



Office of Inspector General | United States Postal Service

Audit Report

Physical and Environmental Controls Site Security Review – Summary Report

Report Number IT-AR-19-004 | August 15, 2019



Table of Contents

Cover.....	1	Recommendation #2	7
Table of Contents	2	Finding #2: Review of Facility Employee Access.....	8
Highlights.....	1	Recommendation #3.....	9
Objective	1	Recommendation #4.....	9
What the OIG Found.....	1	Other Matters	10
What the OIG Recommended	1	Facilities Without	10
Transmittal Letter	2	Management’s Comments.....	10
Results.....	3	Evaluation of Management’s Comments	11
Introduction/Objective	3	Appendices	12
Background.....	3	Appendix A: Additional Information.....	13
Summary of Physical and Environmental Controls Site Security Review Audits.....	5	Scope and Methodology.....	13
Recommendations and Management Corrective Actions .	6	Prior Audit Coverage.....	14
Potential Physical Security Control Issues at Other Processing & Distribution Centers	7	Appendix B: Causes for Physical Security Control Issues ..	15
Finding #1: Remediation of Vulnerability Risk Assessment Tool Deficiencies.....	7	Appendix C: Analysis of Employee Access to Computer Rooms.....	16
Recommendation #1	7	Appendix D: Management’s Comments.....	18
		Contact Information	21

Highlights

Objective

Our objective was to identify and summarize the findings and recommendations in four issued area physical and environmental controls site security reports. The objective of those four audits was to determine whether the U.S. Postal Service established effective physical and environmental security controls at processing and distribution centers (P&DC). As part of this audit, we identified other P&DCs where data suggest similar risks and conditions may exist.

The Postal Service has 205 P&DCs nationwide, which range in interior size from about 46,500 square feet to about 1.3 million square feet and in age from one year to 83 years old. The Vulnerability Risk Assessment Tool (VRAT) is the application employees use to identify security risks and vulnerabilities at these facilities.

During fiscal years 2017 – 2019, the OIG conducted site security audits at P&DC facilities in four Postal Service areas: Pacific, Western, Capital Metro, and Northeast. These audits focused on physical and environmental controls that protect information technology (IT) and mail processing assets.

What the OIG Found

Overall the Postal Service has effective physical security and environmental protection over its IT assets for the four sites visited because it uses a defense-in-depth strategy employing multiple physical security controls. For example, a server room is protected by multiple layers of security to include: facility gates, guards, cameras, and a badge access reader. However, we identified specific controls that needed improvement, including [REDACTED]. These control weaknesses occurred because facility management did not review, update, and limit access to the four facilities; and management did not keep perimeter controls operational [REDACTED] such as propping doors. The Postal Service has implemented 23 of the 26 recommendations in the four security reports.

We identified similar control weaknesses at [REDACTED] of 205 P&DCs, as reported within VRAT reports and our analysis of access lists. We found that at the four facilities we visited, management [REDACTED]

[REDACTED] for the [REDACTED] P&DCs. In addition, we found indications at [REDACTED] P&DCs that designated [REDACTED] administrators [REDACTED] as required and as we found at the four facilities we visited. The Postal Service [REDACTED]

[REDACTED] to address VRAT deficiencies, and management did not [REDACTED]

When the Postal Service [REDACTED] [REDACTED] the risk of unauthorized individuals gaining access to critical IT and mail processing systems that process, transfer, and store data vital for business operations increases.

What the OIG Recommended

We recommended the Postal Service:

- Develop and implement a [REDACTED] that requires management to follow-up on each physical security deficiency identified by the VRAT within a specified time frame.
- Revise the Administrative Support Manual 13 to describe the [REDACTED] in response to VRAT deficiencies, including management roles and responsibilities.
- Review [REDACTED] basis to remove unauthorized persons and limit access to secure areas to authorized employees only.
- Develop and review an exception report semiannually that would use data from [REDACTED] and the human resource system of record, which would flag employees who should not be authorized access to a designated facility.

“The Postal Service

[REDACTED]

Transmittal Letter




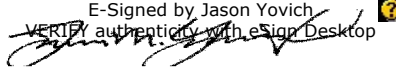
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 15, 2019

MEMORANDUM FOR: DAVID E. WILLIAMS, JR., CHIEF OPERATING OFFICER
AND EXECUTIVE VICE PRESIDENT

GARY R. BARKSDALE, CHIEF POSTAL INSPECTOR

PRITHA N. MEHRA, VICE PRESIDENT,
INFORMATION TECHNOLOGY

E-Signed by Jason Yovich
VERIFY authenticity with eSign Desktop 


FROM: Jason Yovich
Acting Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Physical and Environmental Controls
Site Security Review - Summary Report
(Report Number IT-AR-19-004)

This report presents the results of our audit of the Physical and Environmental Controls Site Security Review - Summary Report (Project Number 19TG007IT000).

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

Attachment

cc: Postmaster General
Corporate Audit Response Management
Vice President, Capital Metro Area
Vice President, Eastern Area
Vice President, Great Lakes Area
Vice President, Northeast Area
Vice President, Pacific Area
Vice President, Southern Area
Vice President, Western Area
Vice President, Employee Resource Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Physical and Environmental Controls Site Security Review - Summary Report (Project Number 19TG007IT000). Our objective was to identify and summarize the findings and recommendations in four U.S. Postal Service Office of Inspector General (OIG) issued area physical and environmental controls site security reports. The objective of those four audits was to determine whether the U.S. Postal Service established effective physical and environmental security controls at processing and distribution centers (P&DC). As part of this review, we identified other P&DCs where data suggest similar risks and conditions may exist. See [Appendix A](#) for additional information about this audit.

Background

Physical security controls protect personnel, hardware, software, and networks from unintentional loss of impairment of data, system availability, or long-term facility loss. Environmental security controls protect facility-, room-, and information-level resources from damage, destruction, or interruption due to fire, humidity, water, and power outage.

The Postal Service has 205¹ P&DCs² nationwide, which range in interior size from about 46,500 square feet to about 1.3 million square feet and in age from one to 83 years old. From fiscal years (FY) 2017 to 2019, the OIG conducted a series of site security audits focused on physical and environmental controls that protect information technology (IT) and mail processing assets at P&DCs in four Postal Service areas: Pacific, Western, Capital Metro, and Northeast.

[Table 1](#) compares each P&DC audited by work floor space (mail processing capacity), mail volume, and age. Total interior space reflects the space required for other facility functions.

¹ Source: U.S. Postal Service Newsroom, Frequently Asked Questions for Phase 2 Network Rationalization, January 2014.

² A central mail facility that distributes and dispatches incoming and outgoing mail for a designated service area and provides instructions on preparing collection mail, dispatch schedules, and sorting plan requirements to mailers. Processing and distribution facilities, which are similar in operation but not in scale to a P&DC, were not included.

Table 1: P&DCs Audited by Postal Service Area

Facility Name/Area	Work Floor Space/ Interior Space (Footage)	Mail Processing Volume (FY 2018) (billion pieces)	Age (Years)	Additional Facility Functions	IT Resources
██████████ Capital Metro	341,889/860,334	3.1	47	Credit Union; Retail; Administrative offices; Business Mail Entry Unit (BMEU)	██████████ ██████████
██████████ Northeast	715,132/1,233,935	3.2	83	Retail Store; Administrative Offices; BMEU	██████████ ██████████
██████████ Western	608,572/630,806	5.2	28	Retail Store; Administrative offices; BMEU	██████████ ██████████
██████████ ██████████ Pacific	305,000/710,000	3.8	25	Vehicle Maintenance Facility; Retail Store; Administrative Offices	██████████ ██████████

Source: 2019 Facilities Inventory and Mail Variance Program.

To better control facility access, the Postal Service implemented the ██████████ ██████████ in 2009. This badge access system was designed to ensure standardized identification protocols (e.g., badge access cards) for granting access to facilities, while maintaining access records in a centralized national database. The Postal Service implemented ██████████ at 362 total sites, including P&DCs, at the end of 2018.

In FY 2012, the Postal Inspection Service implemented the Vulnerability Risk Assessment Tool (VRAT) as the single tool for identifying risks and vulnerabilities at postal facilities. The VRAT comprehensively assesses interior and exterior facility security conditions and these assessments are conducted by both Postal Inspection Service and Postal Service security personnel. Each deficiency identified during an assessment is assigned a priority level (high, medium, or low), which is a subjective determination based on the type of asset at risk and potential threats and vulnerabilities at each facility.

Summary of Physical and Environmental Controls Site Security Review Audits

Overall, the Postal Service has implemented effective physical security and environmental controls for the four sites visited because it uses a defense-in-depth strategy employing multiple layers of physical security controls. For example, a server room is protected by multiple layers of security to include:

However, we identified specific controls could be improved, including . We identified the following pervasive physical security issues at the four facilities visited:

-
-
- Perimeter controls were not effective. For example, employee entrance and dock doors were broken, or doors were intentionally altered to allow unimpeded employee access.
- Facilities had inoperable surveillance cameras.
- Employees did not challenge unauthorized individuals seeking access to secure areas.

“Overall, the Postal Service has implemented effective physical security and environmental controls for the four sites visited because it uses a defense-in-depth strategy employing multiple layers of physical security controls.”

- Entrance gates were not operational or working properly.

Table 2 summarizes the physical controls not in compliance with Postal Service policy at the four facilities.

Table 2: Non-Compliant Physical Controls By P&DC

Physical Control Weakness				
Unauthorized access allowed to secure areas.				
Access to secure areas (IT and mail processing support server rooms) were not reviewed or restricted as required. ⁶	✓	✓	✓	✓
Access for separated employees was not removed.	✓	✓	✓	✓
Unidentified individuals were allowed unauthorized access to secure areas (Retail Store or BMEU).		✓	✓	✓
Perimeter controls were not effective:				
Entrance gates were not operational or not working properly.	✓		✓	✓
Employee entrance (ingress) or emergency (egress) and dock doors were not secure.	✓	✓	✓	✓
Closed Circuit TV (CCTV) cameras were not operational.	✓		✓	

Source: OIG analysis.

⁶ We identified the following employees with

Postal Service policy requires management and employees to establish and oversee access to controlled areas, manage employee separations, and keep perimeter control devices, such as gates and surveillance cameras operational. We cited the following Postal Service policies:

- Handbook AS-805, *Information Security*,⁷
- *Administrative Support Manual (ASM)* 13,⁸ and
- Handbook RE-5, *Building and Site Security Requirements*.⁹

These issues occurred because facility management did not [REDACTED] to the four facilities, and management [REDACTED]

Appendix B summarizes the specific cause for each issue by facility.

When the Postal Service does not review and update facility access, or perimeter controls, such as gates and surveillance cameras are not working properly, the risk increases for unauthorized access to critical IT and mail processing systems that process, transfer, and store data vital for business operations.

Overall, the Postal Service had sufficient environmental controls (e.g., fire detection, surge protection, and redundant power sources) in place to protect IT and mail processing servers and equipment. However, we identified two issues related to water damage and fire suppression controls at one area P&DC which have since been mitigated and the associated recommendation closed.

“Of the 26 physical and environmental security control recommendations directed at the four P&DCs, the Postal Service took corrective action for OIG to close 23.”

Recommendations and Management Corrective Actions

Of the 26 physical and environmental security control recommendations directed at the four P&DCs, the Postal Service took corrective action for OIG to close 23. Specifically, the Postal Service took corrective action during the Pacific, Capital Metro, and Northeast area audits and during this audit to address six issues related to unauthorized access to secure areas and ineffective perimeter controls. We recommended management improve 13 physical security controls and one environmental control to address weaknesses identified at the four facilities.

All recommendations for the Pacific, Capital Metro, and Northeast area P&DCs have been closed. We noted that Western area management has established an implementation date of August 31, 2019, for their open recommendations. Table 3 shows the status of all recommendations made at the four audited facilities by area.

Table 3: Status of Recommendations

Area	Recommendations		
	Total	Closed	Open
Pacific	8	8	0
Western	9	6	3
Capital Metro	5	5	0
Northeast	4	4	0
Total	26	23	3

Source: OIG analysis.

⁷ Handbook AS-805, *Information Security*, Sections 6-6.1 Routine Separations; 7.2.2, Establishment of Controlled Areas, 7-2.4, Establishment of Access Control Lists, 11-11.8.2, Physical Security Requirements, dated December 2018.

⁸ Sections 273.122, Door Locks; 273.123, Compliance; 273.131, Unauthorized Individuals; 273.451, Postal Service Keys and Access Control Cards, updated through October 30, 2018.

⁹ Sections 2-1.5 Access Control System at Mail Processing Facilities; 2-5.2, Security CCTV System; 4-1.2.1, Retail CCTV Standards.

Potential Physical Security Control Issues at Other Processing & Distribution Centers

Based on the similarity of the conditions identified at the four facilities we visited, we analyzed data for additional P&DCs that demonstrated physical security risks to IT assets may be similar at other facilities nationwide. We reviewed VRAT¹⁰ assessments and determined that [REDACTED] at [REDACTED] of 205 P&DCs. We also found indications at [REDACTED] P&DCs that designated administrators [REDACTED] in [REDACTED] as we found at the four facilities we visited.

Finding #1: Remediation of Vulnerability Risk Assessment Tool Deficiencies

Based on our review of VRAT assessments,¹² we identified potential physical security control conditions at [REDACTED]¹³ of 205 judgmentally selected P&DCs across the seven Postal Service areas. We found during our review of the four sites visited that facility management [REDACTED] and that could be the [REDACTED] P&DCs. Of the VRAT assessments we reviewed, deficiencies existed from assessments performed from December 22, 2017 to February 13, 2019. Specifically, the following are physical security control weaknesses identified by the VRAT:

- Secure areas may not be restricted;
- Separated employee access may not be removed;
- Unidentified individuals could enter secure areas (e.g., BMEU, server room, and retail store);

- Entrance gates may not be fully operational or unused;
- Employee entrance, exit, or dock doors may not be secure; and
- Video cameras may not be fully operational or may need upgrades.

The Postal Service [REDACTED] to address VRAT deficiencies. Postal Service IT assets become vulnerable to potential theft or breach when weaknesses are identified in physical security controls and are not addressed.

Recommendation #1

We recommend the **Chief Operating Officer** and **Executive Vice President** and the **Chief Postal Inspector** develop and implement [REDACTED] that requires management to follow-up on each physical security deficiency identified by the Vulnerability Risk Assessment Tool within a specified time frame.

Recommendation #2

We recommend the **Vice President, Information Technology** in coordination with the **Chief Postal Inspector** and the **Chief Operating Office** and **Executive Vice-President**, revise the Administrative Support Manual 13 to describe the [REDACTED] in response to Vulnerability Risk Assessment Tool deficiencies, including management roles and responsibilities.

¹⁰ Application that employees use to identify security risks at mail processing facilities.

¹² We downloaded VRAT assessment data on March 26, 2019.

¹³ We reviewed Tier 2 P&DCs, facilities where a loss of operations would have a detrimental effect on mail operations locally or affect area- or district-wide operations.

¹⁴ ASM 13, Section 271.341, Security Reviews.

Finding #2: Review of Facility Employee Access

Based on our analysis of the access lists at 22 P&DCs as shown in Table 4, we identified [REDACTED] and the number of employees working at the facilities based on the facility's official time and attendance records.¹⁷ While we did not perform an onsite review of the listed facilities, the data below suggest that [REDACTED] to the facility as we found at the four facilities we visited.

Table 4: Analysis of Employee Access at Selected P&DCs

Area	Facility Name	[REDACTED]	[REDACTED]	[REDACTED]
Capital Metro	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Eastern	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Great Lakes	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Area	Facility Name	[REDACTED]	[REDACTED]	[REDACTED]
Northeast	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Pacific	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Southern	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Western	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Source: [REDACTED] facility door reports, from April to May 2019 and [REDACTED] Employee Listing Reports, as of April 2019.

While Postal Service policy requires semiannual reviews of facility access lists,¹⁹ P&DC management at the sites we visited [REDACTED]. In addition, these differences could occur as a result of [REDACTED] employees because [REDACTED] is not integrated with the [REDACTED] System. Further, best practices²⁰ recommend that physical access control systems be integrated when

15 [REDACTED]

17 For this report, we are referring to [REDACTED], which collects employee hours and attendance for payroll processing.

18 [REDACTED]

19 Handbook AS-805, Section 7-2.4, Establishment of Access Control Lists.

20 Gartner, *Technology Insight for Physical Access Control Systems (PACS)*, September 21, 2016. The article was revalidated on July 20, 2019 by Nick Ingelbrecht, Research Director - Gartner.

“Postal Service management stated it would be feasible to develop and review

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ”

feasible with a human resource system of record (HRSOR). [REDACTED]

We brought this to the attention of Postal Service management, and they stated it would not be cost effective at this time to integrate [REDACTED] with the HRSOR. However, Postal Service management stated it would be feasible to develop and review an [REDACTED]

In addition, we identified employees who may have inappropriate access based on our analysis of 29 [REDACTED]

computer room employee lists and identified job titles of employees who may have questionable access. For example, we identified four secretaries, two clerk vehicle dispatchers,²¹ and an office clerk for vehicle operations²² with access to the IT and mail processing server rooms. [Table 6 in Appendix C](#) shows the results of our analysis of questionable employee access to computer rooms.

Postal Service policy²³ requires management to update access control lists when assigning new personnel to the secure area or when someone leaves. Based on our previous work, this occurred because P&DC managers [REDACTED]

[REDACTED] When [REDACTED] lists are not reviewed for proper access, the risk that unauthorized personnel would access IT assets increases. In addition, personnel not receiving the required technical and safety training could cause outages and impact the availability of Postal Service plant resources and even injury to untrained employees.

Recommendation #3

We recommend the **Chief Operating Officer and Executive Vice President** require the review of [REDACTED] access lists on a semiannual basis to remove unauthorized persons and limit access to secure areas for authorized employees.

Recommendation #4

We recommend the **Vice President, Information Technology**, in coordination with the **Chief Postal Inspector** and the **Chief Operating Officer and Executive Vice President** develop and review an [REDACTED]

²¹ The official title is “clerk vehicle dispatching.”

²² The official title is “office clerk vehicle operations.”

²³ Handbook AS-805, Sections 7-2.4, Establishment of Access Control Lists, 7-2.1 (a), Access to Controlled Areas.

Other Matters

Physical security must be implemented properly to prevent unauthorized personnel from gaining physical access. All the firewalls, cryptography, and other security measures would be useless if an intruder interrupted IT services, or stole, disclosed or destroyed data, including the equipment the data reside on. Physical security should always use a “defense-in-depth” approach to reinforce security through different controls.²⁴ Multiple security controls in place make it tougher for attackers to get to valuable IT resources.

The Postal Service uses a defense-in-depth approach to protect IT assets; however, to be effective, each component or layer must be operating as intended. Two of the physical controls used to ensure there is appropriate physical security are the [REDACTED] system and the VRAT assessment tool.

P&DC facilities using [REDACTED]

Facilities

Facilities managing [REDACTED]. We found that nine facilities did not have [REDACTED] implemented as the standard badge access system. Based on our work at the [REDACTED] we found that management was running [REDACTED]. We reported problems with excessive access. For example, 39 percent of facility individuals had access to the maintenance server room and 17 percent to the IT server room. In addition, [REDACTED] (48 percent) card readers [REDACTED] and management [REDACTED]

During our audit, management told us the [REDACTED]. Nine facilities are running badge systems [REDACTED]. Postal Service policy²⁵ states that facilities meeting the minimum size²⁶ must have an [REDACTED]

[REDACTED] We plan to make a referral to the OIG Supply Management and Facilities audit directorate.

Management's Comments

Management agreed with all of the findings and recommendations in the report.

Regarding recommendation 1, management stated they will enhance [REDACTED] process to review and address the physical security deficiencies identified through the VRAT by [REDACTED]

Regarding recommendation 2, management stated they will make the necessary changes identified in recommendation 1 to update the ASM 13 by [REDACTED]

Regarding recommendation 3, management stated they will reinforce the requirement to review the [REDACTED] access lists on a semiannual basis to remove unauthorized persons and limit access to secure areas. The target implementation date is [REDACTED]

Regarding recommendation 4, management stated they will [REDACTED]. The target implementation date is [REDACTED]. See [Appendix D](#) for management's comments in their entirety.

²⁴ SANS Institute white paper, The Importance of Physical Security.

²⁵ RE-5, Section 2-5.3, Access Control System.

²⁶ 60,000 SF or more.

Evaluation of Management's Comments

The OIG considers management's comments responsive to all recommendations in the report and the proposed corrective actions should resolve the issues identified in the report. All recommendations require OIG concurrence before closure. 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.....13
 - Scope and Methodology.....13
 - Prior Audit Coverage.....14
- Appendix B: Causes for Physical Security Control Issues ..15
- Appendix C: Analysis of Employee Access to Computer Rooms 16
- Appendix D: Management’s Comments.....18



Appendix A: Additional Information

Scope and Methodology

The scope of this audit was audit results of the physical and environmental controls site security reviews from the following P&DCs:

- [REDACTED] (Pacific Area)
- [REDACTED] (Western Area)
- [REDACTED] (Capital Metro Area)
- [REDACTED] (Northeast Area)

Additionally, as part of the scope, we identified additional P&DCs with a significant IT presence and with similar risk characteristics, as identified by VRAT assessments and differences between facility [REDACTED] main employee entrance and [REDACTED] personnel counts. We did not visit the [REDACTED] additional P&DCs nor did we interview any P&DC personnel to assess internal controls and obtain evidence.

To accomplish our objective, we:

- Reviewed and analyzed the physical and environmental control issues for the four site security reviews to identify common issues, trends, and causes.
- Summarized corrective actions and recommendations closed during and after the four reviews.
- Obtained and reviewed the latest VRAT Deficiency Report to identify similar issues and remediation efforts at other higher-risk P&DCs.
- Obtained the latest facilities inventory data to confirm addresses at other higher-risk facilities identified in the VRAT.

- Compared [REDACTED] employee main entrance door access lists to [REDACTED] employee data for selected facilities.
 - If available, obtained and reviewed [REDACTED] employee access lists for the IT and mail processing server rooms.
 - Determined if job titles indicated appropriate access to IT and mail processing server rooms.
- Identified possible physical security control issues from the combined data results that management could act on at other P&DCs.

We conducted this performance audit from April through August 2019, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary based upon the scope of our audit. 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. The evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective and scope. We discussed our observations and conclusions with management on July 12, 2019 and included their comments where appropriate.

We assessed the reliability of facilities inventory, VRAT assessment, [REDACTED], and Electronic Data Warehouse data by testing for completeness, reasonableness, accuracy, and validity. We also noted the original source data (manually input by a Postal Service employee, fed by another Postal Service system, and the Postal Service's overall reliance on the system) in making our assessment. 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
<i>Northeast Area Environmental and Physical Controls Site Summary Review</i>	Determine whether the Postal Service established and implemented effective environmental and physical security controls according to Postal Service policy at the [REDACTED] P&DC.	IT-AR-19-003	1/31/2019	None
<i>Capital Metro Physical and Environmental Controls Site Security Review</i>	Determine whether the Postal Service established and implemented effective physical and environmental security controls according to policy at the [REDACTED] P&DC.	IT-AR-18-005	9/28/2018	None
<i>Western Area Physical Security and Environmental Controls</i>	Determine whether the Postal Service has implemented effective physical security and environmental and wireless access controls according to policy and industry best practices at the [REDACTED] P&DC.	IT-AR-18-002	3/19/2018	None
<i>Facility Security at Network Distribution Centers</i>	Determine whether the Postal Service effectively addressed security deficiencies at NDCs to enhance the safety and security of the work environment.	HR-AR-18-001	12/28/2017	None
<i>Pacific Area Processing and Distribution Center Physical and Environmental Security Controls</i>	Determine whether the Postal Service has adequate and effective physical and environmental security controls at the [REDACTED].	IT-AR-17-005	5/3/2017	None

Appendix B: Causes for Physical Security Control Issues

Table 5: Causes for Physical Security Control Issues By P&DC

Causes for Physical Security Weaknesses	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
<i>Facility access was not reviewed or updated, or was limited</i>				
Was not aware of semiannual badge access review requirement or did not assign individual managers to approve and review badge access to secure areas.	✓	✓	✓	✓
Human Resources manager or employees was not aware of, did not have, or did not follow procedures for removing separated employees.	✓		✓	✓
Retail and BMEU employees were not aware of the policy for challenging and escorting unauthorized individuals, or expected to see unfamiliar individuals in secure areas, or they believed the unidentified individual worked in the mail processing plant and needed to use the BMEU facility.	✓	✓	✓	✓
<i>Facility management did not keep perimeter controls operational due to [REDACTED]</i>				
Gates did not operate properly because				
<ul style="list-style-type: none"> Gate sensor at employee entrance did not function properly; Management instructed employees to open truck entrance gate upon driver arrival without verifying identification; or Budget constraints prevented facility management from repairing the parking lot gates. 	✓	✓	✓	
Employee entrance (ingress), emergency (egress), and dock doors did operate properly because:				
<ul style="list-style-type: none"> Employees intentionally altered entrance and dock doors (rocks, zip ties, screws, and seat belts) to allow contract drivers and employees access; Management was not aware of broken door locks; Motion detectors did not operate properly; or Management did not perform adequate oversight. 	✓	✓	✓	✓
[REDACTED] prevented facility management from repairing the [REDACTED].		✓	✓	

Source: OIG analysis.

Appendix C: Analysis of Employee Access to Computer Rooms

Table 6: Employees with Questionable Access to Computer Rooms at Selected P&DCs

P&DC	Total Access	Questionable Access	Total Access	Questionable Access	Total Access	Questionable Access	Total Access	Questionable Access
[REDACTED]	29	7	N/A	N/A	N/A	N/A	29	23
[REDACTED]	16	2	N/A	N/A	N/A	N/A	N/A	N/A
[REDACTED]	77	18	N/A	N/A	N/A	N/A	77	56
[REDACTED]	32	6	N/A	N/A	23	6	22	6
[REDACTED]	21	5	N/A	N/A	N/A	N/A	N/A	N/A
[REDACTED]	19	4	N/A	N/A	N/A	N/A	N/A	N/A
[REDACTED]	16	2	N/A	N/A	N/A	N/A	16	11
[REDACTED]	36	7	N/A	N/A	N/A	N/A	N/A	N/A
[REDACTED]	N/A	N/A	8	2	N/A	N/A	N/A	N/A
[REDACTED]	15	1	N/A	N/A	N/A	N/A	19	14
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	9	7
[REDACTED]	31	5	N/A	N/A	N/A	N/A	27	18
[REDACTED]	17	5	N/A	N/A	N/A	N/A	17	14
[REDACTED]	N/A	N/A	N/A	N/A	N/A	N/A	6	5
[REDACTED]	26	6	N/A	N/A	23	6	N/A	N/A
[REDACTED]d	N/A	N/A	N/A	N/A	N/A	N/A	35	10

P&DC	Total Access	Questionable Access	Total Access	Questionable Access	Total Access	Questionable Access	Total Access	Questionable Access
	33	5	N/A	N/A	N/A	N/A	25	16
	17	4	N/A	N/A	N/A	N/A	N/A	N/A
	N/A	N/A	N/A	N/A	N/A	N/A	25	18
Total	385	77	8	2	46	12	307	198

Source: [redacted] computer room door reports, from April to May 2019.

IPSS, TMS, and Admin Questionable Access³⁰ include these jobs:

1. Clerk, Vehicle Dispatching
2. Office Clerk, Vehicle Operations
3. Secretary

Computer/IS Questionable Access³¹ include the following jobs:

1. Maintenance Support Clerk
2. Clerk Vehicle Dispatching
3. Office Clerk, Vehicle Operations
4. Secretary

³⁰ The description of the jobs listed under IPSS, TMS, and Admin may not warrant access to the servers that control the mail operations system.

³¹ The description of the jobs above may not warrant access to the servers that connect the facility to the Postal Service network.

Appendix D: Management's Comments



August 7, 2019

LAZERICK POLAND
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Physical and Environmental Controls Site Security Review – Summary
Report (Report Number IT-AR-19-DRAFT)

Thank you for the opportunity to review and comment on the above referenced audit,
Physical and Environmental Controls Site Security Review – Summary.

Management agrees with the findings of the audit and addresses our disposition of
each recommendation below.

Recommendation 1:

We recommend the Chief Operating Officer and Executive Vice President and the
Chief Postal Inspector develop and implement a [REDACTED] that requires
management to follow-up on each physical security deficiency identified by the
Vulnerability Risk Assessment Tool within a specified time frame.

Management Response/Action Plan:

Management agrees with this recommendation. The Chief Postal Inspector will
coordinate with the Chief Operating Officer and Executive Vice President to enhance
a [REDACTED] to review and address the physical security deficiencies
identified through the Vulnerability Risk Assessment Tool within a specified time
frame.

Target Implementation Date:

[REDACTED]

Responsible Official:

Chief Operating Officer and Executive Vice President and Chief Postal Inspector

475 L'Enfant Plaza SW
Washington, DC 20260
www.usps.com

Recommendation 2:

We recommend the Vice President, Information Technology in coordination with the Chief Postal Inspector and the Chief Operating Office and Executive Vice President, revise the *Administrative Support Manual 13* to describe the [REDACTED] in response to Vulnerability Risk Assessment Tool deficiencies, including management roles and responsibilities.

Management Response/Action Plan:

Management agrees with this recommendation. The Vice President, Information Technology will collaborate with the Chief Postal Inspector, the Chief Operating Officer and Executive VP and the Office of Brand and Policy to make the necessary changes identified in Recommendation #1 to the ASM-13.

Target Implementation Date:

[REDACTED]

Responsible Official:

Vice President, Information Technology

Recommendation 3:

We recommend the Chief Operating Officer and Executive Vice President require the review of [REDACTED] on a semiannual basis to remove unauthorized persons and limit access to secure areas for authorized employees.

Management Response/Action Plan:

Management agrees with this recommendation. The Chief Operating Officer and Executive Vice President will reinforce the requirement of each Area to review the [REDACTED] on a semiannual basis, to include removing unauthorized persons and limiting access to secure areas for authorized employees.

Target Implementation Date:

[REDACTED]

Responsible Official:

Chief Operating Officer and Executive Vice President

Recommendation 4:

We recommend the Vice President, Information Technology, in coordination with the Chief Postal Inspector and the Chief Operating Officer and Executive Vice President develop and review an exception report semiannually that would use data from the

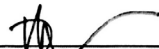
Management Response/Action Plan:

Management agrees with this recommendation. The Vice President, Information Technology, in coordination with the Chief Postal Inspector and the Chief Operating Officer and Executive Vice President

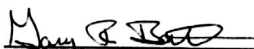
Target Implementation Date:

Responsible Official:

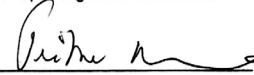
Vice President, Information Technology



David E. Williams
Chief Operating Officer and Executive VP



Gary R. Barksdale
Chief Postal Inspector



Pritha N. Mehra
Vice President, Information Technology

cc: *Manager, Corporate Audit Response Management*



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

For media inquiries, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov