OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Pacific Area Processing and Distribution Center Physical and Environmental Security Controls

Audit Report

Report Number
IT-AR-17-005

May 3, 2017

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

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

Background

The U.S. 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 vital for business operations. The Postal Service implements physical and environmental security controls over systems to reduce the risk of system and equipment failure, damage from environmental hazards, and unauthorized access to its facilities and assets.

The Margaret L. Sellers (MLS) Processing and Distribution Center (P&DC) is 760,000 square feet and processes up to 12 million mailpieces daily. The facility houses a vehicle maintenance facility, retail store, district and area administrative offices, and the U.S. Postal Inspection Service.

Our objective was to determine whether the Postal Service has adequate and effective physical and environmental security controls at the MLS P&DC.

What the OIG Found

Although we did not identify any significant environmental security issues, the Postal Service does not have adequate and effective physical security controls over systems at the MLS P&DC. Specifically, we found that managers did not review, update, and limit access to the facility or ensure perimeter controls restricted access to it. We also found retail store employees allowed unauthorized access to restricted areas; employees, contractors, and unauthorized individuals were able to enter facility parking lots without verification.

These issues occurred because:

- There was no oversight of access to secure areas.
- The Human Resources manager did not follow separated employee clearance procedures.
- Employees allowed unfamiliar individuals into the retail area and altered dock doors to give contract drivers access to the P&DC.
- The gate sensor at the employee entrance did not function properly.
- Managers instructed employees to open the truck entrance gate upon driver arrival without verifying identification.

Improperly implemented physical security controls increase the risk of theft or disruption of critical operations; and unauthorized access to the facility, IT assets, and mail processing equipment.

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

What the OIG Recommended

We recommended management assign personnel to approve access to secure areas, and review and update badge and key access requirements for all offices semiannually as required by policy. In addition, management should communicate and enforce policies and procedures to remove access for separated employees and to prevent unauthorized access to restricted areas.

Management should also repair the gate sensor at the employee entrance; instruct employees to verify access before allowing trucks into the facility; issue badges to contractors; and ensure dock doors lock and function properly.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

May 3, 2017

MEMORANDUM FOR: JAMES P. OLSON
SAN DIEGO DISTRICT MANAGER

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskt

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

SUBJECT: Audit Report – Pacific Area Processing and Distribution Center Physical and Environmental Security Controls (Report Number IT-AR-17-005)

This report presents the results of our audit of Pacific Area Physical and Environmental Security Controls for the Margaret L. Sellers Processing and Distribution Center (Project Number 17TG001IT000).

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
Corporate Audit Response Management
Vice President, Pacific Area
Senior Plant Manager, Margaret L. Sellers P&DC

Table of Contents

Findings

The Postal Service has the mail processing resources, IT network, and transportation infrastructure necessary to deliver mail to every residential and business address in the country.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's physical and environmental security controls for the Margaret L. Sellers (MLS) Processing and Distribution Center (P&DC) (Project Number 17TG001IT000). Our objective was to determine whether the Postal Service has adequate and effective physical and environmental security controls at the MLS P&DC. See Appendix A for additional information about this audit.

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 that are 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.

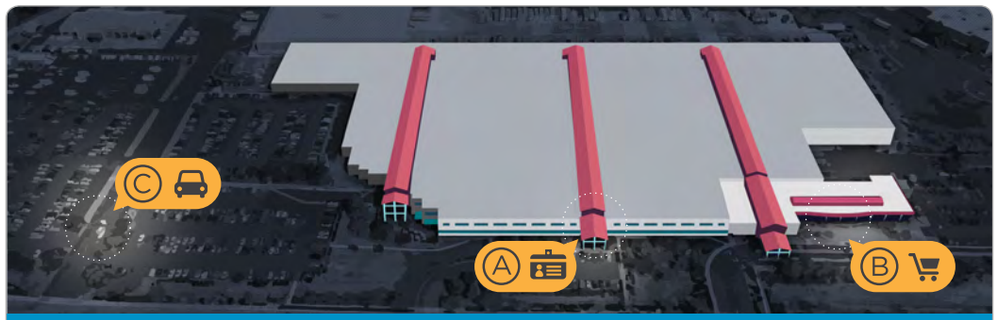
Summary

Although we did not identify any significant environmental security issues, the Postal Service did not have adequate and effective physical security controls at the MLS P&DC. Specifically, we found that:

- Managers did not review, update, and limit access to the facility. For example, they did not control access to secure areas of the P&DC, code temporary badges to expire on their termination date, or remove access for separated employees.
- Retail store employees allowed an unauthorized individual to enter restricted areas of the store unchallenged.
- Management did not ensure that perimeter controls were effective to restrict access to the facility. In addition, employees, contractors, and unauthorized individuals were able to enter facility parking lots without verification.

These issues occurred because:

- The plant manager did not assign managers to approve and review badge access to secure areas and the Human Resources manager did not follow procedures for employee separation.



Facility managers did not consistently remove access to the facility for separated and temporary employees and did not monitor visitor access.

- Employees expected to see unfamiliar individuals in the retail area because district managers and facility employees often visit and use the retail door.

- Employees intentionally altered dock doors to allow contract drivers access to the P&DC when they arrived. In addition, the gate at the employee entrance stayed open long enough to allow multiple cars to go through with a single badge swipe. Further, management instructed employees to open the truck entrance gate upon driver arrival without verifying identification.

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.

Management of Facility Access Controls

Facility managers did not review, update, and limit access to controlled areas within the facility in accordance with Postal Service policy.[1] Specifically, MLS managers granted access to secure areas and did not verify whether access was required to perform job duties. Our review identified:

- Three hundred sixty-two employees with access to the NDSS/IPSS computer room.

- Three hundred fifteen employees with access to the IT computer room.[2]

- Ninety-one employees with access the registry room.

Employees should have the minimum amount of access to information resources that they need to perform their duties. Based on our analysis, access to the computer room was excessive. For example, we identified mail carriers, tractor-trailer operators, maintenance support clerks, a labor relations specialist, the budget/finance analyst, and mail processing clerks with access to the computer rooms. One employee still had access to the registry room although management reassigned her over three years ago. We determined excessive access existed because the plant manager did not assign individual managers to approve and review access to each secured area. Instead, any manager can approve access for any secure area.

Removing and Monitoring Facility Access

Facility managers did not consistently remove access to the facility for separated and temporary employees and did not monitor visitor access. Specifically:

- Facility managers did not remove access to the facility for separated employees[3] to coincide with the employee's termination date in accordance with policy.[4] We reviewed employee termination dates for a twelve-month period[5] and identified 176 separated employees that retained access to the facility. This occurred because Human Resources employees were aware of, but did not complete and forward PS Form 337, Clearance Record for Separated Employees, to training department personnel responsible for removing badge access.

---

1 Handbook AS-805, *Information Security*, Section 7-2.2, Establishment of Controlled Areas, dated November 2016.
2 The designated computer room for IT resources. The room has switches, routers, and a file server that manages all ACE computers, printers, and monitors for the facility.
3 For the purposes of this report, separated employees include those who were transferred/reassigned, retired, resigned, or terminated.
4 Handbook AS-805, Section 6-6.1, Routine Separations.
5 The termination dates are from November 16, 2015 through November 21, 2016.

- Facility managers did not code temporary employee badges to expire on their termination date in accordance with policy.[6] Instead, temporary badges were set to expire after five years. This occurred because Human Resources employees coded temporary badges the same as badges for permanent employees. During our audit, management implemented procedures to ensure that badge expiration dates matched temporary employees' termination dates; therefore, we are not making a recommendation for this issue.

- Facility managers did not consistently control visitor access and review visitor logs, as required by policy.[7] Specifically, employees did not require all visitors, including U.S. Postal Service Office of Inspector General (OIG) employees, to sign visitors' logs or always escort them into the facility. This occurred because visitor access controls were no longer centralized due to staff reductions. Each department is responsible for controlling its visitors, and managers were unaware that employees did not require all visitors to sign-in.

- Facility managers did not conduct key inventory and badge access reviews semiannually in accordance with policy. Specifically, managers have not conducted a key inventory since 2013, and have never reviewed and updated the badge access control list. This occurred because management was unaware of the policy[8] to conduct key inventory and badge access reviews semiannually.

When the MLS P&DC does not manage access controls, there is an increased risk of theft of assets, unauthorized access to sensitive data, or the disruption of mail processing operations.

Access to Retail Store

Retail store employees allowed an unauthorized individual to enter restricted areas unchallenged. During our site visit, an OIG employee was able to enter an area with access to point-of-sale[9] terminals, customer packages, and stamp and money order stock. This employee did not have a visible badge and was not questioned or reported by employees, as required by policy.[10]

This occurred because retail employees expected to see unfamiliar individuals in the retail store. Area and district managers and facility employees often visit the store and use the retail door to enter restricted areas of the facility. Unauthorized access to those restricted areas increases the risk to employee safety and of theft or damage of Postal Service assets.[11]

During our audit, management provided evidence that maintenance fixed the lock and the buzzer on the retail doors; therefore, we are not making a recommendation regarding securing the door to the restricted area.

---

6 Handbook AS-805, Section 6-6.1, Routine Separations.
7 Handbook AS-805, Section 7-2.1, Access to Controlled Areas.
8 *Administrative Support Manual* (ASM) 13, Section 273.451, Postal Service Keys and Access Control Cards, dated July 1999, updated through October 15, 2015.
9 Electronic system that records sales and payment transactions.
10 ASM 13 Section 273.131, Unauthorized Individuals.
11 The OIG assessed assets at risk for stamp and money order stock that was accessible to unauthorized personnel entering the retail area. We valued this stamp and money order stock at $73,235 based on the daily accountable retail stamp stock balance for December 8, 2016, and the average money order sales for the month of December. We assumed a low-moderate risk of this occurring; therefore, we only identified assets at risk totaling $48,101.

Employees intentionally altered dock doors to allow access to the facility. Although badge readers were installed and functioning, employees used zip ties and screws to prevent the doors from locking.

Perimeter Access Controls

Management did not ensure that perimeter controls were effective in restricting access to the facility, as required by policy.[12] Specifically, we found that:

- Employees intentionally altered dock doors to allow access to the facility. Although badge readers were installed and functioning, employees used zip ties and screws to prevent the doors from locking. Figure 1 shows the entry and exit doors to the dock altered with zip ties.
- Employees and unauthorized individuals were able to tailgate through the employee parking lot gate. Specifically, the employee gate stayed open for about 35-45 seconds after a badge swipe, allowing additional vehicles to enter the parking lot without verification. Postal Service policy[13] prohibits tailgating and states that personnel are responsible for immediately reporting any instance of tailgating. Figure 2 shows the gate opening as vehicles enter the employee parking lot.
- Employees monitoring the security cameras opened the dock gate to allow trucks access without using the intercom to verify the purpose of the visit.

Figure 1. Altered Dock Doors

Source: OIG photograph taken January 11, 2017.

12 Handbook AS 805, Section 11-11.8.2, Physical Security Requirements.
13 Handbook AS-805, Section 7-2.1, Access to Controlled Areas.

Management has not implemented adequate environmental controls to protect critical resources, as required by policy.

Figure 2. Employee Parking Lot Entrance Gate

Source: OIG photograph taken January 11, 2017.

This occurred because the facility installed badge readers on all dock doors; however, contract drivers were not issued badges to access the facility. Since the facility is a 24-hour operation, employees altered the doors with zip ties and screws to allow contract drivers access to any dock door when they arrived. In addition, the gate sensor and intercom at the employee entrance were not functioning properly. Specifically, the gate stalled and did not close immediately and the intercom was not operational. Finally, management instructed employees to open the truck entrance gate upon driver arrival without verifying identification.

Without effective perimeter controls, the Postal Service is less able to prevent unauthorized access to critical assets, such as mail processing equipment. When employees bypass perimeter controls, they increase the risk of unintentional loss or impairment of data and system availability; and disruption of mail processing operations.

During our audit, management repaired the intercom at the employee parking gate; therefore, we are not making a recommendation for this issue.

Recommendations

We recommend management assign responsible managers to approve employee access to each secured area, review and update the current badge access list, and communicate procedures to employees to prevent unauthorized individuals from entering restricted areas.

We recommend the district manager, San Diego District, direct the senior plant manager to:

1. Assign responsible managers to approve employee access to each secured area and review and update the current badge access list to allow only authorized personnel access into secure areas.
2. Communicate and enforce procedures to ensure a Postal Form 337, Clearance Record for Separated Employees, is completed and forwarded to Human Resources for employees who no longer need facility access.
3. Enforce the use of visitor logs for all departments and perform monthly reviews.
4. Conduct and document key inventory and badge access reviews semiannually.
5. Communicate procedures to employees to prevent unauthorized individuals from entering restricted areas of the retail store.
6. Adjust the gate at the employee parking lot to prevent employees from tailgating.
7. Instruct employees to verify contractors before allowing trucks to access the facility.
8. Issue badges to contract drivers and ensure that dock doors lock and function properly.

Management's Comments

Management agreed with the findings and recommendations in the report and stated they have begun to take corrective action.

Regarding recommendation 1, management will assign access approvers and alternates for each secure/critical location. They will also review current levels of access granted for each individual as required. Management plans to complete these actions by May 1, 2017.

Regarding recommendation 2, management will develop an employee separation process that includes badge termination, key check-in, etc. Management plans to complete this by May 1, 2017.

Regarding recommendation 3, management will implement a policy for each department to review their visitor logs and an assigned person will be responsible for periodic reviews. The facility security manager will review the logs every six months for compliance. Management plans to complete these actions by May 1, 2017.

Regarding recommendation 4, management will audit the key inventory process and perform key inventory twice a year. In addition, management will perform individual badge reviews when issuing new badges, when there is an increase in access level requested, or when there are position changes. Management stated these actions are currently in place.

Regarding recommendation 5, management will review access to controlled spaces and place signage in all restricted areas. Management plans to complete these actions by May 1, 2017.

Regarding recommendation 6, based on subsequent communications with Postal Service management, a security review was performed and determined that an adjustment to the gate will be made. Management stated they plan to complete these actions by April 28, 2017.

Regarding recommendation 7, management has placed instructions at the security console to challenge those entering the facility and a log book to record visitors by name and company. Management stated this is completed.

Regarding recommendation 8, management stated that contract drivers have been issued access badges. For the long-haul drivers who do not carry badges, a wireless door bell will require someone to open the door for them. At that point they will be challenged again. Management plans to complete these actions by May 1, 2017.

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 in the report except for recommendation 4, and the corrective actions proposed should resolve the issues identified.

Regarding recommendation 4, management stated they would perform individual badge reviews when issuing new badges, when there is an increase in access level requested, or when there are position changes. We believe management should also conduct semiannual reviews of badge access in accordance with Postal Service policy.

Management stated they have taken corrective actions for all recommendations in the report or will take corrective actions by May 1, 2017. Management has not provided support showing that they have implemented these corrective actions; therefore all recommendations will remain open until sufficient support is provided.

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 to the right to navigate to the section content.

Appendix A: Additional Information

Background

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 physical and environmental security measures to protect assets from loss or damage. Examples of these security measures include guards, gates, access control cards, and fire alarms. Without effective physical and environmental controls in place, organizations can spend thousands of dollars on technology that supports logical security[14] only to have operations interrupted by physical and environmental hazards.

The Postal Service implements physical and environmental security controls to protect the physical integrity of information resources located at its facilities. These controls are designed to reduce the risk of theft, system and equipment failure, damage from environmental hazards, and unauthorized personnel access.

The MLS P&DC is a 760,000 square foot facility that opened in 1992 and houses a vehicle maintenance facility, retail store, district and area administrative offices, and U.S. Postal Inspection Service offices. The facility is also a designated Concentration and Convey (CON-CON) “Registry” location. The MLS P&DC processes 7 to 12 million mailpieces daily, operating 24 hours a day, seven days a week, and employs about 1,000 people.

Objective, Scope, and Methodology

Our objective was to determine whether the Postal Service has adequate and effective physical and environmental security controls at the MLS P&DC. We selected the MLS P&DC using the following methodology:

- Obtained data for the 67 Postal Service districts listed in the OIG’s FY 2016 Performance and Results Information System (PARIS) Facilities Risk Module;[15] and identified the districts that ranked the highest in square footage, revenue, mail volume, hours worked, and co-located functional areas (P&DC, retail, administrative).

- Obtained data from the OIG’s FY 2016 PARIS IT Security Risk Model[16] to rank the top five facilities based on highest number of malware incidents.

To accomplish our objective, we:

- Obtained and reviewed physical security policies, processes, and procedures to gain an understanding of the environment.

- Obtained and reviewed the most recent Vulnerability and Risk Assessment Survey for the facility to determine if a risk-based approach was used to implement controls and identify sensitive areas and critical resources.

- Obtained a list of employees and contractors with badge access to the facility to:

  - Determine required level of access on a need to know basis, according to Postal Service policy.[17]

14 Logical security includes user account management, security activity reports, and firewalls.
15 Identifies and measures at risk districts that could affect the facilities’ ability to provide facility services.
16 Measures inbound spam emails and antivirus security events detected on the Postal Service’s nationwide network.
17 Handbooks AS-805 and RE-5, *Building and Site Security Management*, are intended to ensure a safe and secure environment for Postal Service employees, assets, and mail.

- Verify that access for terminated or reassigned employees and contractors is discontinued.
- Ensure that individuals with access to sensitive areas or critical resources are restricted based on job function.
- Observe and review appointment and verification procedures for visitors.

- Observed and assessed the effectiveness of physical and perimeter security procedures for controlling access to the facility during our site visit to the facility.
- Interviewed facility managers and IT and Postal Inspection Service personnel to determine the roles and responsibilities for the Postal Service's physical and environmental security program and controls.
- Verified that appropriate environmental controls are in place to protect facility personnel, equipment, and IT resources during our site visit.

We conducted this performance audit from November 2016 through May 2017, 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 March 17, 2017, and included their comments where appropriate.

We assessed the reliability of data from the Schlage Security System[18] by analyzing employee data, observing security procedures, and interviewing Postal Service officials. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact (in millions)
Electronic Media Disposal	Determine the effectiveness of the IT electronic media disposal process.	IT-AR-16-008	6/28/2016	$15.2
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 provide reasonable assurance that computer assets, processed payroll data, and vendor data are secure.	IT-AR-14-006	6/11/2014	None

18 The Schlage Security Management System delivers a single source solution for integrating a facility's access-control technologies and alarm monitoring systems.

Appendix B: Management's Comments

SENIOR PLANT MANAGER
SAN DIEGO DISTRICT

UNITED STATES POSTAL SERVICE

April 12, 2017

Lori Lau Dillard
Director, Audit Operations
U.S. Postal Service Office of the Inspector General

SUBJECT: Pacific Area Processing And Distribution Center Physical and Enviromental Security Controls.

Attached are the eight recommendations and the action plans for ensuring future compliance.

Jeffery A. Vibbert
Senior Plant Manager

April 12, 2017

LORI LAU DILLARD

DIRECTOR, AUDIT OPERATIONS

SUBJECT: Pacific Area Processing and Distribution Center Physical and Environmental Security Controls (Report number IT-AR-17-DRAFT

Management agrees with the findings from the Audit. Better control of access badges is needed.

Recommendation 1

- Assign responsible managers to approve employee access to each secured area and review and update the current badge access list to allow only authorized personnel access into secured areas.

Action Plan

- Management will assign access approvers and alternates for each secure/critical location. We will also review current levels of access to ensure access grant to each individual is required. May 1, 2017- Security Manager, HR, Plant Manager

Recommendation 2

- Communicate and enforce procedures to ensure a Postal Form 337, Clearance Record for Separated Employees, is completed and forwarded to Human Resources for employees who no longer need facility access. HR to review April 17, 2017

Action Plan

- Facility will develop a process for employees being separated, badge termination, key check-in, etc.... May 1, 2017- Security Manager, HR, Plant Manager

Recommendation 3

- Enforce the use of departmental visitor logs and perform monthly reviews.

Action Plan

- A policy will be put in place and each department will review their visitor logs. An assigned person will be responsible for periodic reviews. The Facility Security Manager will review them every 6 month's for compliance. May 1, 2017- Security Manager, HR, Plant Manager

Recommendation 4

- Conduct and document key inventory and badge access reviews semiannually.

Action Plan

- Key inventory management will be audited and a route placed in eMARS to perform key inventory twice a year. In place
- Individual badge reviews will be performed when new badges are issued, increase in access level is requested or changes in positions occur. May 1, 2017- Security Manager, HR, Plant Manager

Recommendation 5

- Communicate procedures to employees to prevent unauthorized individuals from entering restricted areas of the retail store.

Action Plan

- Access to controlled spaces will be reviewed. We will also place signage at all restricted areas. May 1, 2017- Security Manager, HR, Plant Manager

Recommendation 6

- Adjust gate at the employee parking lot to prevent employees from tailgating.

Action Plan

- A call was placed for a security review with the Physical Security Specialist. The request is being reviewed. Unknown

Recommendation 7

- Instruct employees to verify contractors before allowing trucks to access the facility.

Action Plan

- Instructions have been placed at the Security console to 'challenge' those entering the facility. A log book was also placed to log visitors with name and company. Complete

Recommendation 8

- Issue badges to contract drivers and ensure that dock doors lock and function.

Action Plan

- Contract drivers have been issued access badges. For the long haul drivers who do not carry badges, a wireless door bell will require someone to open the door for them and at that point they will be challenged again. The doors are locked. Door bells on order. May 1, 2017- Security Manager.

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