Office of Inspector General | United States Postal Service

Audit Report

U.S. Postal Inspection Service's Oversight of Facility Security and Access Control

Report Number 22-037-R22 | September 19, 2022

Table of Contents

Highlights

Background

The U.S. Postal Inspection Service is responsible for Postal Service policies, procedures, standards, and requirements for facility security and access controls. It has also established a risk management process — the Vulnerability Risk Assessment Tool (VRAT) — to ensure compliance with facility security policies and procedures and identify facility security deficiencies. Additionally, the Postal Inspection Service is an associate member of the Interagency Security Committee (ISC) formed by Executive Order 12977 to enhance the quality and effectiveness of security in protecting federal facilities.

What We Did

Our objective was to assess whether the Postal Inspection Service's facility security and access control policies align with federal standards and best practices and how identified security deficiencies are addressed. Specifically, we evaluated policies and procedures related to facility security and access control, assessed risk management policies and procedures for facilities, reviewed the ISC's standards and best practices for facility security, and analyzed VRAT data.

What We Found

The Postal Inspection Service has taken positive steps to align Postal Service facility security and access control policies and procedures with ISC's standards and best practices; however, its processes for determining facility security levels and baseline levels of protection do not align with the ISC's *Risk Management Process for Federal Facilities Standard* (RMP Standard). Specifically, we found that the Postal Inspection Service groups facilities into three security tiers based on the criticality of the facility to the U.S. Postal Service's mission. Because the Postal Inspection Service relies on only one of the six required security factors for determining the security level, 99 percent of facilities are placed in the lowest risk group. Further, the Postal Inspection Service does not assign a baseline level of protection based on the security level or regularly reassess the required security measures. As a result, required security measures may not be commensurate with the risks faced by a particular facility, causing facilities to potentially face unmitigated risks or resources to be expended on unnecessary security measures. We also found that the guidance surrounding the VRAT is insufficient for security control officers to identify the appropriate status of facility security deficiencies identified in VRAT.

Recommendations

We recommended management align their processes and policies for establishing facility security levels and baseline levels of protection for postal facilities with the RMP Standard and update the *VRAT User Guide*.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 19, 2022

MEMORANDUM FOR: GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

PETER R. RENDINA
DEPUTY CHIEF INSPECTOR, HEADQUARTERS

Margaret B. McDavid

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service, Cybersecurity and Technology

SUBJECT: U.S. Postal Inspection Service's Oversight of Facility Security and Access Control
(Report Number 22-037-R22)

This report presents the results of our audit of the U.S. Postal Inspection Service's Oversight of Facility Security and Access Control.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Elizabeth Kowalewski, Director, Inspection Service, 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 the U.S. Postal Inspection Service's Oversight of Facility Security and Access Control (Project Number 22-037). Our objective was to assess whether the Postal Inspection Service's facility security and access control policies align with federal standards and best practices and how it addresses identified security deficiencies. See Appendix A for additional information about this audit.

Background

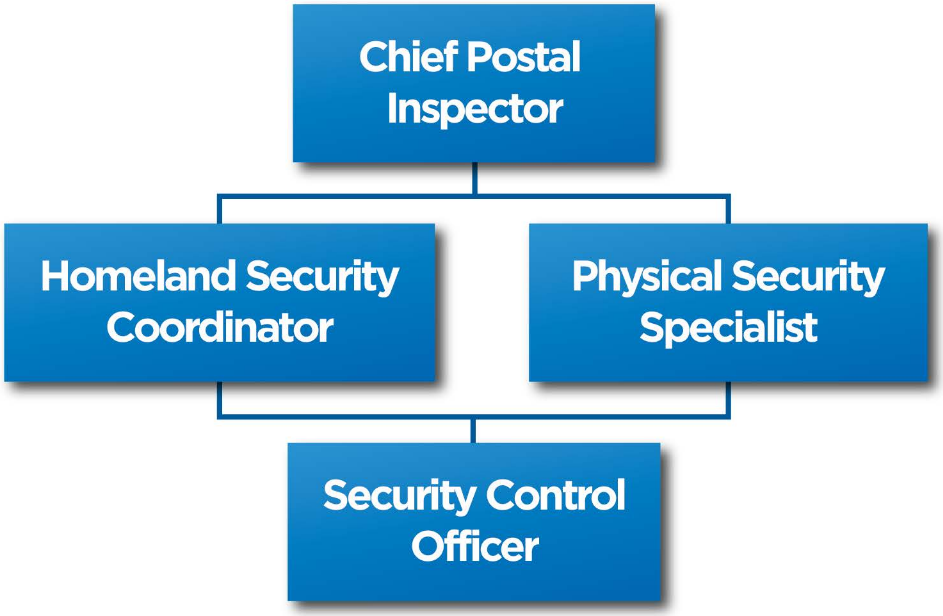
The Postal Inspection Service is responsible for ensuring the security of 516,636 career and 136,531 pre-career postal employees[1] and 32,122[2] postal facilities. The Chief Postal Inspector is the Chief Security Officer for the U.S. Postal Service and is responsible for Postal Service policies, procedures, standards, and requirements for facility security and access controls. Additionally, the Postal Inspection Service has established a risk management process — the Vulnerability Risk Assessment Tool (VRAT) — to ensure compliance with facility security policies and procedures and identify facility security deficiencies.

Facility Security and Access Controls

The Postal Inspection Service sets physical security standards for existing and new postal facilities. These standards are meant to protect the interior and exterior of a facility and can include items such as cameras, physical barriers, and facility locks and keys. For new facilities, the Postal Inspection Service conducts security assessments[3] to identify the specific security standards for owned and leased postal facilities.

In addition, the Postal Inspection Service maintains and provides technical guidelines for access control requirements such as employee and contractor badge access, visitor screening, and escort procedures. The Postal Inspection Service is responsible for providing guidance, training, and oversight to postal facility Security Control Officers (SCO) to ensure the general security of postal facilities. Physical Security Specialists[4] and Homeland Security coordinators[5] act as liaisons between the Postal Inspection Service and SCOs to provide oversight of the SCO program at facilities in their assigned area (see Figure 1).

Figure 1. Postal Facility Security Reporting Hierarchy



Source: United States Postal Service Office of Inspector General (OIG) analysis of Postal Service policy.

1 *United States Postal Service 2021 Annual Report to Congress*, pg. 1.
2 Postal Service VRAT data as of April 7, 2022.
3 Handbook RE-5, *Building and Site Security Requirements*, Section 1-3.1, Security Assessments.
4 Postal Inspection Service employees who complete VRAT surveys and make facility security recommendations.
5 Postal Inspection Service employees who oversee, coordinate, and monitor program performance reviews in compliance with postal policies and procedures according to applicable laws and regulations; provide results of field reviews to management; identify discrepancies and deficiencies; provide information, technical guidance, and assistance to managers and supervisors regarding appropriate corrective measures; and monitor compliance to meet performance metrics.

Prior OIG Audits

Prior OIG audits have identified consistent challenges related to the Postal Service's implementation of facility security and access controls.[6] For example, during fiscal years (FY) 2017-2019, we conducted site security audits at processing and distribution centers in four Postal Service areas. These audits identified weaknesses such as unauthorized badge and server room access, broken locks on facility property, and physical access control weaknesses.[7] Other audits found problems in how access badges are issued and managed.[8]

Vulnerability Risk Assessment Tool

The VRAT is an interactive tool that the Postal Inspection Service implemented and SCOs use to identify security vulnerabilities at postal facilities. The Postal Inspection Service has categorized each postal facility into one of three facility security levels: Tier 1 (Most Critical), Tier 2 (Critical), and Tier 3 (Least Critical).[9] The vast majority of postal facilities (99 percent) are Tier 3 facilities. The VRAT also notes a risk score for each facility based on crimes impacting people and property in the area surrounding the facility.[10] This risk score is unrelated to the tier level.

The SCOs at all postal facilities are required to complete a Tier 3 VRAT survey annually. This survey is structured to capture major physical security and procedural vulnerabilities through quick and simple assessments.[11] When security deficiencies are identified, SCOs are responsible for identifying and implementing corrective action within 30 days.[12] The Postal Inspection Service conducts more comprehensive VRAT surveys for Tier 1 and Tier 2 facilities every two years. When the Postal Inspection Service completes a VRAT survey, it submits formal reports with recommendations for security enhancements via the VRAT to the installation head for their review and remediation.[13]

Interagency Security Committee Standards

The Interagency Security Committee (ISC) was formed by Executive Order 12977 in 1995 to enhance the quality and effectiveness of security in and protection of federal facilities occupied by federal employees for nonmilitary activities by establishing relevant standards and best practices. The Postal Inspection Service is an associate member of the ISC and coordinates with ISC committee members annually to assess the Postal Inspection Service's compliance with ISC standards and best practices.

"The vast majority of postal facilities (99 percent) are Tier 3 facilities."

The ISC's *Risk Management Process for Federal* Facilities (RMP Standard) defines the criteria and process executive agencies, and departments must follow when assessing risks to their facilities. Specifically, the RMP Standard provides the criteria and processes to determine the facility security level and single source of physical security countermeasures, as well as guidance for customizing countermeasures for federal facilities. Additionally, the ISC's *Facility Access Control: An Interagency Security Committee Best Practice* and *Best Practices for Planning and Managing Physical Security Resources* provide guidance to federal agencies on facility access controls and practices most beneficial for physical security programs, respectively.

Findings Summary

We determined that Postal Service facility security and access control policies generally align with the RMP Standard. However, we found that the Postal Inspection Service's process for determining facility tier levels does not align with the RMP Standard for determining the facility security level. We also found

6 Eight prior OIG audits conducted from FY 2015 to 2021 had 23 recommendations relating to facility security and access controls.
7 *Physical and Environmental Controls Site Summary Review – Summary Report* (Report Number IT-AR-19-004).
8 *Badges for Postal Service Contractors* (Report Number HR-AR-15-004), *Pacific Area Processing and Distribution Center Physical and Environmental Security Controls* (Report Number IT-AR-17-005), *Western Area Physical Security and Environmental Controls* (Report Number IT-AR-18-002), *Capital Metro Physical and Environmental Controls Site Security Review* (Report Number IT-AR-18-005), *Northeast Area Environmental and Physical Controls Site Security Review* (Report Number IT-AR-19-003), *National Security Clearance Program* (Report Number OV-AR-19-001), *U.S. Postal Service Exit Process* (Report Number 20-167-R21).
9 VRAT data analysis count of postal facilities in each tier as of March 1, 2022: Tier 1:18, Tier 2: 268, Tier 3: 31,660.
10 *VRAT User Guide*, pg. 6. This is known as a CAP score and is a commercially provided risk score.
11 *VRAT User Guide*, pg. 4.
12 *Administrative Support Manual* (ASM) 13, Section 273.114, Remediation of Facility Security Surveys, dated July 1999, updated through July 31, 2021.
13 ASM 13, Section 273.113, Facility Security Surveys, dated July 1999, updated through July 21, 2021.

that the policy for determining the required baseline level of protection at a given facility does not align with the RMP Standard. Additionally, we found that SCOs inconsistently responded to VRAT deficiencies.

Finding #1: Facility Security and Access Control Policies

We found that Postal Service facility security and access control policies generally align with ISC standards and best practices, and in one case exceeds RMP Standard requirements. Specifically, requirements for postal facilities to be equipped with security measures such as closed-circuit televisions, security alarms, facility and vehicle barriers, and electronic access controls systems align with the ISC's best practices for facility security. For example, ISC's best practices state that access to federally occupied spaces should be managed by installing Physical Access Control Systems to electronically authenticate identity credentials. The Postal Inspection Service manages an ePhysical Access Control System that provides access to postal facilities using identity credentials for authorized personnel. Although prior OIG audits identified areas for improvement surrounding the implementation of various facility security policies, our assessment concluded that the policies themselves generally align with the ISC's standards and best practices.

> *"Additionally, we found that one aspect of the Postal Service's risk assessment policy for facility security exceeds the requirements of the RMP Standard."*

Additionally, we found that one aspect of the Postal Service's risk assessment policy for facility security exceeds the requirements of the RMP Standard. Specifically, Postal Service policy requires SCOs at each postal facility to conduct a Tier 3 VRAT survey annually, while the RMP Standard requires risk assessments every three to five years based on facility security levels.[14] In addition, the Postal Inspection Service conducts more comprehensive risk assessments of Tier 1 and Tier 2 facilities every two years.[15] Per the *VRAT User Guide*, any level of VRAT can be performed on any level facility. We determined that 30,242 of 32,122 facilities (or 94 percent) had at least one VRAT survey from October 2020 through March 2022.

Finding #2: Facility Security Level

We found that Postal Inspection Service processes for establishing tier levels do not align with the RMP Standard for determining facility security levels. Specifically, according to the Postal Inspection Service's *VRAT User Guide*, facilities are grouped into three tier levels and assigned security levels based on mission criticality:

- Tier 1: facilities such as postal headquarters and data centers are the most critical and their loss of operations would have national implications.
- Tier 2: facilities such as processing and distribution centers experiencing loss of operations would have area – or district-wide implications.
- Tier 3: facilities such as post offices are the least critical and loss of operations would have minimal effect on postal operations.

The RMP Standard states that all federal facilities should be assigned one of five facility security levels, from lowest to highest risk. The RMP Standard requires facilities to determine the facility security level based on an analysis of six security-related facility factors, five of which are required and equally weighted. The five required factors are mission criticality, threat to tenant agencies, facility size, facility population, and symbolism. A sixth factor — intangibles — may be considered to adjust a facility security level up or down one level after the first five factors have been considered. Each facility security level aligns with a set of security countermeasures that may be customized to address site-specific conditions. According to the RMP Standard, the scope of security countermeasures should be commensurate with the risk posed to a facility.

However, the Postal Inspection Service's tier-based approach includes three levels rather than five and is determined entirely on one factor — mission criticality — instead of all six factors identified by the RMP Standard. Additionally,

14 *Interagency Security Committee Standard, The Risk Management Process*, Section 4.1, Making the Facility Security Level Determination.
15 The Postal Inspection Service may also perform a more comprehensive survey of a Tier 3 facility in the event of a security incident, such as a burglary.

management has acknowledged that no postal facilities have undergone a facility security level determination (see Figure 2).

Figure 2. Comparison of Postal Inspection Service Tier Levels to RMP Standard Facility Security Levels

Postal Inspection Service Facility Tier Levels

Number of Levels

3

Factors Considered

1. Mission Criticality

Purpose

Each Tier level aligns with the type of VRAT required for the facility.

RMP Standard Facility Security Levels

Number of Levels

5

Factors Considered

1. Mission Criticality
2. Symbolism
3. Facility Population
4. Facility Size
5. Threat to Tenant Agencies
6. Intangible Adjustment

Purpose

Each facility security level aligns with a set of security countermeasures that may be customized to address site-specific conditions.

Source: OIG analysis of Postal Inspection Service's *VRAT User Guide* and the RMP Standard.

As a result, 99 percent of postal facilities are categorized as Tier 3 facilities. While all tier-level VRATs include questions that are used to score each facility's risk based on crimes impacting people and property in the area surrounding the facility, this risk score does not affect the assigned tier level. Specifically, although Tier 3 facilities are considered the lowest risk based solely on their mission criticality, the risk score the Postal Inspection Service uses identified [redacted] as being at moderate, elevated, or significant risk levels. Despite this, all Tier 3 facilities are assessed against the same set of countermeasures in the VRAT. In contrast, the same risk measures identified [redacted] of Tier 1 and 2 facilities as low or slight risk even though they are assessed against enhanced security measures in the Tier 1 and Tier 2 VRATs.

> *"We found that the Postal Service's policy for determining the required level of protection at a given facility does not align with the RMP Standard."*

Without considering all relevant factors when determining the facility security level, the countermeasures required by the Postal Inspection Service and assessed by the VRAT may not be commensurate with the risks faced by a particular facility. As such, facilities may face unmitigated risks, or the Postal Service may be expending resources on unnecessary security measures.

Recommendation #1

We recommend the **Chief Postal Inspector** establish a facility security level determination process that considers all six factors in the Risk Management Process Standard.

Finding #3: Baseline Level of Protection

We found that the Postal Service's policy for determining the required level of protection at a given facility does not align with the RMP Standard. Handbook RE-5 requires a baseline level of protection to be established for all facilities at the time of acquisition or construction.[16] This policy identifies two levels of security countermeasures, the first being a standard set of countermeasures required for all postal facilities. The second level provides an enhanced set of countermeasures for facilities identified as requiring a "high security" level of protection based on facility risk factors and crime that exist at the time of acquisition or construction.

According to the RMP Standard, the baseline level of protection should directly correspond to a facility's determined security level and then a risk assessment will determine whether the baseline level of protection is sufficient, or whether further customization is warranted. Deviations from the baseline level of protection established at facility acquisition or construction are allowed if supported by a Postal Inspection Service risk assessment.

However, established levels of protection are not readily available to SCOs responsible for facility security. Further, as discussed previously, when facilities are assessed for compliance with security countermeasures through the VRAT, they are assessed based on the countermeasures associated with the facility tier level, not the baseline level of protection established at facility acquisition or construction. Any countermeasures not in place at the time of the VRAT are considered security deficiencies that must be resolved, even if they are not applicable to a particular facility.

The RMP Standard also states that facilities are required to reassess and adjust, if necessary, the baseline level of protection as part of the regularly recurring risk assessment. While the VRAT contains elements designed to assess the level of risk at a facility, the results of this annual risk assessment do not change the countermeasure requirements the facility is assessed against in the VRAT and are not used to reassess the facility's baseline level of protection (see Figure 3).

Figure 3. Comparison of Postal Inspection Service Baseline Level of Protection Policies to RMP Standard

Source: OIG analysis of Handbook RE-5 and the RMP Standard.

16 Handbook RE-5, Section 1-3.3.

The RMP Standard requires facilities to conduct risk assessments every three to five years depending on their security level and to reassess the facility security level and corresponding baseline level of protection at that time. As such, it is not necessary to reassess the baseline level of protection each time a VRAT is conducted. However, without regularly integrating the risk information collected by the VRAT into security requirements, management cannot ensure that required countermeasures are commensurate with a facility's level of risk.

Recommendation #2

We recommend the **Chief Postal Inspector** redesign the baseline level of protection process to align with the Risk Management Process Standard, to include establishing a baseline level of protection for each facility security level and regularly reassessing the baseline level of protection.

Finding #4: Vulnerability Risk Assessment Tool Guidance

We found that SCOs inconsistently responded to VRAT deficiencies. When a VRAT survey is completed by an SCO or the Postal Inspection Service, any security deficiencies identified are reported and tracked in the VRAT to be remediated by the facility SCO. Within the VRAT, SCOs can select from four resolution status options: Resolved, In Progress, Deferred, and No Action Required. In addition, SCOs can enter an explanation for the status option selected. Generally, this explanation includes information about the corrective action taken to address the deficiency.

"While SCOs responses to the identified deficiencies are allowed by the VRAT, without consistent responses to deficiencies by SCOs, the Postal Inspection Service cannot rely on the information in the VRAT to accurately assess the status of security deficiencies and ensure they are appropriately addressed."

We found that 1,010 explanations were used more than once to explain 4,600 deficiencies. Of the 1,010 explanations, 110 (11 percent) were associated with more than one resolution status. For example, the same description "Not required" was written in the open-text field for 69 deficiencies. However, 49 of the 69 deficiencies (71 percent) had a status of "Resolved", while the remaining had a status of "No Action Required", which is inconsistent and can lead to inaccuracies in assessing and resolving deficiencies.

Postal Inspection Service policy states that SCOs are responsible for facility security, with the Postal Inspection Service providing guidance, training, and oversight.[17] However, because the *VRAT User Guide* does not define the four resolution status options, there was a lack of consistency in how SCOs determined which status was appropriate. While SCOs responses to the identified deficiencies are allowed by the VRAT, without consistent responses to deficiencies by SCOs, the Postal Inspection Service cannot rely on the information in the VRAT to accurately assess the status of security deficiencies and ensure they are appropriately addressed.

Recommendation #3

We recommend the **Chief Postal Inspector** update the *Vulnerability Risk Assessment Tool User Guide* to provide specific guidance on responding to identified security deficiencies.

Management's Comments

Management generally agreed with all findings, disagreed with recommendations 1 and 2, and agreed with recommendation 3.

Regarding recommendation 1, management believes that the current Postal Inspection Service facility security level determination process exceeds the RMP Standard.

17 *Inspection Service Manual*, Section 5.7.3.1, Security Control Officer Program.

Regarding recommendation 2, management believes the process used to establish the baseline level of protection for each postal facility exceeds the RMP Standard because facilities receive a yearly assessment to modify or change existing security measures.

Regarding recommendation 3, management will update the Vulnerability Risk Assessment Tool User Guide to provide specific guidance on responding to identified security deficiencies. The target implementation date is September 2023.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendation 3 and the action plan to address the recommendation should resolve the issue identified in this report. We view the disagreement with recommendations 1 and 2 as unresolved and plan to pursue them through the audit resolution process.

Regarding recommendation 1, management believes that their current facility security level determination process exceeds the RMP Standard. However, as noted in the report, the Postal Inspection Service determines its tier-based approach entirely on one factor instead of on all six factors identified by the RMP Standard. Additionally, the RMP Standard is designed to grant agencies further flexibility via one of the factors (intangible adjustments), which allows agencies to take into consideration any special agency needs and requirements when establishing facility security levels. Considering only one factor limits the Postal Inspection Service's assessment of potential risk to postal facilities, which could have a significant impact on the level of security needed for a postal facility. As a result, 99 percent of facilities are in the Tier 3 level.

Regarding recommendation 2, although management believes the process used to establish the appropriate level of protection for each facility exceeds the RMP Standard, as stated in our report, we do not agree. Specifically, the Postal Inspection Service's two baseline levels of protection are unrelated to its three facility tier levels. Further, the annual assessment of security measures is based only on tier level, not on a facility's specific baseline level of protection. As a result, any countermeasures not in place at the time of the VRAT are considered security deficiencies that must be resolved, regardless of whether or not they apply to a particular facility. Management also states that they use the yearly assessment to modify or change existing security measures. However, as stated in our report, the outcome of the VRAT does not change the baseline level of protection established at facility construction or acquisition, or the security measures against which a facility is assessed and held accountable.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendation 3 should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation 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 our audit covered a review of the Postal Inspection Service's oversight of facility security and access control and its compliance with applicable policies and procedures during the period October 1, 2020, through March 31, 2022.

To accomplish our objective, we:

- Reviewed Postal Inspection Service policies and procedures for facility security and access controls.
- Reviewed Postal Inspection Service risk management policies and procedures for facility security.
- Compared Postal Inspection Service policies and procedures for facility security and access control to the ISC's RMP Standard.
- Analyzed Postal Inspection Service VRAT data.
- Conducted interviews with the Postal Inspection Service and postal facility SCOs.
- Reviewed cases in the Case Management System related to facility security incidents.

We conducted this performance audit from December 2021 through September 2022 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 17, 2022, and included their comments where appropriate.

We assessed the reliability of computer-generated data by analyzing and reviewing the raw data, performing automated and manual reviews to supporting documents or systems, and interviewing personnel knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact (in millions)
U.S. Postal Service Exit Processing	Assess the Postal Service's exit processing and determine whether managers revoked facility access for separated employees and inactive contractors in a timely manner.	20-167-R21	4/12/2021	None
Physical and Environmental Controls Site Security Review – Summary Report	Identify and summarize the findings and recommendations in four OIG-issued area physical and environmental controls site security reports. The objective of those audits was to determine whether the Postal Service established effective physical and environmental security controls at processing and distribution centers.	IT-AR-19-004	8/15/2019	7/29/2020
National Security Clearance Program	Determine whether controls are in place to effectively manage the Postal Inspection Service's national security clearance processes and safeguard personally identifiable information.	OV-AR-19-001	6/18/2019	$318
Northeast Area Environmental and Physical Controls Site Security Review	Determine whether the Postal Service established and implemented effective environmental and physical security controls according to Postal Service policy at the processing and distribution center.	IT-AR-19-003	1/13/2019	None
Capital Metro Physical and Environmental Controls Site Security Review	Determine whether the Postal Service established and implemented effective physical and environmental security controls according to Postal Service policy at the processing and distribution center.	IT-AR-18-005	9/28/2018	None
Western Area Physical Security and Environmental Controls	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 processing and distribution center.	IT-AR-18-002	3/19/2018	None

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

September 9, 2022

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: U.S. Postal Inspection Service's Oversight of Facility Security and Access Control (Project Number 22-037-DRAFT)

Thank you for the opportunity to provide comments on the United States Postal Service Office of Inspector General (USPS -OIG) draft audit report, "*U.S. Postal Inspection Service's Oversight of Facility Security and Access Control (22-037-DRAFT).*" Management has reviewed the report along with its findings and recommendations. With respect to the findings, management generally agrees with the findings. With respect to the recommendations, management disagrees with recommendations 1 and 2, and agrees with recommendation 3, as discussed below. Management appreciates USPS-OIG's consideration and implementation of requested changes to the report raised during the exit conference and the subsequent meeting with the USPS-OIG on this project.

Recommendation #1: We recommend the **Chief Postal Inspector** establish a facility security level determination process that considers all six factors in the Risk Management Process Standard.

Management Response/Action Plan: Management disagrees with this recommendation. Although the Postal Inspection Service is an associate member of the Interagency Security Committee (ISC) and coordinates with ISC committee members annually to assess the Postal Inspection Service's compliance with ISC standards and best practices, we are not required to use the standard. The ISC encourages agencies to use their own security standards if they exceed the standards set forth in the Risk Management Process Standard. Management believes the current United States Postal Service (USPS)/United States Postal Inspection Service (USPIS) facility security level determination process exceeds the Risk Management Process Standard and offers us greater flexibility in addressing the unique security challenges of Postal facilities.

<u>Recommendation #2</u>: We recommend the **Chief Postal Inspector** redesign the baseline level of protection process to align with the Risk Management Process Standard, to include establishing a baseline level of protection for each facility security level and regularly reassessing the baseline level of protection.

Management Response/Action Plan: Management disagrees with this recommendation. Although the Postal Inspection Service is an associate member of the Interagency Security Committee (ISC) and coordinates with ISC committee members annually to assess the Postal Inspection Service's compliance with ISC standards and best practices, we are not required to use the standard. The ISC encourages agencies to use their own security standards if they exceed the standards set forth in the Risk Management Process Standard. Management believes the process used to establish the appropriate level of protection for each Postal facility exceeds the Risk Management Process Standard. Our facilities receive a yearly assessment to modify or change existing security measures.

<u>Recommendation #3</u>: We recommend the **Chief Postal Inspector** update the *Vulnerability Risk Assessment Tool User Guide* to provide specific guidance on responding to identified security deficiencies.

Management Response/Action Plan: Management agrees with this recommendation and will update the *Vulnerability Risk Assessment Tool User Guide* to provide specific guidance on responding to identified security deficiencies.

Target Implementation Date: September 2023

Responsible Official: Deputy Chief Inspector, Headquarters, Operations – Security

Gary R. Barksdale
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

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100