Office of Inspector General | United States Postal Service

Audit Report

Western Area Physical Security and Environmental Controls

Report Number IT-AR-18-002 | March 19, 2018

Table of Contents

Highlights

Objective

Our objective was to determine whether the U.S. Postal Service has implemented effective physical security and environmental and wireless access controls according to policy and industry best practices at the [redacted] Processing & Distribution Center (P&DC).

The Postal Service has the mail processing resources, information technology (IT) network, and transportation infrastructure necessary to deliver mail to every residential and business address in the country. These resources include facilities, equipment, and systems that allow processing, transfer, and storage of data vital for business operations. The Postal Service implements physical and environmental security controls to reduce the risk of system and equipment failure, damage from environmental hazards, and unauthorized access to its facilities and assets.

> *"The Postal Service implements physical and environmental security controls to reduce the risk of system and equipment failure, damage from environmental hazards, and unauthorized access to its facilities and assets."*

The [redacted] P&DC is 630,806 square feet and processes about 475 million mail pieces annually. The facility also includes a retail store, business mail entry unit (BMEU), and administrative offices. We selected this site based on Postal Service and OIG facility risk assessments.

What the OIG Found

We did not identify any wireless issues at the [redacted] Processing & Distribution Center; however, the Postal Service did not implement effective physical security and environmental controls. During our site visit in October 2017, we noted the following:

- Excessive access to IT assets and controlled areas. For example, [redacted] of individuals had access to the [redacted] and [redacted] to the [redacted].
- [redacted]
- [redacted]
- [redacted]
- [redacted]

We found that:

[redacted]

These issues occurred because facility management was not aware of the requirement for semiannual badge access reviews and did not communicate proper access procedures or enforce requirements for emergency and exterior door use [redacted]. This occurred because employees were not aware of the policy for challenging and escorting unauthorized individuals in controlled areas.

Finally, facility management did not implement environmental controls to protect IT assets against water and fire damage in the information system office and the IT server room. This occurred because the information system office was not intended to be a server room and budget constraints prevented recharging the fire suppression system.

When the Postal Service does not implement proper physical security, there is an increased risk of theft, vandalism, and unauthorized access to IT assets and controlled areas. In addition, without effective environmental controls to protect IT assets, water and fire damage would disrupt mail processing operations.

What the OIG Recommended

We recommended facility management communicate access policy requirements to all personnel and conduct a badge access review for all controlled areas. We also recommended facility management communicate and enforce policy requirements for using emergency and exterior doors.

In addition, we recommended facility management implement compensating controls for the doors without functioning card readers and the parking lot gates until installation of the new badge access system and repairing the gates, repair security cameras, and communicate policy for challenging and escorting unauthorized individuals in controlled areas. Finally, facility management should implement environmental controls to protect IT assets from water damage in the information system office and from fire damage in the IT server room.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 19, 2018

MEMORANDUM FOR: KEVIN V. ROMERO
COLORADO/WYOMING DISTRICT MANAGER

FROM: E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Deskt

Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Western Area Physical Security and Environmental Controls (Report Number IT-AR-18-002)

This report presents the results of our audit of the Western Area Physical Security and Environmental Controls (Project Number 17TG008IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Jason Yovich, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Vice President, Western Area
Senior Plant Manager, [redacted] P&DC
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's Western Area Physical Security and Environmental Controls (Project Number 17TG008IT000). Our objective was to determine whether the Postal Service has implemented the physical security and environmental and wireless access controls according to policy and industry best practices at the [redacted] Processing and Distribution Center (P&DC).

Background

The Postal Service has the mail processing resources, information technology (IT) network, and transportation infrastructure necessary to deliver mail to every residential and business address in the country. These resources include facilities, equipment, and systems used to process, transfer, and store data vital for business operations. The Postal Service implements physical security and environmental controls at facilities to reduce the risk of system and equipment failure, damage from environmental hazards, and unauthorized access to its facilities and assets.

In addition, the Postal Service relies on a high-quality, secure, and cost-effective wireless infrastructure to support its operations. Unauthorized wireless access points allow attackers to gain access to the Postal Service network and disrupt operations.

The Denver P&DC is 630,806 square feet and processes about 475 million mail pieces annually. The facility also includes a retail store, business mail entry unit (BMEU), and administrative offices. We did not identify any wireless issues at the [redacted] P&DC; however, the Postal Service did not implement effective physical security and environmental controls.

Finding #1: Access Control Management

Facility management did not implement effective access controls to restrict unauthorized access to the facility and protect critical assets.

"Facility management did not implement effective access controls to restrict unauthorized access to the facility and protect critical assets."

Specifically, we found:

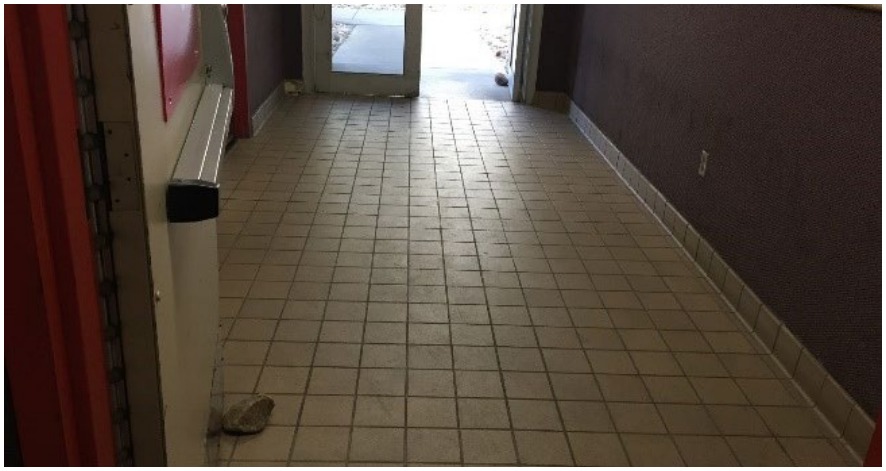
- Excessive access was granted to the [redacted] Of the [redacted] facility employees, we found:
  - [redacted]
  - [redacted]
- [redacted]

This occurred because facility management was not aware of the requirement to perform semiannual badge access reviews.[3]

1 Handbook AS-805, *Information Security*, Section 7-2.2, Establishment of Access Control Lists, dated August 2017.
2 [redacted].
3 Handbook AS-805, Section, 7-2.4, Establishment of Access Control Lists.
4 Handbook AS-805, Section 7-2.1 (b), Section Access to Controlled Areas.

- [redacted]
- [redacted]

[redacted]



Source: U.S. Postal Service Office of Inspector General (OIG) photograph taken October 23, 2017.

[redacted]

Source: OIG photograph taken October 23, 2017.

- [redacted][8]
- [redacted][11]

According to facility management, budget constraints prevented them from repairing the [redacted].

5 [redacted]
6 Handbook ASM-13, *Administrative Support Manual*, Section 277.233, Form 4098-F and Employee Identification, dated July 20, 2017.
7 Handbook ASM-13, Sections 273.122 and 273.123, Door Locks and Compliance.
8 Handbook RE-5, *Building and Site Security Requirements*, Section 2-1.5, Site Access Control System at Mail Processing Facilities, dated September 2009.
9 [redacted].
10 Handbook RE-5, Section 2-5, Exterior CCTV Security System, pg. 17-18.
11 [redacted]

When the Postal Service does not implement proper physical security controls, there is an increased risk of theft; disruption of critical operations; and unauthorized access to facilities, IT assets, and mail processing equipment.

[redacted]

Recommendation #1:
We recommend the **District Manager, Colorado/ Wyoming District**, direct the senior plant manager to communicate badge access review policy requirements to managers.

Recommendation #2:
We recommend the **District Manager, Colorado/Wyoming District**, direct the senior plant manager to require responsible managers to complete badge access reviews.

Recommendation #3:
We recommend the **District Manager, Colorado/Wyoming District**, direct the senior plant manager to implement compensating controls for doors without a functioning card reader.

Recommendation #4:
We recommend the **District Manager, Colorado/Wyoming District**, direct the senior plant manager to communicate access procedures to the resource management personnel to ensure employees without a Postal Service badge do not gain access to the facility west entrance.

Recommendation #5:
We recommend the **District Managerr, Colorado/Wyoming District**, direct the senior plant manager to enforce emergency exit and exterior door security policy requirements to employees.

Recommendation #6:
We recommend the **District Manager, Colorado/Wyoming District,** direct the senior plant manager to implement [redacted]

Finding #2: [redacted]

[redacted]

This occurred because [redacted] employees were not aware of the policy for challenging and escorting unauthorized individuals. They expected to see unfamiliar individuals in the [redacted] area because they are accessible from the [redacted]

When the Postal Service does not implement physical security controls, there is an increased risk of theft, disruption of critical operations, and unauthorized access to Postal Service assets. [redacted]

Recommendation #7:
We recommend the **District Manager, Colorado/ Wyoming District**, direct the senior plant manager to communicate policy requirements for challenging and escorting unauthorized individuals in controlled areas.

Finding #3: Environmental Controls

Facility management did not implement water and fire safeguard environmental controls in the information system office and the IT server room according to policy.[14] Specifically:

- IT assets in the information system office were not protected against water damage from the sprinkler system. Figure 3 shows a sprinkler head above IT equipment in the information system office.

12 [redacted].
13 Handbook ASM-13, Section 273.131, Unauthorized Individuals.
14 Handbook AS-805, Section 7-4, Environmental Security (b and e).

Figure 3. Information System Office

Source: OIG photograph taken October 23, 2017.

- The fire suppression system in the IT server room was discharged in 2006 and never refilled.

According to facility management, these occurred because the information system office was not intended to be an IT server room. In addition, budget constraints did not allow facility management to recharge the fire suppression system.

When the Postal Service does not implement proper environmental controls, there is an increased risk of fire or water damage to IT assets which could jeopardize employee safety or disrupt the mail processing and distribution operations.

Recommendation #8:

We recommend the **District Manager, Colorado/Wyoming District**, direct the senior plant manager to implement environmental controls for protecting information technology assets against water damage in the information system office.

Recommendation #9:

We recommend the **District Manager, Colorado/Wyoming District**, direct the senior plant manager to recharge the fire suppression system in the Information Technology server room.

Management's Comments

Management agreed with all findings and recommendations in the report and stated they have implemented recommendations 1 and 2 and will implement the remaining seven recommendations by September 2018.

Regarding recommendations 1 and 2, management has purged the existing security access database and reassigned only current and authorized personnel and conducted a semiannual review on November 8, 2017.

Regarding recommendations 3 and 4, management will install a new security system, [redacted], to address [redacted]. In the interim, management will secure doors with keys and give instruction to employees on wearing/displaying ID badges and challenging any person who does not display the appropriate credentials. Management will implement [redacted]

Regarding recommendation 5, management will [redacted] The target date for completion was January 2018.

Regarding recommendation 6, management will install [redacted] that will include new card readers and gates. The target date for implementation is [redacted] The response did not address [redacted].

Regarding recommendation 7, management will conduct security talks with all employees by March 15, 2018.

Regarding recommendation 8, management will cap the sprinklers head in the information system office upon implementation of recommendation 9. The target implementation date is May 30, 2018.

Regarding recommendation 9, management will recharge the FM200 fire suppression system. The target implementation date is May 30, 2018.

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 the corrective actions should resolve the issues identified in the report.

Regarding recommendations, 1, 2, 5, and 7, management stated that they have taken corrective action but did not provide support. For the recommendations to be officially closed, management should provide support demonstrating they have taken corrective action.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

The scope of this audit was physical security, environmental and wireless access controls at the [redacted] P&DC. Some OIG surveillance cameras are in this facility; however, we excluded them from the scope of this audit.

We selected the [redacted] P&DC using the following methodology:

- Obtained data for Postal Service districts listed in the OIG's FY 2016 Performance and Results Information System Facilities Risk Model[15] to identify the P&DC that ranked highest in square footage, revenue, mail volume, hours worked, and co-located functional areas.[16]
- Obtained data from the FY 2016 Vulnerability and Risk Assessment Tool (VRAT)[17] report to select from the top five facilities based on information security, security system, and facility site and exterior vulnerabilities.
- Obtained data from the OIG's FY 2017 IT Security Risk Model[18] to rank the top five facilities based on highest number of malware incidents.

To accomplish our objective we:

- Reviewed Postal Service's physical security policies, processes, and procedures to gain an understanding of the environment.
- Reviewed the facility's recent VRAT to determine if a risk-based approach was used to implement controls and identify sensitive areas and critical resources.
- Reviewed the badge access system, surveillance cameras, parking lot gates, facility exit and exterior doors, key inventory, and badge card readers to determine if opportunities for unauthorized access existed.
- Reviewed badge access, ID cards, smartcards, passkeys, and other entry devices to determine if they are controlled and monitored.
- Interviewed management to determine whether they granted access to controlled areas on a need-to-know basis and revoked terminated and re-assigned employees/contractors.
- Observed and assessed the effectiveness of physical and perimeter security procedures for controlling access to the facility during our site visit to the facility.[19]
- Verified appropriate environmental controls are in place to protect facility personnel, equipment, and IT assets during our site visit to the facility.
- Analyzed the wireless network for adequate wireless coverage and unauthorized access points.

We conducted this performance audit from September 2017 through March 2018, 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 February 9, 2018, and included their comments where appropriate.

We assessed the reliability of access system[20] data by analyzing employee data, observing security procedures, and interviewing [redacted] P&DC management. We determined that the data were sufficiently reliable for the purpose of this report.

15 Identifies and measures at risk districts that could affect the facilities' ability to provide facility services.
16 [redacted]
17 U.S. Postal Inspection Service performs this assessment. The VRAT report addresses seven vulnerabilities. We considered the ones related to information systems and physical security controls and did not consider: personnel security or policies procedures and registry/remittance vulnerabilities.
18 Measures inbound spam emails and antivirus security events detected on the Postal Service's nationwide network.
19 Handbook AS-805, Section 11-11.8.2, Physical Security Requirements; and Handbook RE-5, Sections 2-1.5 & 2-5, Building and Site Security Requirements, pg. 23 -24.
20 The [redacted].

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Pacific Area Processing and Distribution Center Physical and Environmental Security Controls	Determine whether the Postal Service has adequate and effective physical and environmental security controls at the Margaret L. Sellers P&DC.	IT-AR-17-005	5/3/2017	None
Electronic Media Disposal	Determine effectiveness of the IT electronic media disposal process.	IT-AR-16-008	6/28/2016	None
Topeka, KS, Material Distribution Center Information Technology General Controls	Determine whether general security controls pertaining to physical access contingency planning, security management, and segregation of duties at the center's administrative building provides reasonable assurance that computer assets, processed payroll data, and vendor data are secure.	IT-AR-14-006	6/11/2014	None

Appendix B: Management's Comments

Colorado/Wyoming
District Manager

UNITED STATES
POSTAL SERVICE

February 28, 2018

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Western Area Processing and Distribution Center Physical Security and Environmental Controls: Report Number IT-AR-18 DRAFT

In response to the subject audit recommendations, we agree with the findings and offer the actions outlined below in response. We would recommend against disclosure of this activity outside the Postal Service except for the redacted version.

Recommendation [1]: We recommend the District Manager, Colorado/ Wyoming District, direct the Senior Plant Manager to communicate badge access review policy requirements to managers.

Management Response/Action Plan: Management agrees with the OIG's findings. Management has purged the existing security access database and reassigned only current and authorized personnel.

Target Implementation Date:
Completed on 11/8/2017

Responsible Official:
Human Resources Manager

Recommendation [2]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to require responsible managers to complete badge access reviews.

Management Response/Action Plan: Management agrees with the OIG's findings.
Management has purged the existing security access database and reassigned only current and authorized personnel. A semiannual review was conducted by LDDC personnel to remain in compliance.

Target Implementation Date:
Completed on 11/8/2017

Responsible Official:
Human Resources Manager

Recommendation [3]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to implement compensating controls for doors without a functioning card reader.

Management Response/Action Plan: Management agrees with the OIG's findings.
[redacted]
In the interim, doors that can be, will be secured with keys. Employees will receive instructions on wearing / displaying ID badges and challenging any persons who do not display appropriate credentials.

Target Implementation Date:
March 15, 2018 - Stand ups
[redacted]

Responsible Official:
[redacted]

WWW.USPS.COM

Maintenance Manager, [redacted]

Recommendation [4]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to communicate access procedures to the resource management personnel to ensure employees without a Postal Service badge do not gain access to the facility west entrance.

Management Response/Action Plan: Management agrees with the OIG's findings. [redacted] In the interim, employees will receive instructions on wearing / displaying ID badges and challenging any persons who do not display appropriate credentials.

Target Implementation Date:
March 15, 2018 – Stand ups
[redacted]

Responsible Official:
Maintenance Manager, [redacted]

Recommendation [5]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to enforce emergency exit and exterior door security policy requirements to employees.

Management Response/Action Plan: Management agrees with the OIG's findings.
Management installed tamper proof fasteners in the door latch assembly to prevent unauthorized door disarmament.

Target Implementation Date:
January 2018

Responsible Official:
Maintenance Manager, [redacted]

Recommendation [6]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to implement security controls for the [redacted]

Management Response/Action Plan: Management agrees with the OIG's findings. [redacted] This upgrade will include new badge readers and gates.

Target Implementation Date:
[redacted]

Responsible Official:
Maintenance Manager, [redacted]

Recommendation [7]: We recommend the District manager, Colorado/ Wyoming District, direct the Senior Plant Manager to communicate policy requirements for challenging and escorting unauthorized individuals in controlled areas.

Management Response/Action Plan: Management agrees with the OIG's findings.
Management will conduct security talks on all three tours.

Target Implementation Date:
March 15, 2018

Responsible Official:
Lead Sr. Manager, Distribution Operations

Recommendation [8]: We recommend the District manager, Colorado/Wyoming District, direct the Senior Plant Manager to implement environmental controls for protecting information technology assets against water damage in the information system office.

Management Response/Action Plan: Management agrees with the OIG's findings. Management will cap the sprinklers heads in the identified room upon completion of recommendation #9.

Target Implementation Date:
May 30, 2018

Responsible Official:
Maintenance Manager, [redacted]

Recommendation [9]: We recommend the District Manager, Colorado/Wyoming District, direct the Senior Plant Manager to recharge the fire suppression system in the IT server room.

Management Response/Action Plan: Management agrees with the OIG's findings. Facilities Project Manager has been on site with contractors to solicit bids to recharge the FM200 Fire Suppression System.

Target Implementation Date:
May 30, 2018

Responsible Official:
Maintenance Manager, [redacted]

Kevin Romero
District Manager
CO/WY District

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100