Office of Inspector General | United States Postal Service

Audit Report

Wireless Assessment

Report Number 21-221-R22 | August 18, 2022

Table of Contents

Highlights

Background

The U.S. Postal Service's daily operations depend on both wired and wireless networks and technologies to collect, process, and deliver the nation's mail. Wireless networks provide access to critical systems and devices without requiring a physical connection. Appropriately securing these networks to increase protection against cyberattacks is vital to Postal Service business operations. The Postal Service's Corporate Information Security Office ensures the security of wireless connections to internal and external resources. The Network & Compute Technology group designs, secures, and manages the wireless network infrastructure, while the Network Change Review Board manages and approves wireless network standards and activities. Finally, the Chief Technology Office performs research and development for delivery, mail processing, and retail systems and equipment.

What We Did

Our objective was to evaluate the effectiveness of the Postal Service's security controls to protect and manage its wireless infrastructure. Specifically, we conducted a technical wireless network assessment at four postal facilities from January through April 2022 using both [redacted] to determine if security controls were in place and functioning as intended.

What We Found

While the Postal Service utilized appropriate encryption standards and managed wireless channels to improve network performance, the agency did not have other technical security controls in place. Specifically, we found insufficient technical security controls that allowed [redacted] and allowed devices to [redacted]. We also found that management did not conduct [redacted] of the wireless network and that they were not aware of [redacted] at Postal Service facilities. These issues occurred because the [redacted] was not configured properly. In addition, instead of performing visual inspections and walk-throughs, management relied on software to identify wireless devices. Finally, there were no established procedures for how to account for [redacted] at Postal Service facilities.

Recommendations

We made five recommendations including that management properly implement [redacted] and implement the use of secure methods to [redacted] establish a strategy to conduct [redacted], develop a process for labeling access points to reflect identifiable information from the inventory, and establish procedures to account for wireless devices.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 18, 2022

MEMORANDUM FOR: LINDA M. MALONE
VICE PRESIDENT, ENGINEERING SYSTEMS

HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

WILLIAM E. KOETZ
VICE PRESIDENT, NETWORK & COMPUTE TECHNOLOGY

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

SUBJECT: Audit Report – Wireless Assessment
(Report Number 21-221-R22)

This report presents the results of our Wireless Assessment audit.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Laura Roberts, Acting Director, Cybersecurity & Technology, 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 wireless assessment audit (Project Number 21-221). Our objective was to evaluate the effectiveness of the U.S. Postal Service's security controls to protect and manage its wireless infrastructure. See Appendix A for additional information about this audit.

Background

Wireless networks and technologies drive key Postal Service operations, including the agency's ability to collect, process, and deliver the nation's mail. For example, wireless networks support:

- Over 50,000 notebook computers, 32,000 smartphones, and 3,700 tablets used by the workforce.
- Over 443,000 hand-held scanners, including over 260,000 [redacted] that provide real-time scanning for daily delivery operations.
- Around 6,600 [redacted] devices that allow employees to serve customers in post office lobbies more efficiently.[1]
- About 12,300 [redacted] laptops equipped with Bluetooth headsets and ring scanners to capture barcodes when packages arrive at delivery units.
- Over 4,700 [redacted] used at delivery units to provide greater package visibility through scanning packages and identifying associated delivery routes.[2]

Cyberattacks across wireless networks are rapidly increasing in frequency, sophistication, and reach because an attacker compromising a wireless network only needs to be within a certain proximity to gain access. Appropriately securing wireless networks is critical to Postal Service business operations because poorly configured wireless networks can be vulnerable to these attacks. The organizations responsible for securing the wireless network are part of the Chief Information Office (CIO). Specifically, the Corporate Information Security Office's (CISO) Cybersecurity Engineering Group protects Postal Service data and information technology assets[3] by developing secure wireless connections to internal and external systems and applications. The Network & Compute Technology (NCT) group designs, secures, and manages the wireless network infrastructure,[4] which includes ensuring that wireless service is available throughout, but not beyond, Postal Service property. The Chief Technology Office (CTO) performs research and development for USPS delivery, mail processing, and retail systems and equipment.

> *"Cyberattacks across wireless networks are rapidly increasing in frequency, sophistication, and reach because an attacker compromising a wireless network only needs to be within a certain proximity to gain access."*

To assess wireless network security controls, we conducted a technical assessment at four processing and distribution centers (P&DC) in [redacted] from January through April 2022. We used a combination of [redacted] and [redacted] to determine if security controls were in place and functioning as intended.

Findings Summary

While the Postal Service utilized appropriate encryption standards to secure the wireless network and appropriately managed wireless channels to improve network performance, the agency did not have [redacted]

1 Postal Facts, *Innovation in the Mail, Facts #698, #396, and #365*, dated March 2022.
2 [redacted] data provided by the Postal Service Asset Management group, dated May 10, 2022.
3 Postal Service Blue Pages, Cybersecurity Engineering (usps.gov).
4 Handbook AS-805-D, *Information Security Network Change Review Process*, Sections 2-3 and 2-5, dated April 2021.

in place to [redacted]. The audit team successfully [redacted]. We also found the Postal Service used [redacted]. Together, these issues [redacted]

Finding #1: Technical Security Controls

The Postal Service did not secure the wireless network as required by internal policy and standards. Specifically, we conducted wireless assessments at four P&DCs and found that they:

- Did not enforce [redacted]
- Allowed the use of [redacted]
- Allowed [redacted]

At each P&DC, the audit team [redacted] Additionally, the team [redacted]

According to internal policy[9] and standards,[10] non-postal devices are not allowed to connect to the network and any new devices attempting to access the network must undergo an [redacted] process to ensure that a Postal Service-issued [redacted] is on the device. Policy also states that technical security requirements must be implemented to provide a framework for strong device [redacted] Based on a device administration guide,[11] it is a security best practice to disable unencrypted forms of communicating with the device over a network. This includes disabling [redacted] and other insecure protocols.

> *"Without proper technical security controls,* [redacted]

These issues occurred because the [redacted] Additionally, the [redacted]. Without proper technical security controls, [redacted]. In addition, using [redacted]

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, and **Vice President, Network & Compute Technology**, properly implement [redacted] to prevent [redacted] from [redacted] to the wireless network.

5 [redacted]
6 [redacted]
7 [redacted]
8 [redacted]
9 Handbook AS-805, Sections 7-3.3, Non-Postal Service Portable Electronic Devices; 11-11.8.3, Technical Security Requirements; and 10-2.7.5, Network Access Control, dated June 2021.
10 *USPS Wi-Fi Hardening Standards*, dated May 2021.
11 [redacted]

Recommendation #2
We recommend the **Vice President, Chief Information Security Officer**, and **Vice President, Chief Technology Office**, disable [redacted] and implement the use of secure methods to [redacted].

Finding #2: Wireless Surveys and Reviews

The Postal Service [redacted], as required by policy.[12] Specifically, during our site visits at the selected facilities, we conducted wireless scanning and discovery to identify wireless access points (AP) and verify the Postal Service inventory. We found APs that were inaccurately mapped, not found, or incorrectly labeled (see Table 1).

Table 1. Access Point Inventory Data

	[redacted]	[redacted]	[redacted]	[redacted]
Number of APs at [redacted]	94	43	22	49
Incorrect Location	0	12	6	9
Devices Not Located	0	3	0	1
Incorrectly Labeled	94	32	0	0

Source: U.S. Postal Service Office of Inspector General (OIG) analysis of Postal Service Cisco Prime database, retrieved 10/28/2021.
Note: The [redacted] had some APs that were both in the incorrect location and incorrectly labeled.

In addition, we found NCT did not place APs so there were no gaps in coverage. Figure 1 displays our analysis of AP locations as reported for the [redacted] compared to the actual physical location identified by the audit team. [redacted]

Figure 1. Analysis of [redacted]

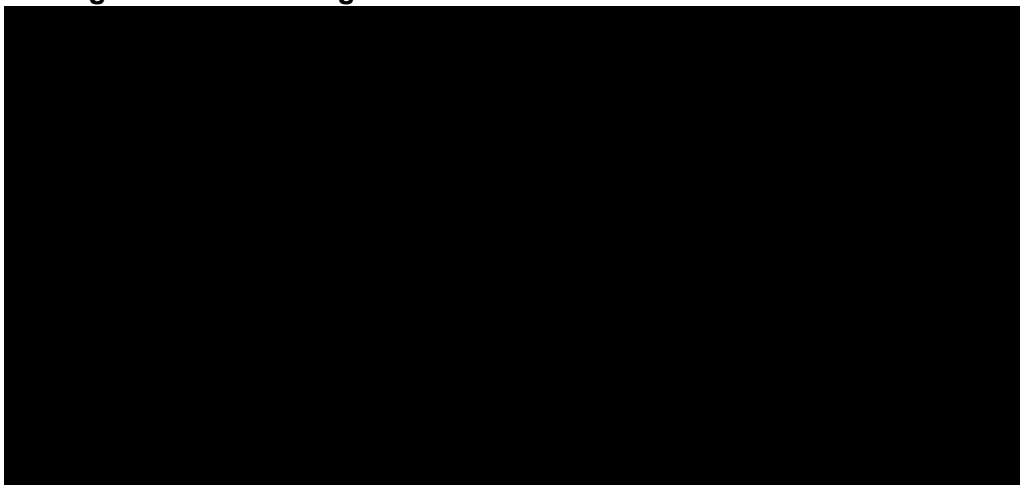
[redacted]

Source: OIG analysis of Postal Service map of [redacted]

In addition, physical AP labels were not standardized and did not display identifying information that correlates to the AP inventory management system. The Postal Service naming standard[13] for all devices is the [redacted]. Figure 2 shows examples of correctly and incorrectly labeled APs.

12 Handbook AS-805, Sections 11-11.8.1, Administrative Security Requirements; and 14-2.1, Regular Testing of Security Systems and Processes.
13 Management Instruction AS-850-2002-13, *Naming Standards for Devices on the Postal Service Managed Network Services (MNS) Network and Implementation of Asset Management,* dated October 2002.

Figure 2. AP Labeling



Source: OIG Photograph.
Note: The correctly labeled AP includes the [redacted]. The incorrectly labeled AP is missing this information.

Postal Service policy requires [redacted] to identify devices on the network and determine their proper location.[14] Instead of performing visual inspections and walk-throughs, the NCT group [redacted] to identify wireless devices and only conducted site visits during the initial install or refresh of APs. Regular physical wireless surveys and reviews increase the Postal Service's ability to manage, troubleshoot, and detect loss or theft of the devices. In addition, these reviews would allow for identification of gaps in service, eliminating dead zones that could impact mail processing and delivery that rely on wireless services.

Recommendation #3
We recommend the **Vice President, Network & Compute Technology**, establish a strategy to conduct [redacted] at Processing and Distribution Centers [redacted] and [redacted] is correct.

Recommendation #4
We recommend the **Vice President, Network & Compute Technology**, develop a process for verifying that physical access points are labeled in accordance with policy.

Finding #3: Visibility of Wireless Devices

The NCT group was not aware [redacted] at Postal Service facilities. Specifically, at the four sites we visited, we identified [redacted]. According to best practices,[15] organizations should conduct a wireless spectrum survey to identify existing wireless devices and sources of interference in their facilities. While it is not clear as to how the devices were identified, according to the Postal Service, [redacted] were found [redacted] and had to be removed due to interferences with the Postal Service network. Management was not aware of these [redacted] because there are no established procedures for how to account for [redacted] at Postal Service facilities. Lack of awareness of [redacted] could leave the [redacted], therefore delaying the [redacted].

> *"According to best practices, organizations should conduct a wireless spectrum survey to identify existing wireless devices and sources of interference in their facilities."*

Recommendation #5
We recommend the **Vice President, Network & Compute Technology**, establish procedures to account for [redacted] and coordinate with appropriate personnel to remove [redacted] networks.

14 Handbook AS-805, Section 14-2.1, Regular Testing of Security Systems and Processes.
15 National Institute of Standards and Technology, Advanced Manufacturing Series 300-4, *Guide to Industrial Wireless Systems Deployments*, dated April 2018.

Management's Comments

Management agreed with all findings and recommendations.

Regarding finding 2, management stated that Management Instruction AS-850-2002-13, Naming Standards for Devices on the Postal Service Managed Network Services (MNS) Network and Implementation of Asset Management, is not currently in effect. However, they agreed to modify the labeling policy.

Regarding recommendation 1, management agreed to strengthen [redacted] The target implementation date is July 31, 2023.

Regarding recommendation 2, management agreed to [redacted]. Management also stated that no other applications depend on these protocols. The target implementation date is August 31, 2022.

Regarding recommendation 3, management agreed to implement a digital strategy and process to conduct inventory reconciliations of wireless access points in [redacted] The target implementation date is February 28, 2023.

Regarding recommendation 4, management agreed that the current policy is outdated and plans to modify the naming policy to use [redacted]. The target implementation date is December 31, 2022.

Regarding recommendation 5, management agreed to establish a process to [redacted] and determine the appropriate personnel to [redacted]. The target implementation date is April 30, 2023.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report. Action plans to address these recommendations should resolve the issues identified in this report.

Regarding finding 2, although management noted the relevant management instruction is not currently in effect, it was the policy provided during our audit. However, as noted in response to recommendation 4, management agreed to modify the naming policy to use [redacted]. This should address our concern about standardizing inventory management system information.

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.

Appendices

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

Appendix A: Additional Information

Scope and Methodology

Our audit scope included the universe of 39,385 wireless APs located at Postal Service mail processing and delivery facilities that rely on wireless connectivity to support operations. We selected a judgmental sample of these facilities to assess and evaluate the effectiveness of wireless network security controls. Our sample included one facility in each area that had an inventory count of between 25 and 100 APs.

To accomplish our objective, we:

- Conducted a site survey to validate and identify potential vulnerabilities and/or misconfigurations that would allow [redacted]
- Reviewed wireless network architecture and configuration requirements for wireless devices.
- Interviewed key officials to review and evaluate the deployment program for wireless devices and systems.
- Reviewed wireless connectivity for selected sites that house and/or support the Postal Service's critical mail processing and delivery infrastructure.
- Reviewed and evaluated security controls to identify, protect, and monitor wireless access points, radio frequency identification and/or Bluetooth devices, and network connectivity to determine compliance with Postal Service policy and industry best practices.
- Used [redacted] to identify [redacted] and analyzed [redacted] to identify and attempt to [redacted] for the selected facilities.
- Discussed root cause of identified issues with Postal Service officials.

We conducted this performance audit from September 2021 through August 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 June 8, 2022 and included their comments where appropriate.

We assessed the reliability of computer-generated data by analyzing and reviewing the raw data, performing [redacted] 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

The OIG identified no prior audits or reviews related to the objective of this audit within the last five years.

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

August 8, 2022

John Cihota,
Director, Audit Services

SUBJECT: **Wireless Assessment (DR-221)**

Finding #1:
Management agrees with the finding and will implement fixes as outlined in recommendations #1 and #2 below.

Finding #2:
Management agrees with the finding and will develop strategy as outlined in recommendation #3. Management disagrees that physical labeling requirements should comply with Management Instruction AS-850-2002-13, *Naming Standards for Devices on the Postal Service Managed Network Services (NMS) Network and Implementation of Asset Management*, dated October 2002. This Management Instruction is not currently in effect. Management agrees to modify the labeling policy as outlined in recommendation #4.

Finding #3:
Management agrees with the finding and will implement a process to address [redacted] that interfere with USPS devices as outlined in Recommendation #5.

Recommendation #1:
We recommend the **Vice President, Corporate Information Security Office**, and **Vice President, Network & Compute Technology**, properly implement [redacted] to prevent [redacted] from [redacted] to the wireless network.

Management Response/Action Plan:
Management agrees to strengthen [redacted] from [redacted] to the Postal wireless network.

Target Implementation Date:
July 31, 2023

Responsible Official:
Vice President, Network & Compute Technology

Recommendation #2:
We recommend the **Vice President, Corporate Information Security Office**, and **Vice President, Chief Technology Office**, disable [redacted] and implement the use of secure methods to [redacted]

Management Response/Action Plan:
Management agrees with this recommendation and has confirmed the [redacted] identified in the assessment can be [redacted] with no adverse effect on mail processing operations. There are [redacted] on these [redacted] subsequently they are scheduled to be [redacted] with a target implementation date by the end of August.

Target Implementation Date:
August 31, 2022

Responsible Official:
Vice President, USPS Engineering Systems, Chief Technology Office

Recommendation #3:
We recommend the **Vice President, Network & Compute Technology,** establish a strategy to [redacted] at Processing and Distribution Centers to [redacted] inventory and [redacted] is correct.

Management Response/Action Plan:
Management agrees and will implement a digital strategy and process to conduct inventory reconciliations of Processing and Distribution Centers [redacted]

Target Implementation Date:
Feb 28, 2023

Responsible Official:
Vice President, Network & Compute Technology

Recommendation #4:
We recommend the **Vice President, Network & Compute Technology,** develop a process for verifying that physical access points are labeled in accordance with policy

Management Response/Action Plan:
Management agrees. The naming policy for wireless devices will be modified to use [redacted] to identify wireless assets.

Target Implementation Date:
Dec 31, 2022

Responsible Official:
Vice President, Network & Compute Technology

Recommendation #5:
We recommend the **Vice President, Network & Compute Technology,** establish procedures to [redacted] in Postal Service facilities and coordinate with appropriate personnel to [redacted] if they are a [redacted] of [redacted] on Postal Service networks

Management Response/Action Plan:
Management agrees to establish a process to identify and alert [redacted] that [redacted] with Postal [redacted] An evaluation will determine the appropriate personnel to [redacted]

Target Implementation Date:
Apr 30, 2023

Responsible Official:
Vice President, Network & Compute Technology

E-SIGNED by William.E Koetz
on 2022-08-08 14:32:25 CDT

William E. Koetz
Vice President, Network & Compute Technology

E-SIGNED by Heather.L Dyer
on 2022-08-08 14:22:24 CDT

Heather L. Dyer
Vice President, Corporate Information Security Office

E-SIGNED by Linda.M Malone
on 2022-08-08 14:04:50 CDT

Linda M. Malone
Vice President, Chief Technology Office

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