Mobile Delivery Device Security Controls Assessment

AUDIT REPORT

Report Number 22-175-R23 | July 7, 2023

Table of Contents

Highlights

Background

The U.S. Postal Service (USPS) must provide customers and employees visibility into where packages are in the mail stream to be competitive and support package growth. The Postal Service recently invested nearly [redacted] million to purchase and deploy 284,000 Mobile Delivery Device-Technology Refresh (MDD-TR) scanners at Postal facilities. Carriers use these handheld scanners to track package delivery in real-time. These scanners are supported by multiple cellular service providers to collect and transmit data to other Postal Service applications. Therefore, adequate security controls and scanning accuracy are important to protect Postal Service resources and support growth in the package delivery business.

What We Did

Our objective was to assess the security controls of the MDD-TRs deployed at Postal Service facilities. Specifically, we performed testing on the devices using automated tools and manual review techniques to evaluate the devices' security controls and functionality.

What We Found

Generally, the Postal Service successfully completed the deployment of MDD-TRs and effectively configured the devices to only allow package scanning activities. However, they [redacted] and carriers [redacted] before performing [redacted].

These issues occurred because the [redacted] we identified [redacted]. Specifically, management [redacted] on the MDD-TRs, which would have [redacted]. Additionally, [redacted]

Recommendations

We made four recommendations including that management properly [redacted] on the MDD-TRs, disable/deactivate the [redacted] on [redacted] devices, implement [redacted] on the MDD-TRs.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 7, 2023

MEMORANDUM FOR: SCOTT BOMBAUGH
VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

PRITHA MEHRA,
VICE PRESIDENT, CHIEF INFORMATION OFFICER

FROM: Wilvia Espinoza
Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report - Mobile Delivery Device Security Controls Assessment
(Report Number 22-175-R23)

This report presents the results of our Mobile Delivery Device Security Controls Assessment.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Laura Roberts, 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 audit of the Mobile Delivery Device (MDD) Security Controls Assessment (Project Number 22-175). The objective was to assess the security controls of the Mobile Delivery Device-Technology Refresh (MDD-TR) scanners deployed at U.S. Postal Service facilities. See Appendix A for additional information about this audit.

Background

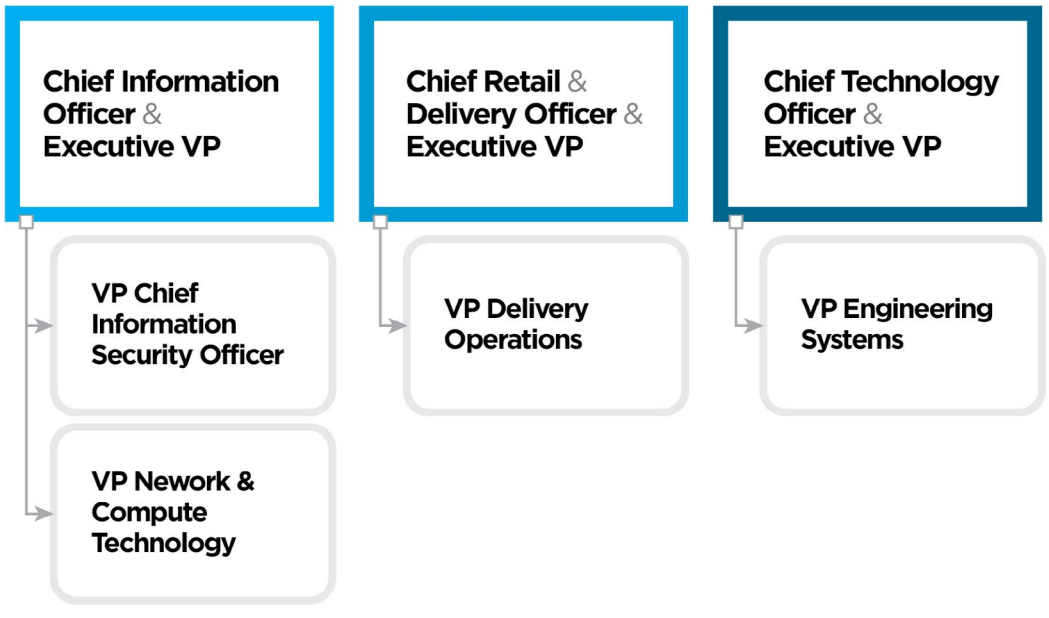
Mobile Delivery Device (MDD) Program

The Postal Service processes and delivers about 23.8 million packages each day and is committed to sustaining this package volume growth.[1] The MDD program[2] supports this effort by providing employees and customers with near real-time package delivery tracking. The program involves several groups that oversee the management, deployment, and operation of mobile scanners. Delivery Operations manages and implements delivery policies and procedures. They work closely with Engineering Systems to design and deploy technical solutions for the scanners. The Corporate Information Security Office (CISO) develops security policies, provides security testing, and approves network device connections. Finally, the Network and Compute Technology office is responsible for the digital networks that allow applications and employees to communicate and interact. Figure 1 displays the various groups involved in the MDD program.

"The Postal Service processes and delivers about 23.8 million packages each day and is committed to sustaining this package volume growth. The MDD program supports this effort by providing employees and customers with near real-time package delivery tracking."

Figure 1. Groups Responsible for the MDD Program

Source: U.S. Postal Service Office of Inspector General (OIG) derived based on USPS Organizational Chart, as of May 4, 2022.



1 Facts.usps.com and Postal Service Blue Page, City Delivery – Mobile Delivery Devices (MDD and MDD-TR) (usps.gov).
2 MDD program refers to all scanners used to support package tracking and delivery, which includes scanners used by carriers and the legacy scanners used in the office to support post office box deliveries and caller services.

MDD Legacy Upgrade and Investment

The MDD program commenced in 2014 with the launch of the legacy MDD,[3] which was in operation for carrier use from 2014 to 2019. This was followed by the launch of the MDD-TR,[4] which is currently in operation (See Figure 2).

Figure 2. Mobile Delivery Device Deployed for Carrier Use

Source: Postal Service MDD-TR introduction presentation, dated January 14, 2020.

In 2019, the legacy MDDs reached the end of their useful life and cellular service providers moved from 3G to 4G technology.[5] As a result, the Postal Service initiated a two phased approach to replace the legacy scanners with a total investment cost of [redacted] million.[6] This investment included the testing, deployment, training, and purchase of 284,000[7] MDD-TR scanners. The Postal Service successfully replaced all existing legacy MDDs used by carriers with new MDD-TRs by the planned completion date of September 6, 2021. These new devices maintained real-time delivery scanning and core functionality of the legacy MDDs, but also included the following enhancements:

- Updated 4G cellular network service
- Improved Global Positioning System
- More memory
- Faster central processing unit
- Higher resolution camera
- Improved battery life
- Bluetooth capability
- Enhanced touch-screen user interface

The MDD-TR scanner uses [redacted] to collect delivery scan data and transmit it to other Postal Service applications. For example, Product Tracking and Reporting houses all delivery status information for mail and parcels with trackable services and barcodes, and the Time and Attendance Collection System (TACS)[8] records carrier workhours for payroll purposes. Therefore, it is crucial to implement security controls that ensure information is protected against unauthorized disclosure, information technology resources operate correctly, and stored information is accurate. These security controls include [redacted] management, which involves [redacted]

Findings Summary

The Postal Service effectively implemented [redacted] security controls and configured the device to only allow carriers to use the scanners for approved functions. However, opportunities exist to improve required [redacted]

Finding #1: MDD-TR Security Controls

We evaluated the Postal Service's adherence to the security requirements and implementation of four security controls[11] on the MDD-TRs. These controls were identified in the supplier's statement of work and Postal Service policy. We found that the

3 The legacy devices are the MDD In Office (MIO) and Intelligent Mail Devices (IMDs) used to support back-office functions.
4 The latest version of the mobile delivery devices used on carrier routes.
5 Refers to generations of cellular technology that enables mobile telecommunication.
6 Decision Analysis Report Business Case Mobile Delivery Device Technology Refresh – Phase 1 Program, Engineering Systems, [redacted] million investment, May 2, 2019. Decision Analysis Report Business Case Mobile Delivery Device Technology Refresh – Phase 2 Program, Engineering Systems, [redacted] million investment, January 24, 2020.
7 75,000 devices purchased under Phase 1 and 209,000 devices purchased under Phase 2.
8 The TACS application was added to the MDD-TRs in July 2021.
9 [redacted]
10 [redacted]
11 [redacted]

Postal Service [redacted] as required by policy. Specifically, the Postal Service [redacted]

> "We found that the Postal Service [redacted] as required by policy."

[redacted]

MDD-TR [redacted]

The Postal Service [redacted] on the MDD-TRs. During our testing, we found that the MDD-TR [redacted]

[redacted]

Postal Service policy states that mobile computing information resources must be protected against damage, unauthorized access, and theft.[20] Policy also states that new devices and software must be evaluated prior to receiving access to the Postal Service network.[21] Further, policy states that the network infrastructure must be protected through security testing.[22]

These issues occurred because [redacted] we identified were not [redacted] Specifically, management stated that the [redacted] In addition, management [redacted] on the MDD-TRs and could not explain why [redacted]. Further, while there was a modification to the master

12 [redacted]
13 [redacted]
14 [redacted]
15 [redacted]
16 [redacted]
17 [redacted]
18 [redacted]
19 [redacted]

20 Handbook AS-805, *Information Security*, Section 10-2.5, Mobile Computing Devices, dated June 2021.
21 Handbook AS-805, *Information Security*, Section 10-2.7.5, Network Access Control, dated June 2021.
22 Handbook AS-805, *Information Security*, Section 11-1.2, Network Infrastructure, dated June 2021.

contract in April 2019, which made [redacted] available for use on MDD-TR scanners, management believed [redacted] In April 2023, management began conducting testing to implement the [redacted] on the MDD-TR scanners.

In addition to the risk that a [redacted] we identified [redacted] MDD-TRs as [redacted] since deployment between September 6, 2021, and May 23, 2023. These [redacted] devices pose a greater risk of [redacted]

The Postal Service is at risk to spend an additional [redacted] MDD-TRs. We consider this amount as funds that could have been put to better use,[25] since this service was previously added to the master contract. However, Postal Service has the option to offset this cost with an [redacted] supplier and is working to remedy the [redacted] as of May 2023.

Recommendation #1

We recommend the **Vice President, Engineering Systems**, [redacted] the Mobile Delivery Device-Technology Refresh [redacted]

Recommendation #2

We recommend the **Vice President, Engineering Systems**, disable/deactivate the Mobile Delivery Device-Technology Refresh [redacted]

Recommendation #3

We recommend the **Vice President, Chief Information Security Officer**, perform security testing on the Mobile Delivery Devices-Technical Refresh scanners to ensure compliance with internal policy.

[redacted]

The Postal Service [redacted] on the MDD-TRs to prevent carriers from [redacted] To operate the devices, a carrier must [redacted] as shown in Figure 3.

According to Postal Service policy,[26] internal users must identify and authenticate themselves to the information resource before being allowed to perform any other actions. Policy also states[27] all managers must ensure that access to information resources is immediately revoked for personnel due to a transfer, change in job responsibilities, routine separation, or involuntary termination.

Figure 3. MDD-TR User Log-in Process

Source: Postal Service MDD Release R7.20 Service Talk.

23 [redacted]
24 Count of MDD-TRs serviced by [redacted] suppliers. The remaining [redacted] MDD-TRs will receive the [redacted] at no cost.
25 Funds that could be used more efficiently by implementing recommended actions.
26 Handbook AS-805, *Information Security*, Section 9-6, Authentication, dated June 2021.
27 Handbook AS-805, *Information Security*, Section 9-3.2.7, Revoking Access, dated June 2021.

During our audit, we reviewed stop-the-clock (STC) scans[28] between September 30, 2022, and December 30, 2022, and identified 253,003 scans performed by carriers using the [redacted]. For example, the [redacted]. In addition, we found that these [redacted] can be used to [redacted]. For example, from October 11, 2022, through October 29, 2022, the [redacted] to conduct STC scans.

As previously stated, management only [redacted]. Therefore, the [redacted] was never considered until the [redacted] was integrated with the devices in July 2021. [redacted]

To address this issue, in July 2022, management developed trainings and implemented the [redacted] that was sent to National, Area, and District levels to identify and resolve [redacted]. While these actions provide visibility, additional [redacted] are needed to ensure the scanners [redacted].

Without [redacted] on the MDD-TRs, issues with [redacted] will continue. In addition, there is an increased potential of [redacted]. For example, we identified 5,246 out of 205,221 (3 percent) missing packages[30] [redacted] between September 30, 2022, and December 30, 2022. When inaccurate scans occur, management [redacted]

In one location we visited, we found supervisors relied on [redacted], as shown in Figure 4. This practice allowed carriers to [redacted] would prevent carriers from [redacted].

Figure 4. [redacted] Printout Posted at a Postal Service Facility

[redacted]

Source: OIG photograph taken at the Hilburn Annex, Raleigh North Carolina on March 2, 2023. The length of time the printout was posted is unknown.

Recommendation #4

We recommend the **Vice President, Engineering Systems**, implement [redacted] controls on the Mobile Delivery Devices-Technology Refresh to prevent the use of [redacted] to the device.

28 A scan that indicates the Postal Service has attempted to or delivered a package.
29 [redacted]
30 Missing package data queried from the Enterprise Data Warehouse system merged against the [redacted] to identify [redacted]

Management's Comments

Management partially disagreed with the findings, agreed with all recommendations, and generally agreed with the monetary impact.

Regarding finding 1, management stated [redacted] They met with the OIG and observed [redacted] In addition, management stated the CISO Risk team conducted a security assessment of the MDD-TRs and provided the Authority To Operate (ATO) to the OIG, [redacted] MDD-TR devices did not occur in 2020 due to inventory issues.

Regarding recommendation 1, management will utilize features provided by cellular service providers [redacted] The target implementation date was June 30, 2023.

Regarding recommendation 2, management will review and update the [redacted] process and include a specific procedure to [redacted] during processing. The target implementation date is July 30, 2023.

Regarding recommendation 3, management performed penetration testing on the MDD-TRs, and requested closure of this recommendation upon issuance of the report. The target implementation date was June 30, 2023.

Regarding recommendation 4, management stated they are working with [redacted] to gain approval [redacted] to the device. The target implementation date is August 31, 2023.

Regarding monetary impact, during discussions after management provided its official comments, they agreed in principle but stated the specific amount should be [redacted], based on [redacted] devices at a charge of [redacted].

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

Evaluation of Management's Comments

The OIG considers management comments responsive to the recommendations and the actions planned to address these recommendations should resolve the issues identified in the report.

Regarding finding 1, as stated in the report and verified by the CISO penetration testing team, [redacted] In addition, the ATO only acknowledges that the CISO Risk team conducted security assessments for the [redacted]. Further, the audit team held several meetings with the CISO team to determine [redacted] MDD-TRs and management stated they could not provide a reason.

Regarding recommendation 1, during discussions after management provided its official comments, management provided an email that included a screenshot of a chart showing the count of MDD-TRs with [redacted] we found the information was not sufficient support to close this recommendation. In addition, a copy of the contract modification with the cellular service provider that outlines the [redacted] was not provided. Therefore, we cannot close this recommendation upon issuance of this report. Management stated their revised target implementation date is July 31, 2023.

Regarding recommendation 3, management provided support that the CISO Risk team completed a penetration test on the MDD-TR scanners. The documentation included the testing methodology, findings summary, and remediations made by the CISO Risk team. Therefore, we agree to close this recommendation upon issuance of this report.

In response to the monetary impact, management provided its own calculation with supporting

documentation for [redacted] devices. However, based on our analysis, we could identify only [redacted] MDD-TRs that received the [redacted]. Therefore, we are revising the monetary amount from [redacted].

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

Recommendations 1, 2, and 4 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. We consider recommendation 3 closed with the issuance of this report.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our scope included the review of the MDD-TRs, supporting infrastructure, and the related contract and statement of work.

To accomplish our objective, the audit team:

- Reviewed Decision Analysis Reports Business Case MDD-TR – Phase 1 and 2, Statement of Work, and related MDD-TR training materials and the MDD-TR configuration manual to determine whether the program achieved its goals.
- Evaluated the MDD-TR approved functionalities/capabilities and type of data it gathers and stores.
- Determined if the MDD-TRs security controls are implemented in accordance with Postal Service security policies, procedures, and supplier's statement of work.
- Reviewed 61,005 MDD-TR helpdesk tickets submitted between April 5, 2021, and November 5, 2022, to identify common issues with the MDD-TR.
- Performed security control testing on the MDD-TRs using both automated tools and manual review techniques to evaluate security controls, updates, and device configurations.
- Interviewed key personnel to gain an understanding of the management, support, and use of the MDD-TRs.

We conducted this review from September 2022 through July 2023 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 objectives. 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 7, 2023, 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

The OIG did not identify any 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

June 29, 2023

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Mobile Delivery Device Security Controls Assessment Report Number 22-175-DRAFT

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft audit report, *Mobile Delivery Device Security Controls Assessment*.

With regard to the OIG findings, CISO previously expressed concerns and disagreement with the following findings and would like to clarify our position.

OIG Statement: [redacted]

CISO Comment: [redacted]

OIG Statement: "In addition, management [redacted] on the MDD-TRs and could not explain why [redacted]."

CISO Comment: The CISO Risk team conducted a security assessment of the MDD-TRs. CISO provided the ATO to the OIG. [redacted] MDD-TR devices did not occur in 2020 due to inventory issues.

Following are our comments on each of the four recommendations.

Recommendation [1]:
We recommend the **Vice President, Engineering Systems**, [redacted] the Mobile Delivery Device-Technology Refresh [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. We will utilize the features provided by the cellular service providers [redacted]

Target Implementation Date: 06/30/2023.

Responsible Official:
Manager, Delivery & Mobile Technology at Engineering Systems is the postal official responsible for implementing recommendation.

Recommendation [2]:
We recommend the **Vice President, Engineering Systems**, disable/deactivate the Mobile Delivery Device-Technology Refresh [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. This is done in today's environment, but opportunities exist to improve the process and [redacted] We will review and update the [redacted] process and include a specific procedure to [redacted] during processing.

Target Implementation Date: 07/30/2023

Responsible Official:
Manager, Delivery & Mobile Technology at Engineering Systems is the postal official responsible for implementing recommendation.

Recommendation [3]:
We recommend the **Vice President, Chief Information Security Officer**, perform security testing on the Mobile Delivery Devices-Technical Refresh scanners to ensure compliance with internal policy.

Management Response/Action Plan:
Management agrees with this recommendation. Management has completed penetration testing and request to close the recommendation.

Target Implementation Date: 06/30/2023

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [4]:
We recommend the **Vice President, Engineering Systems**, implement [redacted] controls on the Mobile Delivery Devices-Technology Refresh to prevent the use of [redacted] to the device.

Management Response/Action Plan:
Management agrees with this recommendation and is working with [redacted] to gain approval [redacted] to the device.

Target Implementation Date: 08/31/2023

Responsible Official:
Manager, Delivery & Mobile Technology at Engineering Systems is the postal official responsible for implementing recommendation.

E-SIGNED by SCOTT.R BOMBAUGH
on 2023-06-29 11:51:08 CDT

Scott Bombaugh
Chief Technology Officer

E-SIGNED by Pritha Mehra
on 2023-06-29 14:48:10 CDT

Pritha Mehra
Chief Information Officer

cc: *Corporate Audit & Response Management*

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