an accurate key inventory for the Topeka Material Distribution Center's administrative building.
2. Rekey doors to those areas in the Material Distribution Center's administrative building with keys that are unaccounted for based on the physical key review.
3. Develop an action plan to update the badge access system or other reliable compensating controls to restrict access to the Material Distribution Center's administrative building.

---

<sup>10</sup> The system is used to request and approve access to Postal Service applications.

<sup>11</sup> Handbook AS-805, Section 9-3.2.5, Periodic Review of Access Authorization.

<sup>12</sup> Operator access allows a person to perform certain functions such as enabling, disabling, and changing computer job scheduling properties.

<sup>13</sup> Handbook AS-805, Section 6-5.3, Training Requirements – Annual Training.



4. Develop a process to ensure required user access to the Ricoh Process Director application is periodically validated and documented.
5. Provide information security training annually to all personnel with access to Postal Service information resources at the Topeka Material Distribution Center's administrative building.

We recommend the vice president, Information Technology, direct the manager, Systems Solutions, to:

6. Perform quarterly reviews of individuals with access to the Topeka Material Distribution Center's computer server room.

### **Management's Comments**

Management agreed with the findings and with recommendations 1 through 4 and 6, and partially agreed with recommendation 5.

In response to recommendation 1, management performed a complete physical key review and inventoried, documented, and secured all excess keys. Management plans to continue periodic physical key reviews.

In response to recommendation 2, management rekeyed all required doors in the administrative area of the MDC.

In response to recommendation 3, management completed a risk assessment of the badge access system with the assistance of the Postal Inspection Service. The assessment concluded the badge access system was functioning but a reassessment will be needed if system replacement parts become unavailable. Management instituted compensating controls to restrict access to the MDC's administrative building.

In response to recommendation 4, management added the RPD to the Postal Service's eAccess System. Employees are required to request and receive approval to use this system and it provides for periodic reviews to validate the need for access.

In response to recommendation 5, management stated that information security training is not available for bargaining unit employees but agreed non-bargaining employees should be trained; therefore, management will issue a communication to all non-bargaining employees at the Topeka MDC to complete annual security awareness training by July 31, 2014.

In response to recommendation 6, management reviewed the records of individuals with access to the Topeka MDC's computer room in conjunction with the compensating controls instituted in recommendation 3. Management will continue these reviews quarterly.

See [Appendix B](#) for management's comments, in their entirety.

### **Evaluation of Management's Comments**

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report. The OIG considers recommendation 3 significant. Since we concur with the actions taken, recommendation 3 can be closed in the Postal Service's follow-up tracking system with the issuance of this report.

## Appendix A: Additional Information

### Background

The Topeka MDC provides parts, equipment, and supplies support to all Postal Service facilities, including facilities in Hawaii, the Caribbean Islands, and Alaska. The MDC's mission is to warehouse and distribute repair parts and supplies in an accurate, responsive, cost-effective, and consistent manner. The warehouse facility contains about 950,000 square feet of floor space that accommodates 26,000 items.

In June 2013, the Postal Service completed the final stage of a three-phase project to reduce its printing costs. As a result, the Postal Service changed the LPC's<sup>14</sup> name to the NPC to reflect the consolidation of all print operations into the new center. The NPC also maintains the RPD system used to print jobs from the mainframe. RPD automates the printing function for payroll, vendor payments, and employee earning statements.

### Objective, Scope, and Methodology

Our objective was to determine whether general controls pertaining to physical access, security management, contingency planning, and segregation of duties at the Topeka MDC's administrative building provide reasonable assurance that computer assets and processed payroll and vendor data are secure.

To meet our objective, we reviewed relevant security policies and procedures and interviewed Postal Service management and other IT staff as necessary. We obtained and reviewed documents related to the controls listed above and observed operations at the facility. In addition, we observed and evaluated physical security controls at the facility.

We conducted this performance audit from November 2013 through June 2014, 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 13, 2014, and included their comments where appropriate.

We did not assess the reliability of any computer-processed data for the purposes of this report. The computer-processed data analyzed during the audit provided the context for the environment audited and did not significantly affect the findings, conclusion, or recommendations in this report.

---

<sup>14</sup> In support of mail processing automation initiatives for postal and mailer operations, the Postal Service formed the LPC in 1975. It consolidated six printing centers across the U.S.

### Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this audit.

## Appendix B: Management's Comments



June 3, 2014

JUDITH LEONHARDT

SUBJECT: Response to Draft Topeka, KS, Material Distribution Center – Information Technology General Controls Report (Report Number IT-AR-14-DRAFT)

Thank you for providing the Postal Service with the opportunity to review and comment on the subject draft report. Management is in agreement with the Office of Inspector General's (OIG) findings and recommendations associated with this report and have implemented several corrective actions.

OIG Audit Recommendations:

We recommend the vice president, Supply Management, direct the manager, Operating Asset Fulfillment, to:

Recommendation 1: Perform a physical key review and maintain an accurate key inventory for the Topeka Material Distribution Center administrative building.

Management Response: Management agrees and has implemented a comprehensive process to account for all facility keys. A physical key review was performed by the Maintenance Control Clerk for the Material Distribution Center resulting in updated individual key record forms (Postal Service Form 1628) for every employee that is issued a key in the facility. These reviews will continue to be performed on an annual basis. Additionally, the Maintenance Control Clerk inventoried all excess keys and maintains a spreadsheet identifying them. The excess keys are currently stored within a secured cabinet with limited access by maintenance personnel who are required to sign a log when removing and returning keys. The key cabinet will be audited on a quarterly basis by the Maintenance Control Clerk.

Target Implementation Date: Completed May 20, 2014.

Responsible Manager: Manager, Operating Asset Fulfillment.

Recommendation 2: Rekey doors to those areas in the Material Distribution Center's administrative building with keys that are unaccounted for based on the physical key review.

Management Response: Management agrees. On May 20, 2014 the maintenance department completed a rekeying of all the doors in the administrative area that are required to be secured.

Target Implementation Date: Completed May 20, 2014

Responsible Manager: Manager, Operating Asset Fulfillment.

Recommendation 3: Develop an action plan to update the badge access system or other reliable compensating controls to restrict access to the Material Distribution Center's administrative building.

Management Response: Management agrees. The Postal Service Inspection Service completed a Tier 1 - Vulnerability Risk Assessment inspection of the badge access system on May 27, 2014. A discussion was held with the inspector regarding the adequacy of the current system and the potential for upgrading the system. The Inspector found that the current system was functioning properly and as long as replacement parts are still available an upgrade would not be necessary. Currently, the Manager, Plant Maintenance is able to buy replacement parts to keep the system operational, but will validate any end of life issues that would require replacement of the controller boards or operating system. Based upon these actions and especially with the Postal Service's financial condition, it has been determined that an upgrade to the badge access system is not beneficial at this time. This action will be revisited should replacement parts become unavailable.

Compensating controls to restrict access to the Material Distribution Center's administrative building have been implemented. A new employee's manager must submit an access card request to the administrative assistant. The administrative assistant will send the request to the Manager, Asset Management Operations for approval to the door access requested by the employee's manager. If access is granted the approval is sent to the Manager, Plant Maintenance for processing. Additionally, the Manager, Plant Maintenance has implemented a process to send specific managers (e.g., Manager, Information Technology and Manager, National Print Center) information on current employee access for review and approval. An access list for all external doors and the gate will be sent to the Manager, Asset Management Operations by the Manager, Plant Maintenance for review and approval on an annual basis. These reviews were completed May 15, 2014.

Target Implementation Date: Completed May 30, 2014.

Responsible Manager: Manager, Operating Asset Fulfillment.

Recommendation 4: Develop a process to ensure required user access to the Ricoh Process Director application is periodically validated and documented.

Management Response: Management agrees. The Ricoh Print Processing Director has been added to the Postal Service's eAccess system which requires employees to request and receive managerial approval to use a system and provides for periodic reviews to validate the need for the employees continued access to a system. Approval of eAccess requests to Ricoh Print Processing Director is assigned to the Manager, National Print Center.

Target Implementation Date: Completed May 15, 2014.

Responsible Manager: Manager, Operating Asset Fulfillment.

Recommendation 5: Provide information security training annually to all personnel with access to Postal Service information resources at the Topeka Material Distribution Center's administrative building.

Management Response: Management agrees in part. The annual security training is driven by requirements defined by the Corporate Information Security Officer (CISO) at the beginning of the fiscal year. Designated personnel, as outlined on the Security Training Matrix located on the CISO internal website, with access to the various Postal Service information data and resources must participate in information security training and data protection requirement training as indicated. Information security is recommended for all other personnel<sup>1</sup>. However, this training is not available for Bargaining Unit personnel which consist of approximately 125 employees at the Topeka Material Distribution Center. Therefore, we agree in part that annual security training will be required for the Non-Bargaining employees only at the Topeka Material Distribution Center and will issue a communication to inform them of this requirement.

<sup>1</sup> Handbook AS-805, Chapter 6, Section 6-5.3, Exhibit 6-5.3, Annual Training



Target Implementation Date: July 2014.

Responsible Manager: Manager, Operating Asset Fulfillment and Supply Management Infrastructure.

We recommend the vice president, Information Technology, direct the manager, Systems Solutions, to:


Recommendation 6: Perform quarterly reviews of individuals with access to the Topeka Material Distribution Center's computer server room.


Management Response: Management agrees and will perform the quarterly reviews in conjunction with the process implemented within recommendation 3 above. The Manager, Enterprise Resource Planning Systems Solutions in Topeka has developed a plan with the Material Distribution Center's Manager, Plant Maintenance to perform the quarterly review. The building equipment maintenance technician sends all the employees who have access to the server to the Manager, Plant Maintenance. The Manager, Plant Maintenance coordinates with the Manager, Enterprise Resource Planning System Solutions on any deletions or additions required to the access control system for the computer server room.

Target Implementation Date: Completed May 15, 2014.

Responsible Manager: Manager, Enterprise Resource Planning Systems Solutions.

This report and management's response does not contain proprietary or sensitive business information that may be exempt from disclosure pursuant to the Freedom of Information Act. If you have any questions about this response, please contact Susan Witt at (202) 268-4833.

  
Susan M. Brownell  
Vice President, Supply Management

  
cc: John T. Edgar  
Vice President, Information Technology

cc: Corporate Audit Response Management