OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Office of Inspector General | United States Postal Service

Audit Report

Facility Security at Network Distribution Centers

Report Number HR-AR-18-001 | December 28, 2017

Table of Contents

Highlights

Objective

Our objective was to determine whether the U.S. Postal Service effectively addressed security deficiencies at Network Distribution Centers (NDC) to enhance the safety and security of the work environment.

NDCs are highly mechanized Postal Service mail processing plants that distribute standard mail and provide package services. There are currently 21 NDCs nationwide and Inspection Service and Postal Service personnel are responsible for security at those locations. The Vulnerability Risk Assessment Tool (VRAT) is the application employees use to identify security risks and vulnerabilities at these facilities.

> *"We determined whether the Postal Service effectively addressed security deficiencies at NDCs to enhance the safety and security of the work environment."*

What the OIG Found

The Postal Service and Postal Inspection Service did not always effectively address and monitor security deficiencies at the 11 NDCs we assessed. Specifically:

- Security officials did not always timely address security deficiencies identified during VRAT assessments.
- Installation heads did not always monitor the status of identified deficiencies, to include tracking the progress of corrective actions taken and closing out deficiencies when resolved.
- Installation heads did not always provide deficiency status updates to security officials.

There were 139 security deficiencies identified on the VRAT assessments at the 11 NDCs we reviewed. Deficiencies included obstructed, damaged, or inoperable gates, fences, doors, locks, and closed circuit television systems.

In addition, security officials did not always conduct VRAT assessments at the prescribed frequencies. Further, the security assessment policy has not been updated to reflect the use of the VRAT assessment tool, which replaced the annual security survey in fiscal year 2012.

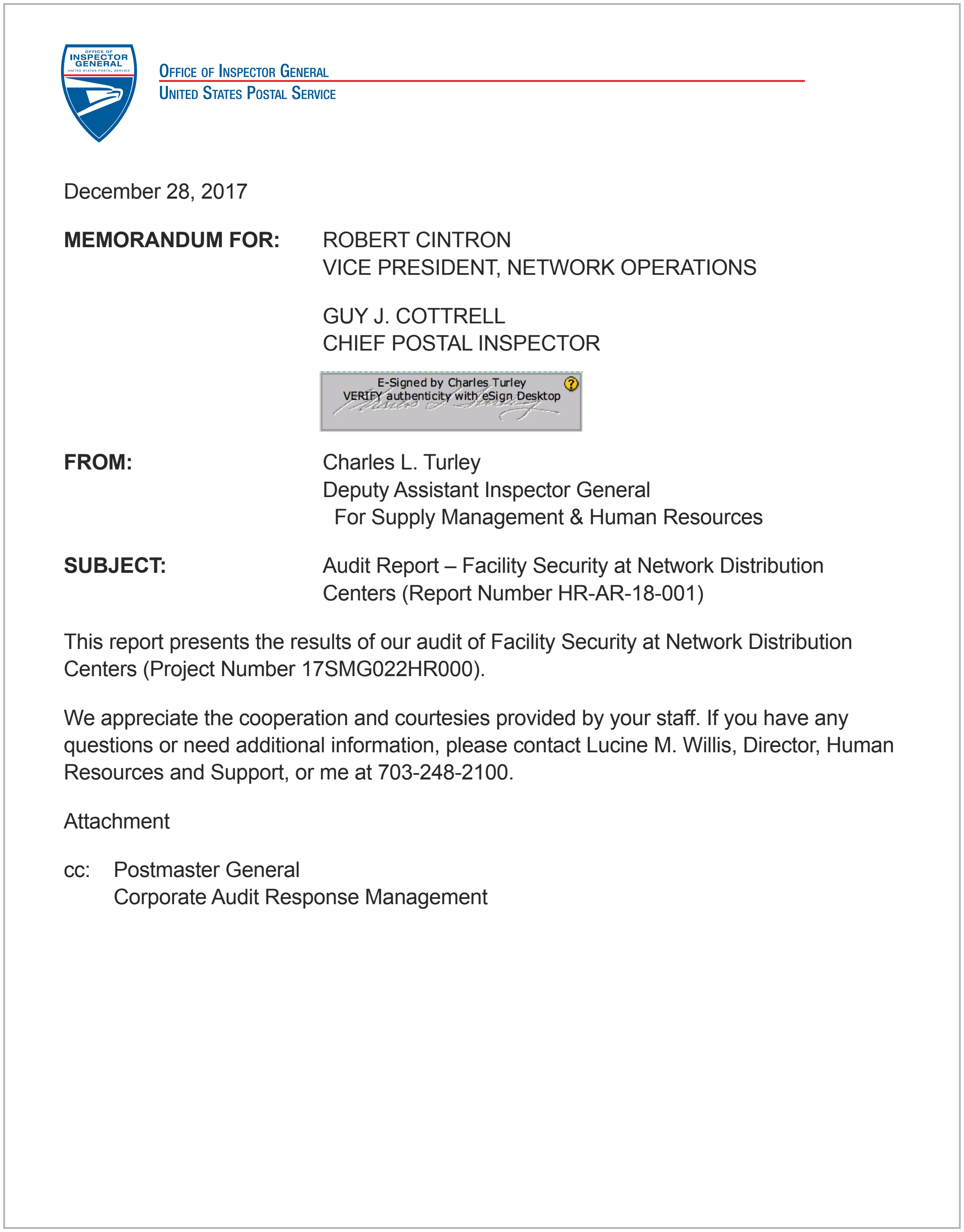
These conditions occurred because internal controls were not sufficient to ensure responsible security and area officials effectively addressed, monitored, and communicated security deficiencies or conducted VRAT assessments, as required.

When security deficiencies are not timely addressed or VRAT assessments are not conducted as required, there is an increased risk to the safety and security of Postal Service employees, customers, the mail, and other assets.

What the OIG Recommended

We recommended management establish standard operating procedures, to include timeframes, to address, monitor, and communicate identified security deficiencies. We also recommended management establish an oversight mechanism to promote accountability and ensure compliance with VRAT requirements and update policy to reference the VRAT assessment.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 28, 2017

MEMORANDUM FOR: ROBERT CINTRON
VICE PRESIDENT, NETWORK OPERATIONS

GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

E-Signed by Charles Turley
VERIFY authenticity with eSign Desktop

FROM: Charles L. Turley
Deputy Assistant Inspector General
For Supply Management & Human Resources

SUBJECT: Audit Report – Facility Security at Network Distribution Centers (Report Number HR-AR-18-001)

This report presents the results of our audit of Facility Security at Network Distribution Centers (Project Number 17SMG022HR000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Lucine M. Willis, Director, Human Resources and Support, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of Facility Security at Network Distribution Centers (NDC)[1] (Project Number 17SMG022HR000). We assessed 11 NDCs based on risk factors and concerns communicated by the American Postal Workers Union (APWU) regarding exterior facility security vulnerabilities.

Our objective was to determine whether the U.S. Postal Service effectively addressed security deficiencies at NDCs to enhance the safety and security of the work environment. See Appendix A for additional information about this audit.

> *"The Postal Inspection Service implemented the VRAT as the single tool for identifying risks and vulnerabilities at postal facilities. Each deficiency identified during an assessment is assigned a priority level (high, medium, or low)."*

Background

The chief postal inspector serves as the security officer for the Postal Service and is responsible for developing security policies and processes to protect Postal Service employees, mail, property, and assets. The Postal Inspection Service oversees facility security and provides training and guidance to responsible Postal Service personnel. Collectively, Postal Inspection Service and Postal Service personnel are responsible for facility security at NDCs (see Table 1).

In fiscal year 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 provides a comprehensive assessment of 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.

[1] An NDC is a highly mechanized U.S. Postal Service mail processing plant that distributes standard mail and package services in piece and bulk form. The Postal Service has 21 NDCs nationwide.

Table 1. Security Personnel

	Postal Inspection Service		Postal Service	
	Homeland Security Coordinator (HSC)	Physical Security Specialist (PSS)	Installation Head	Security Control Officer (SCO)
Location	Division	Division	NDC	NDC
Role	Oversees SCO program. Conducts performance reviews of SCOs. Provides feedback and guidance to SCOs.	Serves as Postal Inspection Service liaison to NDC management. Assesses and approves security-related requests for repairs and upgrades. Provides security guidance to assigned facilities.	Responsible for overall security of the facility, including the security and integrity of the mail, safety of employees, and all postal property entrusted to them. Implements facility security recommendations. Serves as SCO unless the role is delegated.	Serves as the focal point for identifying and addressing security concerns. Implements security policies. Coordinates with Postal Inspection Service on security matters.
VRAT Duties	Monitors completion of VRAT reviews.	Required to conduct VRAT reviews biennially and assign a priority level to identified deficiencies. Issues management letter to installation head summarizing VRAT results and recommendations. Contacts Facilities for security-related matters that cannot be performed at the facility.	Required to respond to PSS' VRAT management letters with an action plan within 30 days. Implements facility security recommendations. Determines whether security deficiencies can be addressed at the NDC or need Facilities support (contact PSS).	Required to conduct VRAT reviews annually and assign a priority level to identified deficiencies. Provides results to the installation head and Postal Inspection Service personnel, including the PSS and HSC.

Source: U.S. Postal Service Office of Inspector General (OIG) analysis.

Installation heads have the option of addressing security deficiencies using NDC maintenance personnel (in-house) or requesting Facilities[2] support.

> *"There were 139 interior and exterior deficiencies identified by VRAT category and priority level at the 11 NDCs we assessed."*

- For in-house repairs, NDC personnel use the [redacted] system, a centralized computer maintenance information system used to submit and track work orders for repairing or correcting all facilities issues, including those identified during VRAT reviews.
- For security-related projects that cannot be performed in-house, the NDC notifies the PSS to request Facilities support. The PSS assesses the deficiency and contacts the Facilities Single Source Provider (FSSP) to initiate the repair request. Facilities uses the [redacted] to log and route the request to appropriate personnel for action. Facilities has established performance goals[3] to ensure repairs are addressed.

There were 139 interior and exterior deficiencies identified by VRAT category and priority level at the 11 NDCs we assessed (see Table 2).

- **Gates and Fencing** – We found 33 deficiencies related to gates and fencing. Specifically, perimeter fencing with growth such as plants, foliage, trees, and shrubs obstructed clear views on both sides of the fence; and gates at vehicle entrance points remained open allowing unvetted entry. Other deficiencies included missing signage and inoperable lighting.
- **Doors and Locks** – We found 43 deficiencies related to doors and locks. Specifically, deficiencies included unsecured doors and locks that included pedestrian doors in dock areas that had been propped open, jammed, or broken. Other deficiencies related to unrestricted elevator access, maintenance of lookout galleries, and the location of security files and containers.
- **Access Control and Closed Circuit Television (CCTV)** – We found 52 deficiencies related to access control devices. Specifically, turnstiles and badge readers did not adequately prevent unauthorized access to Postal Service parking lots and facilities. Additionally, there were inoperable CCTV cameras, malfunctioning monitors, and facilities without cameras at critical pedestrian and vehicle entrance points.
- **Registry/Remittance** – We found 11 deficiencies related to registry cages[4] that were not fully secured to prevent unauthorized access.

Table 2. Analysis of Deficiencies

NDC	Gates and Fencing			Doors and Locks			Access Control and CCTV			Registry/Remittance			TOTAL
	High	Medium	Low	High	Medium	Low	High	Medium	Low	High	Medium	Low	
Cincinnati	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Denver	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[2] The Postal Service's Facilities organization manages repairs and alterations for over 31,000 facilities. Installation heads submit repair and alteration requests to Facilities for completion.

[3] Facilities has established repair goals based on a percentage of the total repair requests received compared to total repairs completed. However, the goals are not specific to the length of time for completing an individual repair.

[4] A registry cage is a secured area for storing registered mail.

NDC	Gates and Fencing			Doors and Locks			Access Control and CCTV			Registry/Remittance			TOTAL
	High	Medium	Low	High	Medium	Low	High	Medium	Low	High	Medium	Low	
Detroit	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Greensboro	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Jacksonville	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Kansas City	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Los Angeles	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
New Jersey	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Philadelphia	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Southern Maryland	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
St. Louis	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
TOTAL	18	10	5	24	9	10	25	13	14	7	3	1	139

Source: OIG analysis.

Finding #1: Addressing Security Deficiencies

The Postal Service and Postal Inspection Service did not always effectively address and monitor security deficiencies at the 11 NDCs we assessed. Specifically:

- In 16 of the 139 (12 percent) VRAT deficiencies, installation heads did not take initial action[5] within 30 days[6] of being notified. Seven of the 16 deficiencies (44 percent) were identified as high priority. Specific to those high priority deficiencies:

> *"The Postal Service and Postal Inspection Service did not always effectively address and monitor security deficiencies at the 11 NDCs we assessed."*

- Two related to gates and fencing took over two years before initial action was taken to address the issues.
- Two related to doors and locks took over one year before initial action was taken to address the issues.
- Three related to access control and CCTV took from between two months and two years before initial action was taken to address the issues.

[5] Initial action includes emails, phone calls, or work order requests to initiate corrective action.

[6] The Postal Service does not have a specific timeframe for taking initial action to address identified deficiencies; however, 30 days is a reasonable amount of time to begin the corrective action process and aligns with the action plan timeline. Installation heads are required to provide an action plan to address identified deficiencies resulting from PSS conducted VRAT assessments within 30 days of receiving the results.

- Ten of 11 (91 percent) installation heads did not always monitor the status of identified deficiencies, including tracking the progress of corrective actions taken and closing out deficiencies when resolved. In addition, installation heads did not always provide PSSs with status updates to assist in ensuring facility security.

Of the 139 deficiencies identified by the VRAT assessments, 60 were resolved, 36 were in progress, and 43 were unresolved. The 43 unresolved deficiencies were out of the NDC's scope of responsibility as they pertained to CCTV cameras maintained by the Postal Inspection Service or the OIG.[7] Since the NDCs were not responsible for remediation of these deficiencies, we did not analyze the elapsed time for repair.

We assessed the elapsed time for projects that were resolved and in progress by priority level — including deficiencies remediated by Facilities and in-house NDC maintenance personnel (see Table 3). Although the Postal Service did not have specific criteria related to timeframes for individual repairs to be completed, we found that 32 percent (31 of 96 projects resolved or in-progress) of the deficiencies designated as high priority ranged from over two years to over four years to resolve or they were still in progress after more than two years.

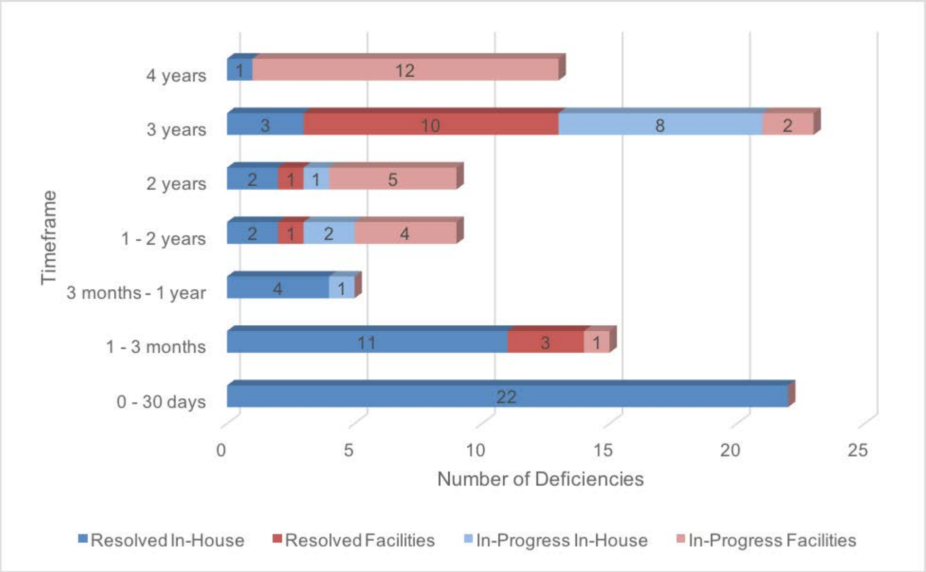
Resolved Deficiencies. Sixty of the 139 (43 percent) deficiencies were resolved as of September 30, 2017, and took between one day and three years and six months to resolve.

- Fifteen (25 percent) were Facilities projects, with 11 of the 15 (69 percent) identified as high priority and taking over two years to resolve.[8] Specifically:
  - Seven deficiencies related to access controls and CCTVs took over three years to resolve.
  - Four deficiencies related to gates, fencing, doors, and locks and took from two years to over three years to resolve.
- Forty-five (75 percent) were in-house projects with six of the forty-five (14 percent) taking over two years to resolve. Five of the six projects were identified as high priority and took over two years to resolve.

In Progress Deficiencies. Thirty-six of the 139 (26 percent) deficiencies were in progress as of September 30, 2017. The elapsed time for these deficiencies ranged from three months to over four years.

- Twenty-four (67 percent) were Facilities projects with 19 (79 percent) in progress for over two years. Eleven of the 19 projects were identified as high priority deficiencies on VRAT assessments. Specifically:
  - Seven deficiencies related to access controls and CCTVs and were in progress for over two years.
  - Four deficiencies related to doors, locks, gates, and fencing and were in progress from two years to over four years.
- Twelve (33 percent) were in-house projects, with nine (75 percent) in progress for over two years. Four of the nine in-house projects were identified as high priority deficiencies related to access control and CCTVs and were in progress for over three years.

Table 3. Elapsed Time - Deficiencies Resolved and in Progress



Source: OIG analysis.

[7] One of the 43 deficiencies related to padlocks and was incorrectly identified on the VRAT but should not have been.
[8] Projects referred to Facilities may take years to complete because Facilities projects involve multiple phases, including planning, architectural design, independent review, and on-site inspection.

These conditions occurred because management did not have sufficient internal controls to assist responsible security and area officials in effectively addressing and monitoring security deficiencies. While the Postal Service had established policy regarding general facility security, they did not have specific guidance pertaining to timeframes for addressing identified deficiencies, procedures for monitoring the completion of corrective actions taken to remediate the deficiencies, or requirements for communicating identified deficiencies to appropriate officials.

Specifically:

- There were no standard operating procedures or operational guidance policies in place regarding steps and timeframes for NDC security and area personnel to address and monitor identified security deficiencies. Also, installation heads were not required to provide periodic status updates to the area manager of operations support (MOS) and Postal Inspection Service security officials to ensure corrective actions were taken to address deficiencies or provide close out notifications when security deficiencies were corrected.
- Although installation heads report to the area MOS, the MOS has no formal responsibilities in the VRAT process and is not responsible for ensuring installation heads take corrective action. In addition, the MOS is not required to review SCO and PSS conducted VRAT assessments or PSS completed management letters.

Postal Service policy[9] states that the primary responsibility of the installation head is ensuring the general security of the facility and implementing security recommendations reported by the Postal Inspection Service.

Additionally, internal control standards set by the Government Accountability Office states that internal control activities such as approvals, authorizations, and verifications help ensure that management's directives are carried out and actions are taken to address risk. They also state that comprehensive standard operating procedures and guidance provide reasonable assurance that agency objectives are met. Further, when deficiencies are identified, management should complete and document corrective actions to remediate deficiencies timely.

When specific processes for addressing and monitoring identified security deficiencies do not exist, there is an increased potential for deficiencies to remain unresolved, thereby increasing the risk to the safety and security of postal facilities and employees. Lack of formal processes or operational guidance at the 11 NDCs we assessed contributed to some deficiencies going unresolved for periods of one to over four years.

Recommendation #1

We recommend the **Vice President, Network Operations**, in coordination with the **Chief Postal Inspector**, establish standard operating procedures detailing steps and timeframes for Network Distribution Center and area personnel to address, monitor, and communicate identified security deficiencies.

Finding #2: Conducting Vulnerability Risk Assessment Tool Assessments

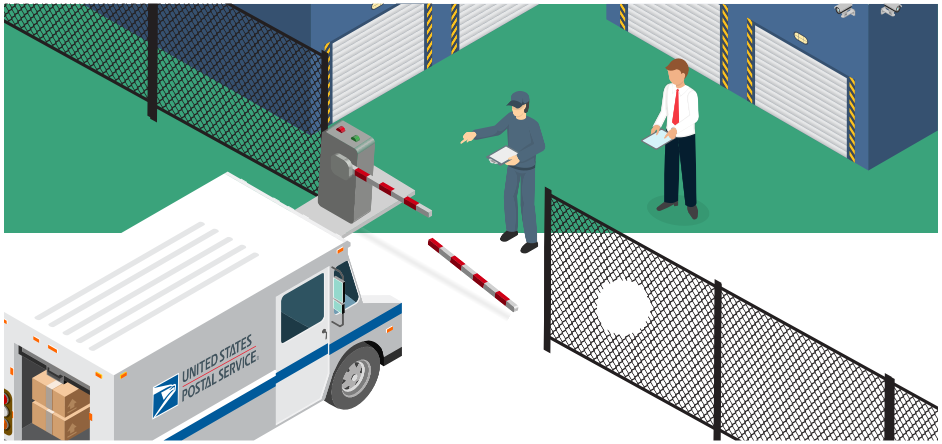
Security control officers (SCO) at the NDCs and physical security specialists (PSS) assigned from the Postal Inspection Service did not always conduct VRAT assessments as required. Specifically:

- Seven of 11 (64 percent) SCOs did not conduct VRAT assessments annually as required by the ASM.

> *"Security control officers at the NDCs and physical security specialists assigned from the Postal Inspection Service did not always conduct VRAT assessments as required."*

[9] *Administrative Support Manual* (ASM), Section 27, Security, December 2015.

- Four of 11 (36 percent) PSSs did not conduct VRAT assessments biennially as required by the Postal Inspection Service's Comprehensive Field Guide. In addition, four of 11 (36 percent) installation heads did not respond to PSS' VRAT management letters with an action plan within 30 days, as required.



These conditions occurred because Postal Service and Postal Inspection Service management did not have sufficient procedures or oversight mechanisms to ensure responsible security personnel conducted VRAT assessments as required. Specifically:

- There were no formal procedures for Postal Inspection Service-assigned homeland security coordinators (HSC) to ensure SCOs conduct VRAT assessments annually, as required.
- There is no guidance to indicate who is responsible for ensuring PSSs conduct VRATs assessments biennially, as required.
- There is not a requirement for NDC installation heads to sign off on their approval of SCO conducted VRAT assessments and acknowledge identified security deficiencies.

The ASM requires SCOs to conduct a facility security survey (FSS) annually. The VRAT assessment replaced the FSS in FY 2012; however, the ASM has not been updated to reflect this change. In addition, according to the HSC job description, the HSC oversees the security control officer program, which includes the completion of VRAT assessments by SCOs.

The Postal Inspection Service's *Comprehensive Field Guide* requires the PSS to perform a VRAT assessment biennially and issue a management letter to the installation head summarizing the results. The management letter requires the installation head to provide a written response with a corrective action plan within 30 days of receipt of the letter.

When VRAT assessments are not completed as required, existing safety measures are not assessed for adequacy and potential security deficiencies are not identified, posing an increased risk to the safety and security of Postal Service employees, customers, the mail, and other assets.

Recommendation #2

We recommend the **Chief Postal Inspector** establish an oversight mechanism to promote accountability and help ensure compliance with the Vulnerability Risk Assessment Tool requirements.

Recommendation #3

We recommend the **Chief Postal Inspector** update the Administrative Support Manual to reflect the requirements to conduct Vulnerability Risk Assessment Tool assessments.

Additional Security Concerns and Observations

American Postal Workers Union Concerns

As part of the audit, we also assessed security concerns identified by the APWU, which primarily involved gates and access controls. We validated the installation heads were aware of the security concerns and have either resolved the security concerns or began taking corrective actions (see Table 4).

Management's Comments

Management agreed with the recommendations but disagreed with portions of the finding regarding conducting VRAT assessments.

Regarding recommendation 1, management stated they will establish standard work instructions detailing steps and timeframes for NDC and area personnel to address, monitor, and communicate identified security deficiencies. The target implementation date is February 28, 2018.

Regarding recommendation 2, management stated the Postal Inspection Service Security Group will update the *Postal Inspection Service Comprehensive Field Guide* to include a section for Homeland Security coordinators to formally ensure Security Control Officers (SCO) conduct VRAT assessments as required by the ASM. In addition, the senior physical security specialist (PSS) at headquarters will oversee the progress on the required biennial VRATs conducted by the field PSSs, with exceptions being reported to the division for resolution. Management further stated the Postal Inspection Service will defer resolving the recommendation that the NDC installation head sign off on approving SCO-conducted VRAT assessments and acknowledging identified security deficiencies to the Postal Service. The target implementation date is September 30, 2018.

Regarding recommendation 3, management stated the Postal Inspection Service Security Group will update the ASM by replacing language that references Facility Security Surveys and updating the information with the VRAT assessments. The target implementation date is September 30, 2018.

Management disagreed with the conclusion in finding 2 that four of 11 (36 percent) PSSs did not conduct VRAT assessments biennially as required. Management indicated that VRAT assessments for Denver were conducted in 2017 and for Los Angeles in 2015; therefore, the exceptions should have been two of 11 (18 percent) and not four of 11 (36 percent) as indicated in the report.

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

Evaluation of Management's Comments

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

In response to management's disagreement with finding 2, the initial VRAT assessment for Denver was conducted on January 20, 2015; however, management could not provide the subsequent VRAT assessment documentation but only communicated this information via email. We consider completion of the VRAT assessment to be unsubstantiated without adequate supporting documentation. The initial VRAT assessment for Los Angeles was conducted on January 14, 2015; however, the subsequent VRAT assessment was conducted on March 24, 2017, so this subsequent assessment was not done within the two-year requirement period.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All 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.

Table 4. APWU-Identified Deficiencies

	NDC	Deficiencies Identified by the APWU	Deficiency Cited on VRAT?	Has Corrective Action Begun or Deficiency Been Resolved?
1	Cincinnati	[redacted]	Yes	Yes
2	Denver	[redacted]	Yes	Yes
3	Detroit	[redacted]	No	Yes
4	Greensboro	[redacted]	No	Yes
5	Jacksonville	[redacted].	No	Yes
6	Kansas City	[redacted]	No	Yes
7	Los Angeles	[redacted]	Yes	Yes
8	New Jersey	[redacted]	Yes	Yes
9	Philadelphia	[redacted]	Yes	Yes
10	Southern Maryland	[redacted]	Yes	Yes
11	St. Louis	[redacted]	Yes	Yes

[10] A Postal Service employee who performs control functions related to truck arrivals, registration, and dispatches.

Appendices

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

Appendix A: Additional Information

Scope and Methodology

We reviewed facility security deficiencies identified during the two most current VRAT assessments conducted by SCOs and PSSs. In addition, we assessed the status of APWU security concerns at the 11 NDCs reviewed. We limited our review to interior and exterior facility security vulnerabilities identified as part of the VRAT assessments.

To accomplish our objective, we:

- Reviewed Postal Service and Postal Inspection Service policies and procedures related to conducting VRAT assessments and procedures for addressing security deficiencies.
- Interviewed Postal Service and Postal Inspection Service personnel responsible for facility security to obtain an understanding of the process and their roles and responsibilities.
- Reviewed training records to determine if responsible personnel received sufficient training to perform their roles and responsibilities.
- Assessed internal controls for identifying, monitoring, and addressing security deficiencies.

We conducted this performance audit from June through December 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 November 22, 2017, and included their comments where appropriate.

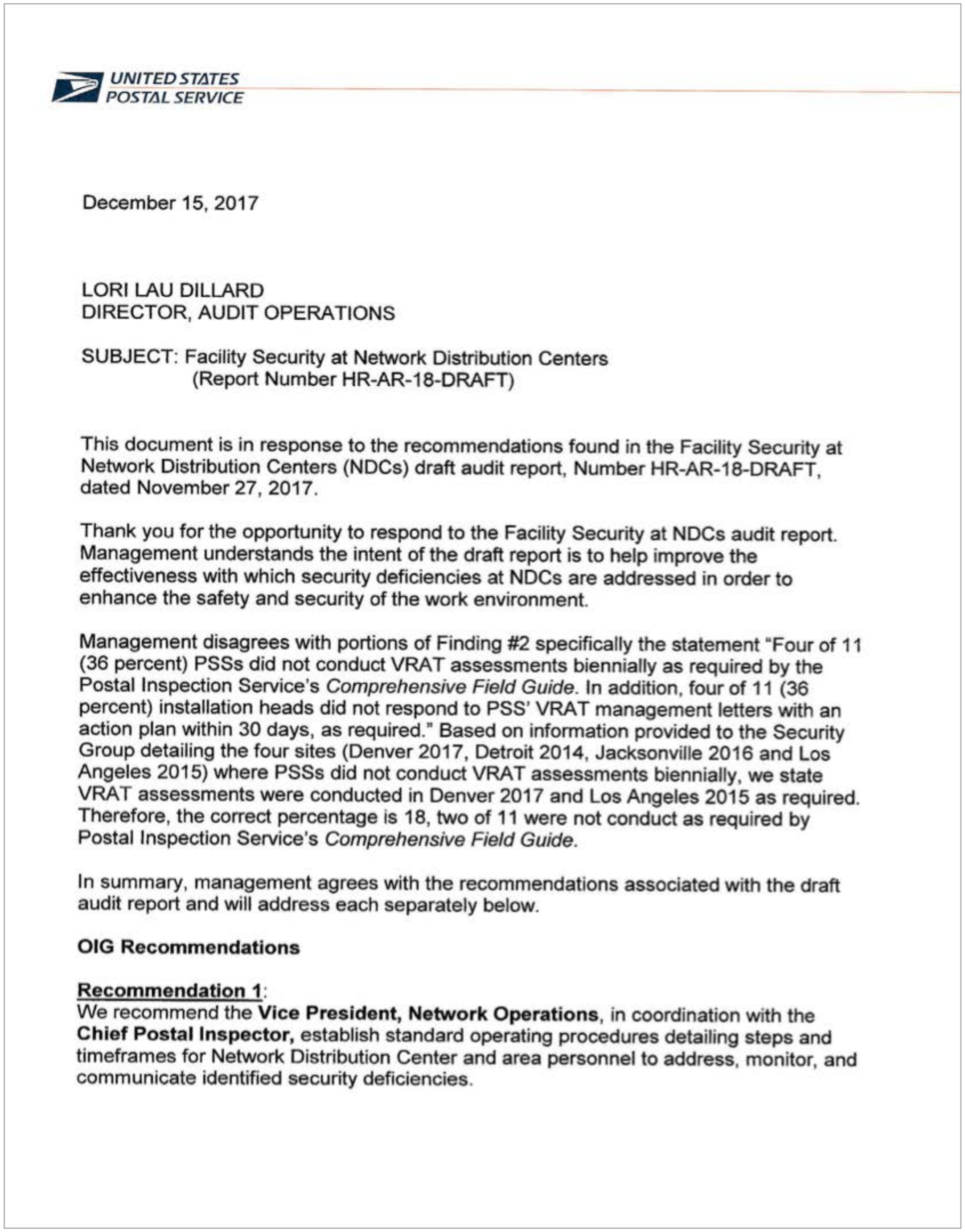
We assessed the reliability of the Postal Service eFMS, eMARS, and the Postal Inspection Service VRAT database by reviewing related source documents and interviewing responsible personnel knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

BACK to COVER

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Facility Condition Reviews – Western Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-17-009	9/8/2017	$84,000
Facility Condition Reviews – Pacific Area	Determine if Postal management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-17-007	9/6/2017	$7 million
Facility Condition Reviews – Eastern Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-17-004	5/10/2017	$32.2 million
Facility Condition Reviews – Southern Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-17-003	4/28/2017	$28.3 million
Facility Condition Reviews – Northeast Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-17-001	11/9/2016	$10.6 million
Facility Condition Reviews – Great Lakes Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-16-010	9/2/2016	$29.4 million
Facility Condition Reviews – Capital Metro Area	Determine if Postal Service management adhered to building maintenance, safety and security standards, and employee working condition requirements at retail facilities.	SM-AR-16-009	7/18/2016	$18.6 million

Appendix B: Management's Comments



UNITED STATES
POSTAL SERVICE

December 15, 2017

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Facility Security at Network Distribution Centers
(Report Number HR-AR-18-DRAFT)

This document is in response to the recommendations found in the Facility Security at Network Distribution Centers (NDCs) draft audit report, Number HR-AR-18-DRAFT, dated November 27, 2017.

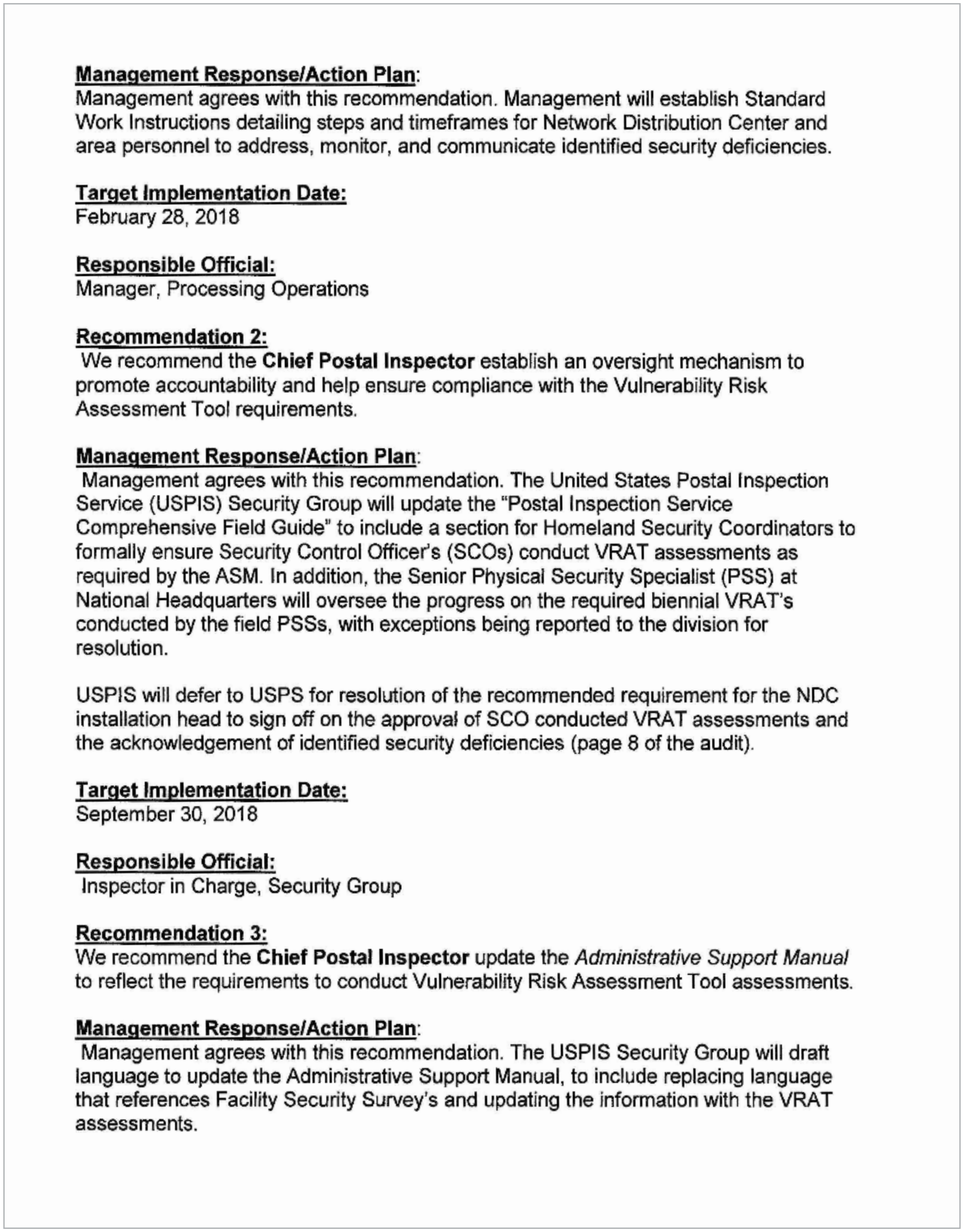
Thank you for the opportunity to respond to the Facility Security at NDCs audit report. Management understands the intent of the draft report is to help improve the effectiveness with which security deficiencies at NDCs are addressed in order to enhance the safety and security of the work environment.

Management disagrees with portions of Finding #2 specifically the statement "Four of 11 (36 percent) PSSs did not conduct VRAT assessments biennially as required by the Postal Inspection Service's *Comprehensive Field Guide*. In addition, four of 11 (36 percent) installation heads did not respond to PSS' VRAT management letters with an action plan within 30 days, as required." Based on information provided to the Security Group detailing the four sites (Denver 2017, Detroit 2014, Jacksonville 2016 and Los Angeles 2015) where PSSs did not conduct VRAT assessments biennially, we state VRAT assessments were conducted in Denver 2017 and Los Angeles 2015 as required. Therefore, the correct percentage is 18, two of 11 were not conduct as required by Postal Inspection Service's *Comprehensive Field Guide*.

In summary, management agrees with the recommendations associated with the draft audit report and will address each separately below.

OIG Recommendations

Recommendation 1:
We recommend the **Vice President, Network Operations**, in coordination with the **Chief Postal Inspector,** establish standard operating procedures detailing steps and timeframes for Network Distribution Center and area personnel to address, monitor, and communicate identified security deficiencies.



Management Response/Action Plan:
Management agrees with this recommendation. Management will establish Standard Work Instructions detailing steps and timeframes for Network Distribution Center and area personnel to address, monitor, and communicate identified security deficiencies.

Target Implementation Date:
February 28, 2018

Responsible Official:
Manager, Processing Operations

Recommendation 2:
We recommend the **Chief Postal Inspector** establish an oversight mechanism to promote accountability and help ensure compliance with the Vulnerability Risk Assessment Tool requirements.

Management Response/Action Plan:
Management agrees with this recommendation. The United States Postal Inspection Service (USPIS) Security Group will update the "Postal Inspection Service Comprehensive Field Guide" to include a section for Homeland Security Coordinators to formally ensure Security Control Officer's (SCOs) conduct VRAT assessments as required by the ASM. In addition, the Senior Physical Security Specialist (PSS) at National Headquarters will oversee the progress on the required biennial VRAT's conducted by the field PSSs, with exceptions being reported to the division for resolution.

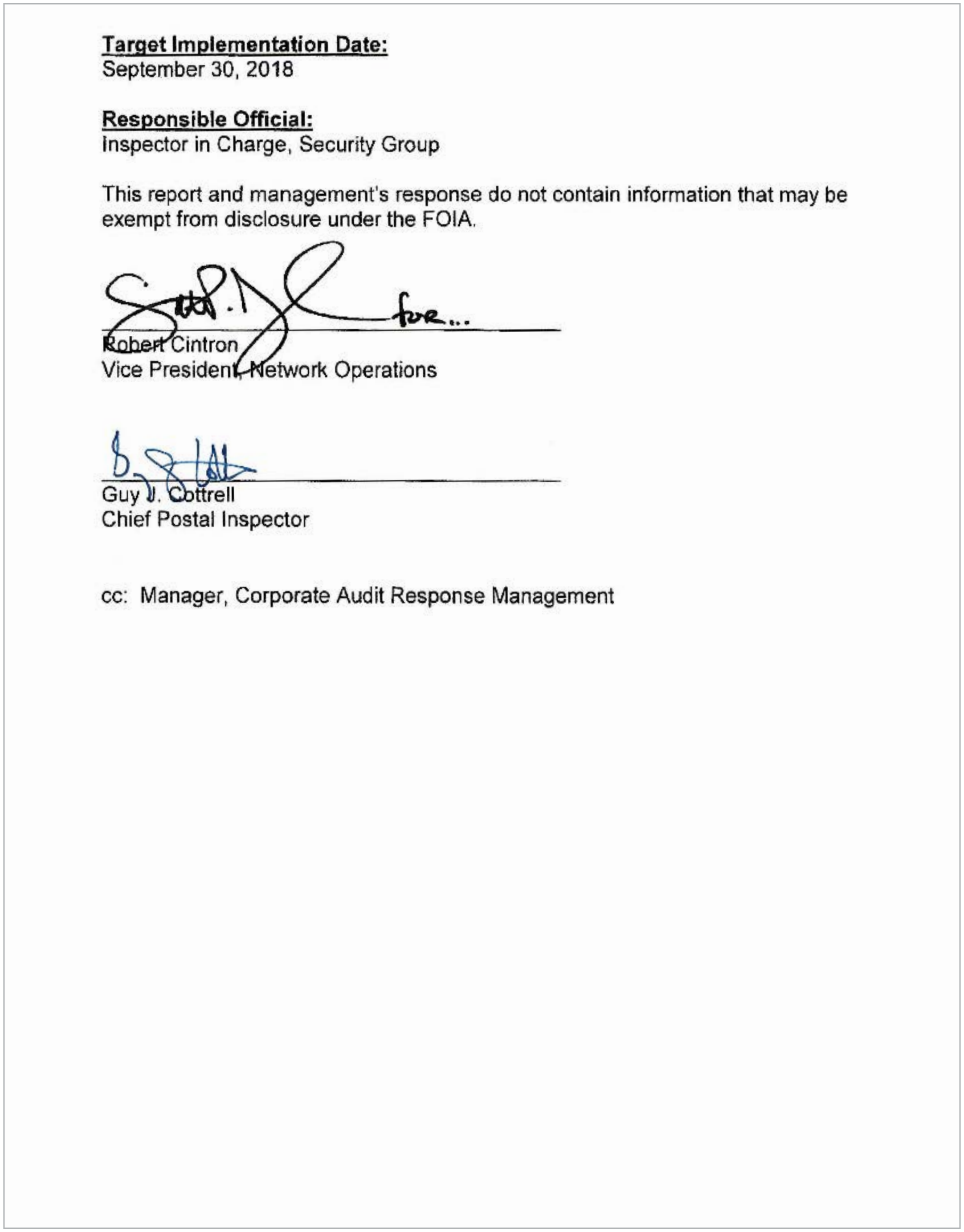
USPIS will defer to USPS for resolution of the recommended requirement for the NDC installation head to sign off on the approval of SCO conducted VRAT assessments and the acknowledgement of identified security deficiencies (page 8 of the audit).

Target Implementation Date:
September 30, 2018

Responsible Official:
Inspector in Charge, Security Group

Recommendation 3:
We recommend the **Chief Postal Inspector** update the *Administrative Support Manual* to reflect the requirements to conduct Vulnerability Risk Assessment Tool assessments.

Management Response/Action Plan:
Management agrees with this recommendation. The USPIS Security Group will draft language to update the Administrative Support Manual, to include replacing language that references Facility Security Survey's and updating the information with the VRAT assessments.



Target Implementation Date:
September 30, 2018

Responsible Official:
Inspector in Charge, Security Group

This report and management's response do not contain information that may be exempt from disclosure under the FOIA.

for...

Robert Cintron
Vice President, Network Operations

Guy J. Cottrell
Chief Postal Inspector

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