Office of Inspector General | United States Postal Service

Audit Report

Capital Metro Physical and Environmental Controls Site Security Review

Report Number IT-AR-18-005 | September 28, 2018

Table of Contents

Highlights

Objective

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

"Our objective was to determine whether the U.S. Postal Service established and implemented effective physical and environmental security controls according to Postal Service policy at the [redacted] 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 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 [redacted] P&DC is 860,334 square feet and processes about 3 billion mailpieces annually. This facility includes a retail store, credit union, administrative offices, business mail entry unit, and U.S. Postal Inspection Service offices. We selected this site based on it being the [redacted] using U.S. Postal Service Office of Inspector General facility risk assessments.

What the OIG Found

We did not identify any environmental security issues at the [redacted] P&DC; however, the Postal Service did not have effective physical security controls.

We found that management did not restrict access to server rooms as required. Over 80 percent of facility employees on the server room access list no longer worked at the P&DC. This occurred because management was not aware of the requirement to do semiannual reviews of server room access control lists. Management took corrective action by removing 1,186 employees from the server room access lists.

In addition, management did not have out-processing procedures to ensure removal of facility access for separated employees. Management took corrective action and started drafting out-processing procedures to address this requirement.

Additionally, during our site visit we found the entrance door to a server room containing critical mail operations servers did not lock and critical system information (e.g., Internet Protocol addresses) was posted on equipment and on a server room wall. These issues occurred because management was unaware that the lock on the server room door was broken and there were risks associated with posting critical system information on walls and computers in the server room. We also observed physical access controls that allowed unauthorized access to the facility and critical assets. Specifically, we found weaknesses in the following areas:

- Vehicle entrance gates remained open 24/7 without being monitored and did not have traffic arms, computerized card access systems, intercoms or functioning closed-circuit television (CCTV) cameras. This allows unauthorized individuals to enter the plant through the loading docks, gaining access to the facility and the server rooms.
- Motion detectors routinely opened the unlocked overhead dock doors, allowing access to the facility.
- Four entrance doors in the dock areas were unlocked during our site visit, allowing unauthorized access to server rooms and mail workroom floors.
- Facility employees did not visibly display Postal Service identification badges while working at the facility.

- Video surveillance cameras were not operating properly. Specifically:
  - Of the 82 CCTV video surveillance cameras, 23 (28 percent) were not operational and 11 (13 percent) displayed unrecognizable images.
  - In the retail counter area, of the eight video surveillance cameras, only one was working to cover five retail positions.

This occurred due to a lack of management oversight of the physical security at the facility and an enforcement of policy. According to management, budget constraints prevented them from upgrading the gates and CCTV cameras. Additionally, management did not enforce the policy requiring employees to wear identification badges while in the facility.

Lastly, we found that an individual with administrative privileges to the facility access system shared their logon identification and passwords with other personnel. This occurred because management did not designate an alternate administrator in the office to grant access to controlled areas at the [redacted] P&DC.

Management took corrective action and instructed employees not to share their passwords and reset all office personnel Enterprise Physical Access Control System (ePACS) passwords. Management also assigned an alternate with appropriate ePACS access to grant access to controlled areas; therefore, we are not making any recommendations for this finding.

Improperly implemented physical security controls increase the risk of theft or disruption of critical operations and unauthorized access to the facility and Postal Service assets.

What the OIG Recommended

We recommended management:

- Review server room access control lists semiannually; and finalize, publish, and implement out-processing procedures, to include disabling badges for separating employees.
- Replace the lock on the server room entrance door and ensure it functions properly and remove all posted critical systems information from the server room.
- Ensure entrance gates are monitored and have traffic arms, computerized card access systems, and intercoms installed at entrance gates.
- Verify all dock and entrance doors are locked when not in use, entrance door locks are replaced, and employees wear and display Postal Service identification badges at all times.
- Complete the capital project to replace non-operational CCTV cameras and those that display unrecognizable images and install CCTV cameras in the retail area in accordance with Postal Service policy.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 28, 2018

MEMORANDUM FOR: TOM SAMRA
VICE PRESIDENT, FACILITIES

DANE A. COLEMAN
DISTRICT MANAGER, [redacted] DISTRICT

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskto

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

SUBJECT: Audit Report – Capital Metro Physical and Environmental Controls Site Security Review (Report Number IT-AR-18-005)

This report presents the results of our audit of U.S. Postal Service Capital Metro Physical and Environmental Controls Site Security Review (Project Number 18TG010IT000).

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, Capital Metro Area
Chief Postal Inspector

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's Capital Metro Physical and Environmental Controls Site Security Review (Project Number 18TJ010IT000). Our objective was to determine whether the Postal Service established and implemented effective physical and environmental security controls according to Postal Service policy at the [redacted] Processing and Distribution Center (P&DC).

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 security measures to protect assets from loss or damage. These physical and environmental security measures include guards, gates, locks, access control cards, fire alarms, suppression systems, and uninterrupted power supplies.

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

> *"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 [redacted] P&DC is about 860,334 square feet and processes about 3 billion mailpieces annually. The [redacted] P&DC has IT, National Directory Support System[1]/Image Processing Subsystem[2] (NDSS/IPSS), and Tray Management System (TMS)[3] server rooms containing 150 servers. In addition to the P&DC, the facility also includes a retail store, credit union, [redacted] District Administrative Offices, business mail entry unit (BMEU),[4] and Postal Inspection Service offices.

Finding #1: Server Room Access Management

Facility management did not restrict access to the server rooms[5] containing information technology assets. Specifically, we found that:

"Facility management did not restrict access to the server rooms containing information technology assets."

- Access to the server rooms was excessive; 794 employees were given access to the NDSS/IPSS server room and 814 employees were given access to the TMS server room. For example, we identified mail carriers, custodians, and tractor trailer operators who had access to the server rooms.
- Of the 794 employees, 647 (81 percent) on the NDSS/IPSS server room access list[6] and 723 of the 814 (89 percent) on the TMS server room access list were not listed as active employees at the facility.

Postal Service policy[7] states that each controlled area must establish an access control list that is updated when new personnel are assigned to the controlled area or when someone leaves. Access control lists must also be reviewed and updated semiannually.

This occurred because facility management was not aware of the requirement to review access lists semiannually. Management took corrective action by removing 583 employees from the NDSS/IPSS and 603 employees from the TMS server room access lists. Additionally, management stated that they did not have out-processing procedures to ensure they remove facility access for separated employees.

When Postal Service management does not review, update, and limit server room access there is an increased risk of individuals gaining unauthorized access to critical IT systems, server rooms, and mail processing equipment. Unauthorized access may result in individuals disrupting the TMS or NDSS/IPSS systems, which automate movement of mail and packages throughout the facility. These systems are critical to mail processing operations at the facility. During the audit, management took corrective action and began to draft out-processing procedures for the facility to address this requirement.

Recommendation #1

The [redacted] **District Manager** review server room access control lists semiannually as required by Postal Service policy; and finalize, publish, and implement employee out-processing procedures, to include disabling badges for separating employees.

Finding #2: Unsecured TMS Server Room

During our site visit, we found that the entrance door to the TMS server room did not lock and 70 Internet Protocol (IP) addresses[8] were posted on equipment and a server room wall. Video 1 shows the TMS server room door not locking. Postal Service policy states physical and administrative security controls must be

1 A database designed to support various Postal Service mail processing automation systems.
2 Used to collect, store, and process images captured during mail processing.
3 An automated tray handling system intended to provide tray delivery to support mail processing operations and short-term tray storage, as needed, at Postal Service P&DCs.
4 The function of a BMEU is to accept, verify, and prepare properly paid bulk mail for movement to dispatch areas.
5 Rooms that are part of the controlled areas that may include computer rooms, telecommunications rooms, computer operations areas, and operating system software support areas.
6 On June 5, 2018, we obtained a list from the Enterprise Physical Access Control System (ePACS) system, which manages identification (ID) badges and is used to secure Postal Service facilities for each of the server rooms.
7 Handbook AS-805, *Information Security*, Section 7-2.2, Establishment of Controlled Areas.
8 A unique string of numbers separated by periods that identifies each computer using the IP to communicate over a network.

implemented at each facility to protect against unauthorized personnel access and to protect the physical integrity of Postal Service information resources located at the facility.[9]

Figure 1: TMS Server Room Door

Source: U.S. Postal Service Office of Inspector General (OIG) recording, dated July 9, 2018.

These issues occurred because facility management was not aware that the lock on the server room door was broken and there were risks associated with displaying IP addresses in the server room. When the Postal Service does not implement proper physical security controls, there is an increased risk of unauthorized access to TMS servers that control flat sorting, parcel sorting, and mail tray transport throughout the [redacted] P&DC.

Recommendation #2

The [redacted] **District Manager** replace the lock on the Tray Management System (TMS) server room entrance door and make sure that it functions properly, and remove all posted Internet Protocol addresses from the TMS server room.

Finding #3: Physical Access Control Weaknesses

During our site visit, we observed physical access controls that allowed unauthorized access to the facility and critical assets. Specifically, we found weaknesses in the following areas:

"During our site visit, we observed physical access controls that allowed unauthorized access to the facility and critical assets."

- **Vehicle Entrance Gates**. The east and west vehicle entrance gates remained open 24/7 without being monitored; and did not have traffic arms, computerized card access systems, intercoms, or functioning closed-circuit television (CCTV)[10] cameras as shown in the east and west vehicle entrance gate photos below. This allows unauthorized individuals to enter the facility through the loading docks gaining access to the facility, workroom floors, and the server rooms.[11] Postal Service policy states that facility entrance gates should have traffic arms, computerized card access systems, intercoms, and CCTV cameras.[12]

9 Handbook AS-805, Section 7-1, Physical and Environmental Security.
10 CCTV can produce images or recordings for surveillance or other private purposes.
11 Information Technology, TMS, and NDSS/IPSS server rooms.
12 Handbook RE-5, *Building and Site Security Requirements*, dated September 2009, 2-1.5, Access Control System at Mail Processing Facilities.

Figure 2. East Vehicle Entrance Gate

Figure 3. West Vehicle Entrance Gate

Source: OIG photographs taken July 9, 2018.

- **Motion Detectors.** Motion detectors routinely opened the unlocked overhead dock doors, allowing unauthorized personnel access to the facility, the server rooms, and mail workroom floors. Postal Service policy states that automatic doors are required to have locking mechanisms.
- **Entrance Doors.** Four entrance doors in the east and west docking areas were unlocked during our site visit, allowing unauthorized access to the facility, the server rooms, and mail workroom floors. Postal Service policy[13] states the entrance doors should be locked at all times; however, exceptions may be granted during heavy traffic periods when employees are reporting to or departing from work.
- **ID Badges.** Facility employees did not visibly display Postal Service ID badges while working at the facility during our site visits. Postal Service policy states that all personnel are responsible for displaying proper ID while at any facility that provides access to Postal Service information resources.[14]
- **Video Surveillance Cameras.** Video surveillance cameras were not operating properly. Specifically, we found that:
  - Of the 82 CCTV video surveillance cameras, 23 (28 percent) were not operational and 11 (13 percent) displayed unrecognizable images of personnel, vehicles, and license plate numbers. Postal Service policy states the CCTV system must cover all pedestrian and vehicle entries into the site and all employee entries into the facility. Additionally, Postal Service policy specifies that the camera's lens configuration must be able to provide identifiable personnel images and read license plate numbers.[15]

13 Handbook ASM-13, *Administrative Support Manual*, Sections 273.122 and 273.123, Door Locks and Compliance
14 Handbook AS-805, Section 2-2.33, All Personnel.
15 Handbook RE-5, *Building and Site Security Requirements*, 2-5.2 Security CCTV System, dated September 2009.

- In the retail counter area, we observed that of the eight video surveillance cameras, only one was functioning to cover the five full-service retail positions. Postal Service policy requires one CCTV camera for every two full-service retail positions.[16]

This occurred due to a lack of management oversight of the physical security at the facility and an enforcement of policy. Management stated that budget constraints prevented them from installing traffic arms, card access systems, and intercoms at the entrance gates. In addition, the entrance door locks were broken, and a badge access reader was not working; and they did not enforce the policy requiring employees to wear ID badges while at the facility. In the retail area, management did not contract to install the eight CCTV cameras that were purchased over a year ago.

Management recognizes that non-operational CCTV cameras and cameras displaying unrecognizable images require attention and have a camera replacement project planned for fiscal year (FY) 2019.

Without adequate physical security measures such as traffic arms, card access systems, intercoms, and video surveillance cameras, there is an increased risk of unauthorized individuals gaining access to IT assets and disrupting critical operations. Additionally, when employees bypass physical security, there is an increased risk of unintentional loss or impairment of critical assets, such as the TMS and NDSS/IPSS servers.

Recommendation #3

The [redacted] **District Manager** ensure entrance gates are monitored and have traffic arms, computerized card access systems, and intercoms are installed at the entrance gates.

Recommendation #4

The [redacted] **District Manager** verify that all dock doors are locked when not in use, entrance door locks are replaced, and employees wear and display Postal Service identification badges at all times while at the facility.

Recommendation #5

The **Vice President, Facilities,** complete the capital project to replace the closed-circuit television cameras that were non-operational or displayed unrecognizable images, and install the cameras in the retail area in accordance with Postal Service policy.

Finding #4: Shared Administrative Account Credentials

We found that an individual with administrative privileges in ePACS[17] shared their log-on IDs and passwords with other facility personnel. Personnel with administrative privileges in ePACS are responsible for issuing Postal Service employee badges and granting access to controlled areas at the [redacted] P&DC. Postal Service policy[18] prohibits an individual from sharing their account, log-on ID, password, personal information number, and token with another individual.

16 Handbook RE-5, 4-1.2.1 Retail CCTV Standards.
17 The system that manages identification badges and secures Postal Service facilities.
18 Handbook AS-805, Section 2-2.23g, Security Roles and Responsibilities.

This occurred because management did not designate an alternate ePACS administrator at the facility to grant access to controlled areas at the [redacted] P&DC. When employees share account credentials, the Postal Service is unable to authenticate who accessed data, track network activity, or identify the source of errors or suspicious activity.

Management took corrective action and informed employees not to share their passwords and reset all office personnel ePACS passwords and assigned an alternate with the appropriate ePACS access to grant access to controlled areas. Therefore, we are not making any recommendations for this finding.

Management's Comment

Management generally agreed with the findings and recommendations in the report except one recommendation.

Regarding recommendation 1, management agreed to implement out-processing procedures and conduct semiannual reviews of server room access. The target implementation date is October 31, 2018.

Regarding recommendation 2, management agreed to repair and verify that the lock for the server room is working properly and stated they have removed the IP addresses in the server room. The target implementation date is September 30, 2018.

Regarding recommendation 3, management did not agree to monitor entrance gates, install traffic arms and intercoms, and grant computerized card access. Management has also requested that we close this recommendation because they have deemed it physically infeasible to install the equipment required. There is no target implementation date.

Regarding recommendation 4, management agreed to repair the dock doors and replace the entrance door locks. Management has also reissued to the entire district the postal policy on wearing and displaying ID badges when at the facility. The target implementation date is September 2018.

Regarding recommendation 5, management agreed to replace CCTV cameras that were non-operational or displayed unrecognizable images. Management requested we close this recommendation because they will implement a project to ensure all cameras are functioning and implement actions in accordance with RE-5 guidelines by August 2019.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 2, and 4 and the corrective actions should resolve the issues identified in the report.

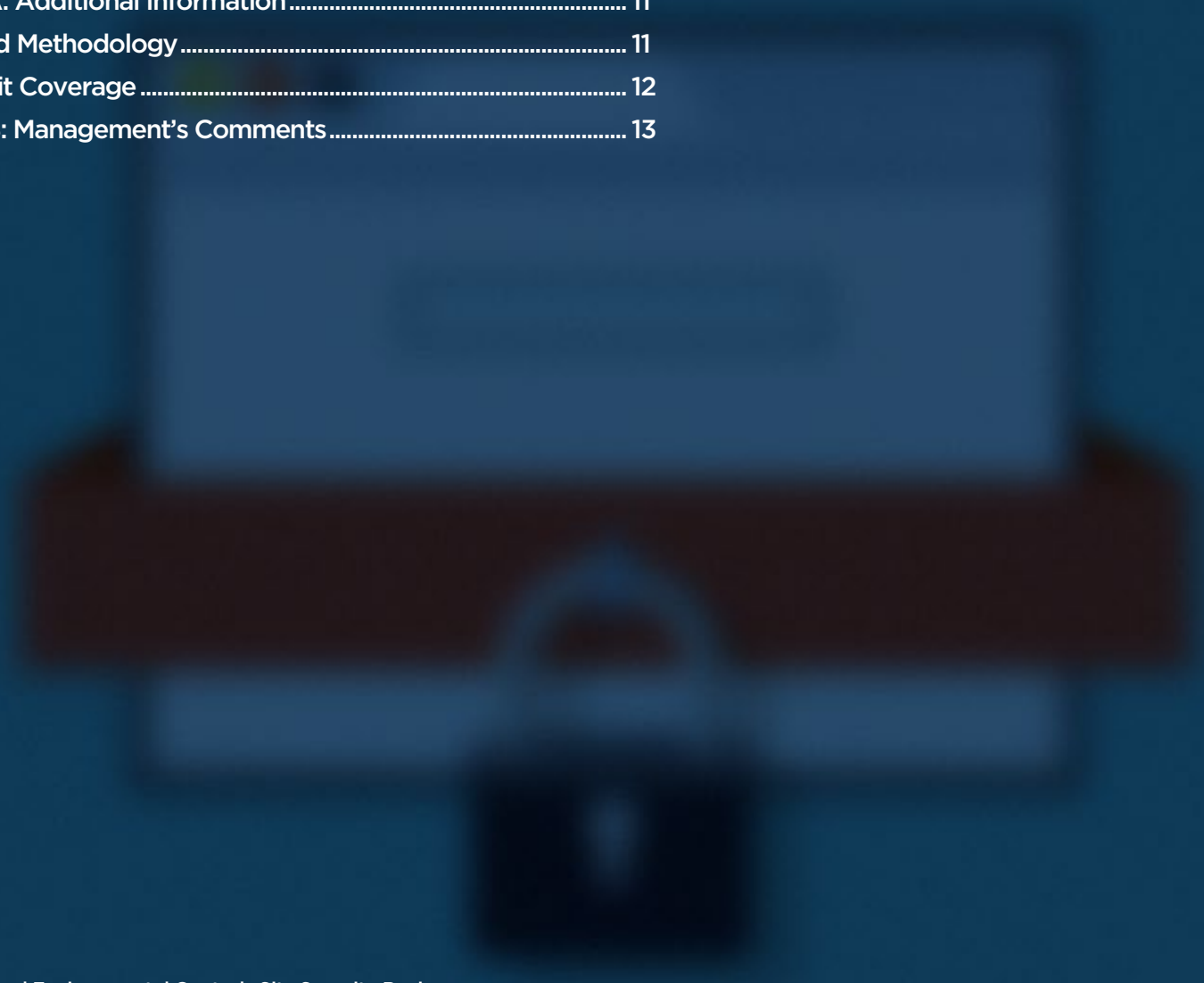
Regarding recommendation 3, management stated that an architectural engineering firm found the requirements outlined in our recommendation physically infeasible. For this recommendation to be officially closed, management should provide supporting documentation demonstrating that they have formally accepted the risk of noncompliance with Postal Service policy.

Regarding recommendation 5, management requested closure of this recommendation with the issuance of this report. The recommendation will remain open until replacement of the CCTV cameras is completed.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 3 and 5 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 and environmental security policies, processes, and controls in place to protect the [redacted] P&DC's mail processing equipment, IT resources, and personnel.

To accomplish our objective, we:

- Obtained data for the Postal Service's Capital Metro district from the OIG's FY 2018, Quarter 2 Performance and Results Information System Facilities Risk Model[19] to identify the [redacted] P&DC as our selected site. The [redacted] P&DC — ranked [redacted] and also with the Postal Service listed responsible for maintenance — had an occupied date prior to 1990 and had co-located Postal Service services.
- Reviewed Postal Service physical security policies, processes, and procedures to gain an understanding of the environment, and the most recent Postal Service Vulnerability and Risk Assessment Tool[20] to identify controlled areas and critical resources.
- Analyzed all security and access control devices used to secure the facility (e.g., Access Control System, CCTV System).
- Determined if badge access, identification cards, smartcards, passkeys, and other entry devices were controlled and monitored.
- Compared a facility server room employee list from ePACS and an active facility employees list from WebCOINS[21] to validate the appropriateness of employee access to the server rooms.
- Observed and assessed the effectiveness of perimeter security procedures for controlling access to the facility.
- Determined that emergency management procedures existed for the facility and interviewed safety managers to confirm the procedures.
- Verified that appropriate environmental controls are in place to protect facility personnel, equipment, and IT resources.

We conducted this performance audit from May through September 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 August 31, 2018, and included their comments where appropriate.

We assessed the reliability of data from the ePACS system by reviewing two listings of personnel with access to the [redacted] P&DC facility and server rooms and comparing that to a listing of active personnel retrieved from WebCOINS. In addition, we interviewed agency officials knowledgeable about the data and process and reviewed required security controls. We determined that the data were sufficiently reliable for the purposes of this report.

19 Identified and measured at risk districts that could affect the facilities ability to provide facility services.
20 Identifies facility security risks and track the progress of improvements.
21 Obtained from the Postal Service's Complement Information System (WebCOINS) Human Resource System, which provides local management with timely and accurate complement information.

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
Western Area Physical Security and Environmental Controls	Determine whether the Postal Service has implemented effective physical security and environment and wireless access controls according to policy and industry best practices at the [redacted] P&DC.	IT-AR-18-002	3/19/2018	None

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

September 20, 2018

Monique Colter
Director Audit Operations
Office of Inspector General
United States Postal Service

Subject: Response to Draft Audit Report – Capital Metro Physical Environmental Controls Site Security Review, Report Number IT-AR-18-DRAFT

Thank you for the opportunity to respond to the OIG Audit of Capital Metro Physical Environmental Controls Site Security Review. Management does agree with the findings noted in the audit report. Management also agrees with the recommendations as outlined in the audit with the exception of one recommendation as the implementation of the recommendation was found to be infeasible.

Recommendation #1

We recommend the [redacted] District Manager review server room access control lists semiannually as required by Postal Service policy; and finalize, publish, and implement employee out-processing procedures, to include disabling badges for separating employees.

Management Response/ Action Plan

Management agrees with this recommendation and has implemented by already removing 583 employees from the NDSS/ IPSS server room access lists. Management is drafting procedures and will conduct a semi-annual review starting at the beginning of the fiscal year and then on a semi-annual basis.

Target Implementation Date

October 2018

Responsible Official

Manager, Human Resources

Recommendation #2

We recommend the [redacted] District Manager replace the lock on the Tray Management System (TMS) server room entrance door and make sure that it functions properly, and remove all posted Internet Protocol addresses from the TMS server room.

Management Response/ Action Plan

Management agrees with this recommendation and has implemented by already removing the IP addresses and the lock has been repaired and verified to be operating properly.

Target Implementation Date

September 2018

Responsible Official

Manager, Maintenance

Recommendation #3

We recommend the [redacted] District Manager ensure entrance gates are monitored and have traffic arms, computerized card access systems, and intercoms are installed at the entrance gates.

Management Response/ Action Plan

Management disagrees with this recommendation. The services of an architectural engineering firm were utilized to review existing site conditions to determine if access controls could be physically accommodated. Review of the existing site has found it physically infeasible to install the necessary equipment required as outlined in this recommendation. The current transportation needs and space constraints prohibit implementation and thus management requests closure of this recommendation.

Recommendation #4

We recommend the [redacted] District Manager verify that all dock doors are locked when not in use, entrance door locks are replaced, and employees wear and display Postal Service identification badges at all times while at the facility.

Management Response/ Action Plan

Management agrees with this recommendation and has implemented by having all managers, maintenance operations, on each tour verify the doors are secured and in good condition and take action to affect repair as needed. Entrance door locks have been replaced. Management has reissued a postal policy letter to the entire district regarding the requirement to wear and display a Postal Service identification badge at all times while at the facility.

Target Implementation Date

September 2018

Responsible Official

Manager, Maintenance
District Manager

Recommendation #5

We recommend the Vice President, Facilities complete the capital project to replace the closed-circuit television cameras that were non-operational or displayed unrecognizable images, and install the cameras in the retail area in accordance with Postal Service policy.

Management Response/ Action Plan

Management agrees with this recommendation and already has a project identified and initiated to address the closed-circuit television concerns with a scheduled project completion in August 2019. Management will ensure all cameras are functioning and implement actions in accordance with RE-5 guidelines. As this project is already being pursued, closure of this recommendation is requested.

Tom A. Samra
Vice President, Facilities

Dane Coleman
Baltimore District 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