Office of Inspector General | United States Postal Service

Audit Report

Northeast Area Environmental and Physical Controls Site Security Review

Report Number IT-AR-19-003 | January 31, 2019

Table of Contents

Highlights

Objective

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

The Postal Service has the mail processing resources, information technology (IT) network, and transportation infrastructure 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, which are critical to business operations.

"Our objective was to determine whether the Postal Service established and implemented effective environmental and physical security controls according to policy."

The [redacted] P&DC has [redacted] interior square feet and processes about 3.2 billion pieces of mail annually. In addition, the facility includes delivery functions, retail store, administrative offices, and a business mail entry unit (BMEU). We selected the [redacted] P&DC based on geographic location, facility size, the number of co-located functions, and overall risk.

What the OIG Found

While we did not identify any environmental control issues, we did find some physical security weaknesses at the [redacted] P&DC. We found that management did not review and update access to the facility and secure areas. For example, management did not remove access for separated employees and did not challenge an unidentified individual at the BMEU facility. Finally, we found broken locks on entrance doors and open unattended doors.

These issues occurred because facility managers were not aware of the requirement to review access lists semiannually and employees did not follow procedures for removing the facility access of separated employees. In addition, facility employees believed the individual worked in the mail processing plant and needed to use the BMEU facility. Finally, management was not aware of the broken locks and did not enforce the policy to secure entrance doors.

When Postal Service management does not review and update facility access, restrict access to critical areas, and secure doors, there is an increased risk of unauthorized individuals gaining access to critical IT and mail processing systems that are vital to business operations.

During the audit, management took corrective action by removing unnecessary access and conducting security briefings to remind employees of their physical security responsibilities such as challenging unidentified individuals and securing doors when not in use.

What the OIG Recommended

We recommended facility management review and update the current badge access list to allow only authorized personnel access to the facility and secure areas. In addition, we recommended management conduct and document semiannual reviews, communicate badge access procedures to Human Resource employees, remove access for separated individuals, and repair broken entrance door locks.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 31, 2019

MEMORANDUM FOR: [redacted]
DISTRICT MANAGER, [redacted] DISTRICT

E-Signed by Charles Turley
VERIFY authenticity with eSign Desktop

for

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Northeast Area Environmental and Physical Controls Site Security Review (Report Number IT-AR-19-003)

This report presents the results of our audit of the Northeast Area Environmental and Physical Controls Site Security Review (Project Number 18TG013IT000).

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, Northeast Area
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's Northeast Area Environmental and Physical Controls Site Security Review (Project Number 18TG013IT000). Our objective was to determine whether the Postal Service established and implemented effective environmental and physical security controls over information technology according to Postal Service policy at the [redacted] Processing and Distribution Center (P&DC).

Background

Environmental security controls protect facility-, room-, and information-level resources from damage, destruction, or interruption due to fire, humidity, water, and power outage. Physical security is the protection of personnel, hardware, software, and networks from intentional or unintentional loss or impairment of data, system availability, or long-term facility loss. Facilities should include risk-based security measures to protect assets from loss or damage. Environmental and physical and security measures include fire alarms, suppression systems, uninterrupted power supplies, guards, gates, locks, and access control cards.

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

The Postal Service has the mail processing resources, information technology (IT) network, and transportation infrastructure 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, which are critical for business operations. The Postal Service implements environmental and physical security controls at facilities to reduce the risk of system and equipment failure, damage from environmental hazards, and unauthorized access to its IT and mail processing assets.

The [redacted] P&DC has [redacted] interior square feet and processes about 3.2 billion pieces of mail annually with over 1,150 IT assets[1] and employs about 1,680 employees. The facility has an IT server room and a National Directory Support System[2]/Image Processing Subsystem (NDSS/IPSS) server room. In addition, the facility includes delivery functions, a retail store, administrative offices, and a business mail entry unit (BMEU).

[redacted] P&DC managers have implemented several environmental and physical security controls to protect its IT and mail processing assets. For example, fire detection and suppression, surge protection, and redundant power sources were in place to protect IT and mail processing servers and equipment. In addition, postal police and security guards provided 24/7 surveillance and conducted random security checks of packages and personal bags for individuals entering

1 IT assets include computers, printers, servers, and switches. We extracted this information from the Asset Management Information System (AIMS) and ForeScout on September 18, 2018.
2 A distributed Database Management System (DBMS) designed to support the various Postal Service mail processing automation systems.

the facility. Finally, 80 new cameras were installed and positioned at critical locations to monitor and record vehicle and employee activities.

Finding #1: Badge Access Control

Facility management did not review, update, or restrict access to the facility and secure areas that contain IT and mail processing servers and computers with access to Postal Service information. Postal Service policy[3] states that management must update access control lists when new personnel are assigned to the controlled area or when someone leaves. In addition, access control lists must be reviewed and updated semiannually and access to controlled areas must be restricted to personnel needing the least amount of access to perform their duties.

"Facility management did not review, update, or restrict access to the facility and secure areas."

We found the following during our review:

- One thousand fifty-five of 2,730 (39 percent) individuals with access to the facility were not on the facility's official time and attendance records.[4] For example, seven OIG employees have had access to the facility since 2014, when they visited during an audit.
- Two hundred fifty-eight of 395 (65 percent) separated employees[5] still had access to the facility because facility management did not remove access.
- Facility managers granted access to secure areas within the facility (i.e., IT and mail processing servers) and did not verify whether access was required to perform job duties. For example, individuals with elevated access include two custodians, two mail carriers, a ramp clerk,[6] and a mail processing clerk. Specifically, we identified:
  - Fifteen of 109 (14 percent) individuals had inappropriate access to the IT server room, which supports file and print activity for the Advanced Computing Environment (ACE).[7]
  - Twenty-eight of 153 (18 percent) individuals had inappropriate access to the NDSS/IPSS server room, which supports address directories for the mail processing environment.

This occurred because facility managers were not aware of the requirement to review access lists semiannually. Additionally, Human Resources employees at the facility did not follow [redacted] District identification badge instructions to ensure removal of facility access for separated employees. When Postal Service management does not review and update facility access, there is an increased risk of unauthorized individuals gaining access to critical IT and mail processing systems that process, transfer, and store data vital for business operations.

During the audit period, management began to remove access of separated and unauthorized employees to the facility and secure areas.

Recommendation #1

The **District Manager,** [redacted] **District**, continue to review and update the current badge access list to allow only authorized personnel access to the facility and secure areas.

Recommendation #2

The **District Manager,** [redacted] **District**, conduct and document semiannual reviews of badge access according to policy.

3 Handbook AS-805, *Information Security*, Section 7-2.4 Establishment of Access Control Lists, 7-2.1 (a) Access to Controlled Areas, dated February 2018.
4 For the purposes of this report, we are referring to the Time and Attendance Collection System (TACS), which collects employee hours and attendance for payroll processing.
5 Separation dates from October 3, 2017, to October 12, 2018.
6 Ramp clerk duties include monitoring mail handling operations of air carriers on the ramp and ensuring all mail due for transport is included on flights for which the mail has been scheduled.
7 Centralizes access management to protect the security and integrity of Postal Service computing resources.

Recommendation #3

The **District Manager, [redacted] District**, communicate Greater [redacted] District identification badge procedures to Human Resources employees and remove access for separated individuals.

Finding #2: Controls to Restricted Areas – Business Mail Entry Unit Access

BMEU employees allowed an unidentified individual with no visible badge to enter the controlled area unchallenged. During our site visit, an OIG employee entered the BMEU with access to ACE computers and the PostalOne! system,[8] which connect to the Postal Service computer network. According to policy, all employees are charged with the responsibility of preventing unauthorized individuals, including off-duty employees, from entering restricted areas. All individuals on the workroom floor not properly identified or escorted should be immediately challenged.[9]

"BMEU employees allowed an unidentified individual with no visible badge to enter the controlled area unchallenged."

This occurred because BMEU employees believed the unidentified individual worked in the mail processing plant and needed to use the BMEU facility. The lack of physical security controls increases the risk of theft, disruption of critical operations, and unauthorized access to Postal Service assets. In addition, unauthorized personnel could access Postal Service systems and negatively affect mail processing activities.

In response to our observation, management promptly held a security briefing to remind BMEU personnel of their physical security responsibility to challenge unidentified individuals. In addition, management required BMEU swinging doors to be locked when not in use; therefore, we are not making any recommendations for this finding.

Finding #3: Perimeter Controls – Facility Doors

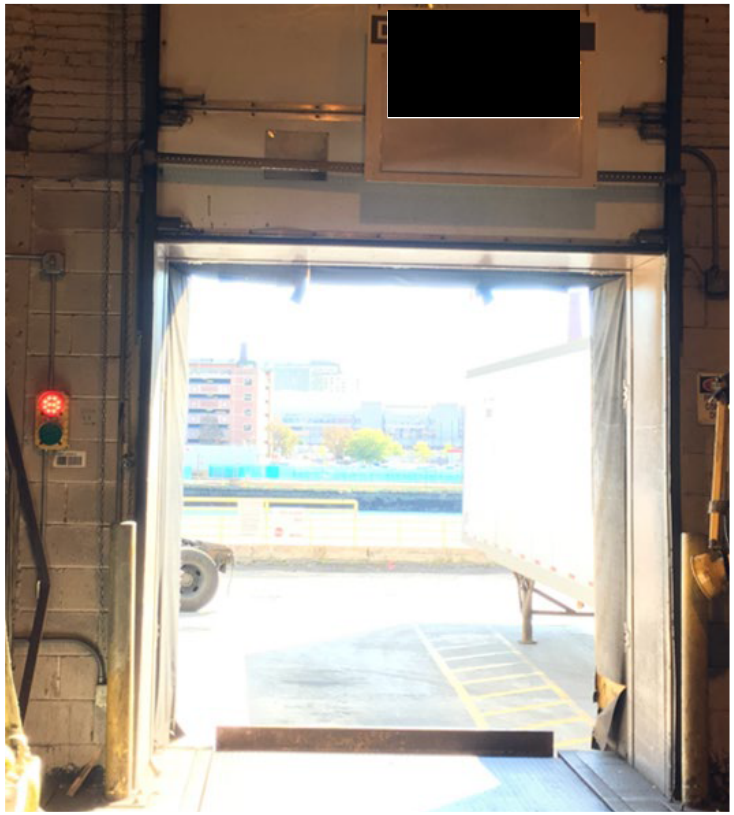
Management did not have operational perimeter security controls in place. Specifically, three entrance door locks were broken and two doors were propped open. In addition, eight overhead dock doors were open and unattended. Figure 1 shows one entrance dock door propped open and Figure 2 shows an open overhead dock door. Postal Service policy[10] states that doors are to be locked and all employees must comply with policy governing access to restricted areas.

8 Contains sensitive financial and mailing information including mailer payment and verifications, and mail volume.
9 Handbook ASM-13, *Administrative Support Manual*, Section 273, Facility Security, Section 273.131, Unauthorized Individuals, dated August 2, 2018.
10 Handbook ASM-13, Sections 273.122, Door Locks, and 273.123 Compliance, dated August 2, 2018.

Figure 1. Entrance Door

Source: U.S. Postal Service Office of Inspector General (OIG) photograph taken October 15, 2018.

Figure 2. Overhead Dock Door



Source: OIG photograph taken October 16, 2018.

This occurred because management was not aware of the broken locks and did not enforce the policy to secure doors. Without secure doors, there is an increased risk of unauthorized individuals gaining access to IT assets and disrupting critical operations.

During the audit, management took corrective action and held a safety discussion for facility personnel stressing the importance of keeping doors secured. Therefore, we are only making a recommendation that the locks be repaired.

Recommendation #4

The **District Manager, [redacted] District**, repair facility entrance door locks.

Management's Comments

During the exit conference held on December 20, 2018, management agreed with all recommendations and stated they will implement corrective action by January 31, 2019. During the meeting, management emphasized their continued commitment to ensuring physical security controls are in place at the facility. Management also agreed to the OIG issuing the report without a formal response from management. The District Manager, [redacted] District, is responsible for implementing the recommendations.

When corrective actions on the recommendations have been implemented, management should provide supporting documentation for the actions taken. This will facilitate closure of the recommendations in the OIG and Postal Service tracking systems.

OIG 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.

Appendix

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

Additional Information

Scope and Methodology

The scope of this audit was environmental and physical security policies, processes, and controls to protect the [redacted] P&DC's mail processing equipment, IT resources, and personnel.

To accomplish our objective, we:

- Obtained the OIG Quarter 3, FY 2018, Facilities Risk Model,[11] which compiles data for all Postal Service facilities, and Handbook RE-5, which list factors that influence the level of security required at Postal Service facilities. The team compared the factors in RE-5 to the data captured in the facility risk model to select a facility to conduct a site security review. We selected the [redacted] P&DC based on geographic location,[12] facility size,[13] the number of co-located functions,[14] and overall risk score.[15]
- Observed and verified that appropriate environmental controls are in place to protect facility personnel, equipment, and IT resources.
- Reviewed physical security policies, processes, and procedures to gain an understanding of the environment.
- Identified and analyzed all security and access controls used to secure the facility ePhysical Access Control System (ePACS)[16] and Closed-Circuit Television System (CCTV).
- Determined whether management controlled and monitored badge access (for example, identification cards, smartcards, passkeys, and other entry devices).
- Compared the lists of employees with access to the facility and secure areas to the Web COmplement INformation System (WebCOINS)[17] to the TACS employee lists to validate the appropriateness of employee access.
- Determined if the CCTV system is monitored and functions according to Postal Service policy.
- Observed and assessed the effectiveness of perimeter security procedures for controlling access to the facility.

We conducted this performance audit from September through January 2019, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on December 20, 2018, and included their comments where appropriate.

We assessed the reliability of data from the ePACS system by comparing it to listings of active personnel retrieved from TACS and WebCOINS. In addition, we interviewed agency officials knowledgeable about the data and processes. We determined that the data were sufficiently reliable for the purposes of this report.

11 Identified and measured at-risk districts that could affect the facility's ability to provide facility services.
12 We covered the [redacted] areas in prior audits, so we removed those sites from selection.
13 For the purposes of this report, we are referring to interior square footage.
14 Processing, delivery, retail, administration, and vehicle maintenance.
15 Facility condition, revenue, and capacity.
16 Provides centralized management and oversight of facility access through identification badges and card readers.
17 A comprehensive complement tracking and planning tool to assist in managing complement.

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 controls at the [redacted] P&DC.	IT-AR-17-005	5/3/2017	None
Western Area Physical Security and Environmental Controls	Determine whether the Postal Service has implemented effective physical and environmental controls according to policy and industry best practices at the [redacted] P&DC.	IT-AR-18-002	3/19/2018	None
Capital Metro Physical and Environmental Controls Site Security Review	Determine whether the Postal Service has established and implemented effective physical and environmental security controls according to Postal Service policy at the [redacted] P&DC.	IT-AR-18-005	9/28/2018	None

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