Security of Postal Service Smartphones

AUDIT REPORT

Report Number 24-009-R24 | July 26, 2024

Table of Contents

Highlights

Background

The U.S. Postal Service issued approximately 27,000 smartphones to its employees to provide telecommunication and connectivity to its information systems and work-related applications. Although smartphones offer opportunities to improve business productivity, they also introduce the risk of cyber threats that could compromise sensitive Postal Service data. Given the level of access a smartphone offers to its internal network, it is imperative the Postal Service appropriately secures its smartphones to mitigate the risk to its data and systems.

What We Did

Our objective was to assess the security of the Postal Service's smartphones. For this audit, we used a combination of data analytics, interviews, and control tests to determine if appropriate controls were in place and functioning as intended to protect the smartphones and Postal Service data.

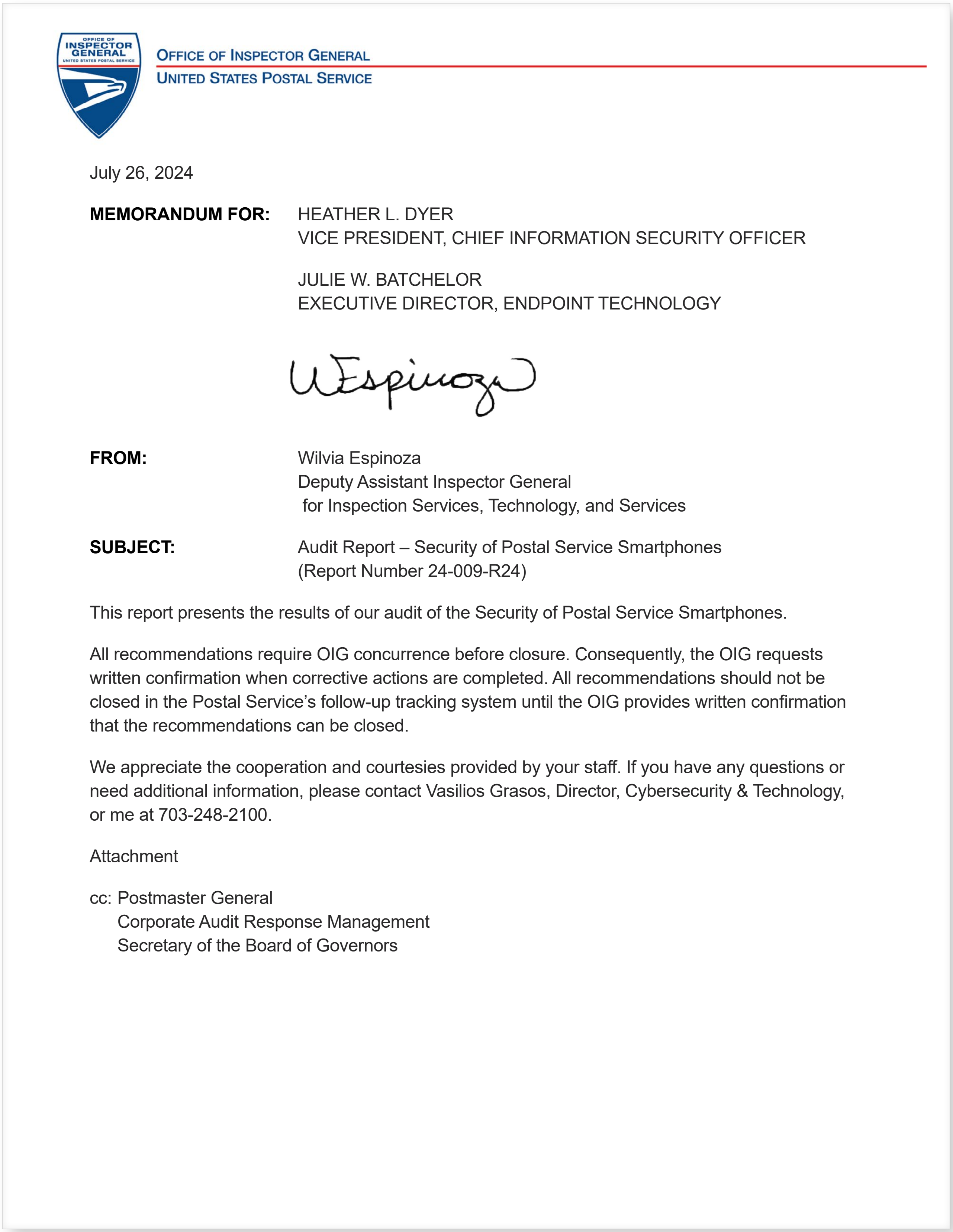
What We Found

The Postal Service's mobile device management platform (MDM) allows information technology staff to control, secure, and enforce policies on applications and operating systems installed on smartphones. The Postal Service did not fully utilize the MDM to adequately restrict the installation of or remove unapproved applications from its smartphones. Additionally, the Postal Service did not force operating system updates or quarantine smartphones without current operating systems. These issues occurred because the Postal Service did not monitor smartphones for unapproved applications or outdated operating systems, nor did it have a policy to do so. The underutilization of the MDM has led to about $4.7 million in questioned cost and funds put to better use.

Recommendations and Management's Comments

We made three recommendations to address the security of applications and operating systems installed on the Postal Service's smartphones. Postal Service management agreed with all recommendations. The U.S. Postal Service Office of Inspector considers management's comments responsive to all three recommendations, as corrective actions should resolve the issues identified in the report. See Appendix B for management's comments in their entirety.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 26, 2024

MEMORANDUM FOR: HEATHER L. DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

JULIE W. BATCHELOR
EXECUTIVE DIRECTOR, ENDPOINT TECHNOLOGY

WEspinoza

FROM: Wilvia Espinoza
Deputy Assistant Inspector General
for Inspection Services, Technology, and Services

SUBJECT: Audit Report – Security of Postal Service Smartphones
(Report Number 24-009-R24)

This report presents the results of our audit of the Security of Postal Service Smartphones.

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.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Vasilios Grasos, Director, Cybersecurity & Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management
Secretary of the Board of Governors

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Security of Postal Service Smartphones (Project Number 24-009). Our objective was to assess the security of the Postal Service's smartphones. See Appendix A for additional information about this audit.

Background

To assist U.S. Postal Service employees in carrying out their duties, the Postal Service issues smartphones that provide telecommunication and connectivity to its information systems using work-related applications. Smartphones help share on-the-go information and run various software applications based on individual needs. These devices provide access to much of the same Postal Service data and systems that are available from a computer and have a greater risk of cyber threats that could compromise sensitive Postal Service data. For example, according to a 2023 study, 80 percent of phishing[1] attacks targeted mobile devices.[2] As of February 2024, individuals across various Postal Service departments used about 27,000 smartphones. Given the level of access a smartphone offers to its internal network, it is imperative that the Postal Service appropriately secures its smartphones to mitigate risk to its data and systems.

Smartphone Cybersecurity Threats

The Postal Service created the Mobile Protection Initiative for mobile application security to protect itself from rising cyberthreats. This initiative states that only approved, business-related applications are allowed to be installed on Postal Service issued smartphones. As of March 2024, the Postal Service's Authorized Applications list consisted of 1,174 applications.

Smartphones using outdated operating systems[3] or unapproved applications are more susceptible to security risks, such as malware[4] and hacking attempts. The Postal Service uses both iPhones and Androids, which are common smartphones that receive regular security updates[5] to address vulnerabilities in the operating systems. The updates are crucial to protect the Postal Service's network and sensitive information. Therefore, it is imperative that the Postal Service safeguards smartphones by:

- Keeping operating systems updated.
- Vetting applications to detect software or configuration flaws that may create vulnerabilities or violate enterprise security or privacy policies.
- Quarantining[6] non-compliant smartphones from Postal Service resources.

Smartphone Oversight

Within the Postal Service, the Chief Information Officer (CIO) has the overall responsibility to manage smartphones, which includes establishing security standards for mobile devices as well as providing administrative support, operations, and device monitoring. The CIO is also responsible for securely configuring devices and allowing only authorized applications on the devices in compliance with policy.

Under the CIO, there are two groups directly responsible for managing the security of smartphones. The Corporate Information Security Office (CISO) is responsible for centrally managing approved mobile applications, vetting applications, and monitoring installed applications and operating systems for compliance. The Endpoint Technology Engineering (ETE) office is responsible for user support and oversight of the mobile device management (MDM) platform. The Postal Service's MDM platform

[1] A technique to acquire sensitive information by deceiving individuals through deceptive computer-based means.

[2] *2023 Global Mobile* Threat Report, Zimperium, 2023.

[3] A collection of software that manages computer hardware resources and provides common services for computer programs.

[4] Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems.

[5] Security updates are patches or modifications made to software, operating systems, applications, or firmware to address vulnerabilities and improve the overall security of the system.

[6] To isolate a device from the network to prevent the ability to access a system due to noncompliance with internal policies or for other security concerns.

allows information technology staff to control, secure, and enforce policies on applications and operating systems installed on smartphones. Managed applications within the MDM allow the Postal Service to appropriately manage the risk associated with them. This includes identifying and removing unauthorized applications and restricting what applications can be installed. The MDM also has the capability to monitor smartphones by updating operating systems and quarantining devices that are not in compliance with policy.

Finding: Postal Service Did Not Properly Manage the Security of its Smartphones

Overall, we identified opportunities for the Postal Service to improve the security of its smartphones. Specifically, we found ETE did not 1) adequately restrict the installation of or remove unapproved applications from agency smartphones, or 2) force operating system updates or quarantine smartphones using outdated operating systems.

Unapproved Applications

ETE did not manage or prevent the installation of, or remove, unapproved applications from Postal Service smartphones. Specifically, as of December 19, 2023, the Postal Service had 11,676 unapproved applications[7] on its mobile devices, which include smartphones.[8] The Postal Service has not reviewed these applications to determine if they should be blocked or allowed. Further, these applications were not managed within the MDM platform. As of March 2024, the OIG judgmentally reviewed 66 of these unmanaged applications and found they either should have been blocked, were not related to business purposes, or had security related concerns.

The Postal Service had a list of 10 applications that users should not install. However, they do not block or prevent installation of any application on mobile devices. Of the 66 applications we reviewed, we found Postal Service employees installed:

- Three of the 10 disallowed applications (TikTok, Telegram Messenger, CamScanner).
- Nineteen applications not related to business purposes, such as sports betting and dating applications.
- Thirty-eight applications that had security-related concerns, such as those originating from countries that are considered foreign adversaries or that allow users to create virtual private networks (VPN).[9]

According to National Institute of Standards and Technology mobile device guidance, organizations should plan their mobile device security with the assumption that unknown third-party mobile device applications should not be trusted. Further, third-party applications installed on a mobile device could compromise the device and access sensitive information.[10] Therefore, it is important to restrict the installation of unapproved applications.

Applications originating from foreign adversary countries should be reviewed due to security concerns over gathering personal or proprietary information from users.[11] Additionally, unapproved VPN applications could allow Postal employees to bypass security controls on the Postal Service's network to access unauthorized websites.

Outdated Operating Systems

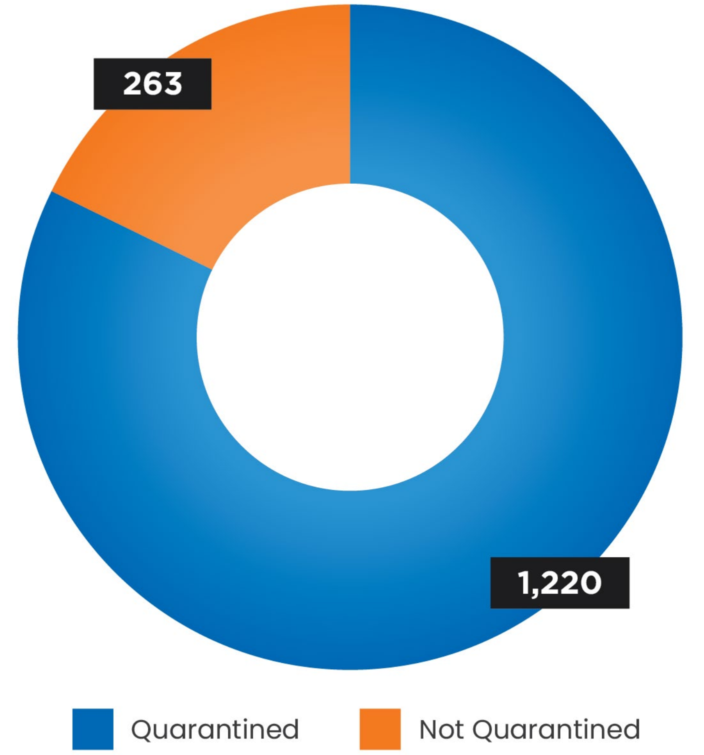
ETE did not ensure Postal Service's smartphones were using updated operating systems and did not quarantine those that were not updated in accordance with policy.[12]

Postal Service Handbook AS-805, *Information Security*, states the CISO has the authority to block or quarantine any asset that does not comply with Postal Service policy and for information technology staff to remove unapproved software. Handbook AS-805 also states that all information resources must use supported operating systems with all updates and patches.

[7] These applications included various versions.
[8] Mobile devices include smartphones, laptops, and tablets. The MDM requires drilling down into each of the 11,676 applications to determine the specific mobile device type.
[9] A virtual network built between existing networks to provide secure communications.
[10] National Institute of Standards and Technology Special Publication 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, May 2023.
[11] Executive Order 14034, Protecting Americans' Sensitive Data from Foreign Adversaries, dated June 2021.
[12] Handbook AS-805, *Information Security*, dated September 2022.

As of February 2024, ETE did not force operating system updates to 1,483[13] (6 percent) of its 26,913 smartphones. In addition, of those 1,483 smartphones, ETE did not quarantine 263 (18 percent) (see Figure 1).

Figure 1: Smartphones with Outdated Operating Systems



Source: OIG analysis of mobile operating systems in the Postal Service's MDM platform.

According to Handbook AS-805, all Postal Service information resources, such as smartphones, must use approved, vendor-supported operating systems, including all approved updates and patches. Operating system updates are to be conducted monthly via automated patch management.[14] The Postal Service's quarantine policy,[15] which only addresses iPhones, states if the device is not updated, it will be placed in quarantine after 9 days using a tiered schedule, as follows:

- Tier 1 – Notification (Once a day for 4 days).
- Tier 2 – Notification (Every 8 hours for 3 days).
- Tier 3 – Notification (Every 4 hours for 2 days).
- Tier 4 – Quarantine (Every 8 hours until the smartphone is updated).

Previously, the USPS Office of Inspector General's *Management of the Postal Service's Smartphones* audit report (22-177-R23) identified 1,286 unsupported smartphones, meaning that they were no longer receiving patches and operating system updates from their respective manufacturers. We recommended those smartphones be replaced with supported smartphones. Of the unsupported smartphones identified in the prior report, we found 40 devices during this audit that had not been replaced, 17 of which were not quarantined. In February 2024, as part of the analysis for this audit, we identified an additional 125 smartphones that did not support current operating systems. On May 23, 2024, we performed further analysis in the MDM to determine if any of the 40 smartphones identified in the previous audit or the 125 smartphones identified during this audit were still active on the Postal Service's network. We found only one of the 125 smartphones was still active on the Postal Service's network in the MDM. Postal Service management is taking corrective action to address this issue, and the original recommendation is now closed. Therefore, we will not be making a recommendation in this report.

These issues occurred because CISO did not monitor smartphones for unapproved applications and outdated operating systems and notify ETE to quarantine noncompliant smartphones or remove unapproved applications. Additionally, the Postal Service did not have policy in place for quarantining smartphones using the Android operating system or fully utilize the capabilities of its MDM platform to 1) block or remove unapproved applications installed by smartphone users; 2) force updates to smartphones that did not have current operating systems; and 3) quarantine smartphones

[13] This number includes unsupported smartphones that cannot hold current operating systems identified in the *Management of the Postal Service's Smartphones* audit report 22-177-R23.
[14] Patch management is the process of acquiring, testing, and installing updates to applications or operating systems to improve functionality, close security vulnerabilities, and optimize performance.
[15] Compliance Policy: Update iOS Version - Notifications and Quarantine, received 8 December 2023.

that had unapproved applications or were missing operating system updates.

The Postal Service paid about [redacted] for its MDM platform licenses for fiscal years (FY) 2022 and 2023.[16] As a result of not using the MDM platform to its fullest capability, we consider about $2.1 million to be questioned cost.[17] Additionally, if the Postal Service does not make changes to its use of the MDM platform, we consider about $2.6 million[18] for FY 2024 and projected for FY 2025, funds put to better use.[19]

Smartphones with unapproved applications are a risk to the Postal Service network because their use and functionality have not been evaluated or approved for use by the Postal Service. These applications could allow access to personal information – such as email contacts, calendar information, call logs, and location data from the device. Additionally, smartphones running outdated operating systems could potentially allow bad actors to exploit vulnerabilities to attack the Postal Service's network and gain access to sensitive information.

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Executive Director, Endpoint Technology**, identify and remove unapproved applications and outdated operating systems on smartphones and/or quarantine noncompliant smartphones.

Recommendation #2

We recommend the **Executive Director, Endpoint Technology**, update the Postal Service's quarantine enforcement process and policy to include provisions for quarantining both iOS and Android smartphones with operating systems missing current security updates, on a recurring basis.

Recommendation #3

We recommend the **Executive Director, Endpoint Technology**, develop a documented plan to fully utilize the capabilities of its mobile device management platform to 1) prohibit employees from installing unapproved applications, 2) identify and remove unapproved applications, 3) force operating system updates to smartphones, and 4) quarantine all smartphones using outdated operating systems.

Postal Service Response

The Postal Service had no comment regarding the finding; however, they disagreed with the monetary impact of $4.7 million, stating that the MDM platform is required for critical business functions and that it is not possible to reduce the cost of the MDM solution and maintain its required business functionality.

Management agreed with recommendations 1, 2, and 3. For recommendation 1, management stated it would develop a process to remove disallowed apps and update its quarantine process to include Android devices (the current process covers iOS devices) without the current operating system security updates, with a target implementation date of January 31, 2025.

For recommendation 2, management stated that iOS devices without current operating system security updates are currently placed into a quarantine state, and they will update the process to include Android devices without the current operating system security updates. The target implementation date is November 27, 2024.

[16] Includes about [redacted] for FY 2022 and about [redacted] for FY 2023.
[17] A cost the OIG believes is unnecessary, unreasonable, or an alleged violation of law, regulation, or contract.
[18] Includes about $1.3 million from FY2024 and conservatively assumes the same amount for FY 2025.
[19] Funds that could be used more efficiently by implementing recommended actions.

For recommendation 3, management stated it would update current policy to prohibit the installation of disallowed applications and prevent them from running. Also, they will develop a process to remove disallowed apps. Finally, they will push operating system updates to smartphones and quarantine those without current operating systems. The target implementation date is January 31, 2025.

OIG Evaluation

Regarding management's disagreement with the monetary impact, the Postal Service paid for critical business capabilities of the MDM that it was not using but should have used to promote effective security of its mobile devices, to include its smartphones.

Management's comments were responsive to recommendations 1, 2, and 3, and corrective actions should resolve the issues identified in the report.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our audit scope included the review of smartphones at the Postal Service. Specifically, we reviewed the security and application management policies and their enforcement.

To accomplish our objective, we:

- Assessed Postal Service policies relating to the security of smartphones.
- Evaluated the effectiveness of the controls over smartphone security management processes and procedures.
- Reviewed smartphone data to determine compliance with policies and best practices, to include whether devices were timely patched, and downloaded applications were authorized.
- Interviewed Postal Service employees on their use and knowledge of smartphones and related security.

We conducted this performance audit from November 2023 through July 2024 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 24, 2024, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the Postal Service's smartphone and mobile device management platform internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the following three components were significant to our audit objective: control activities, information and communication, and monitoring.

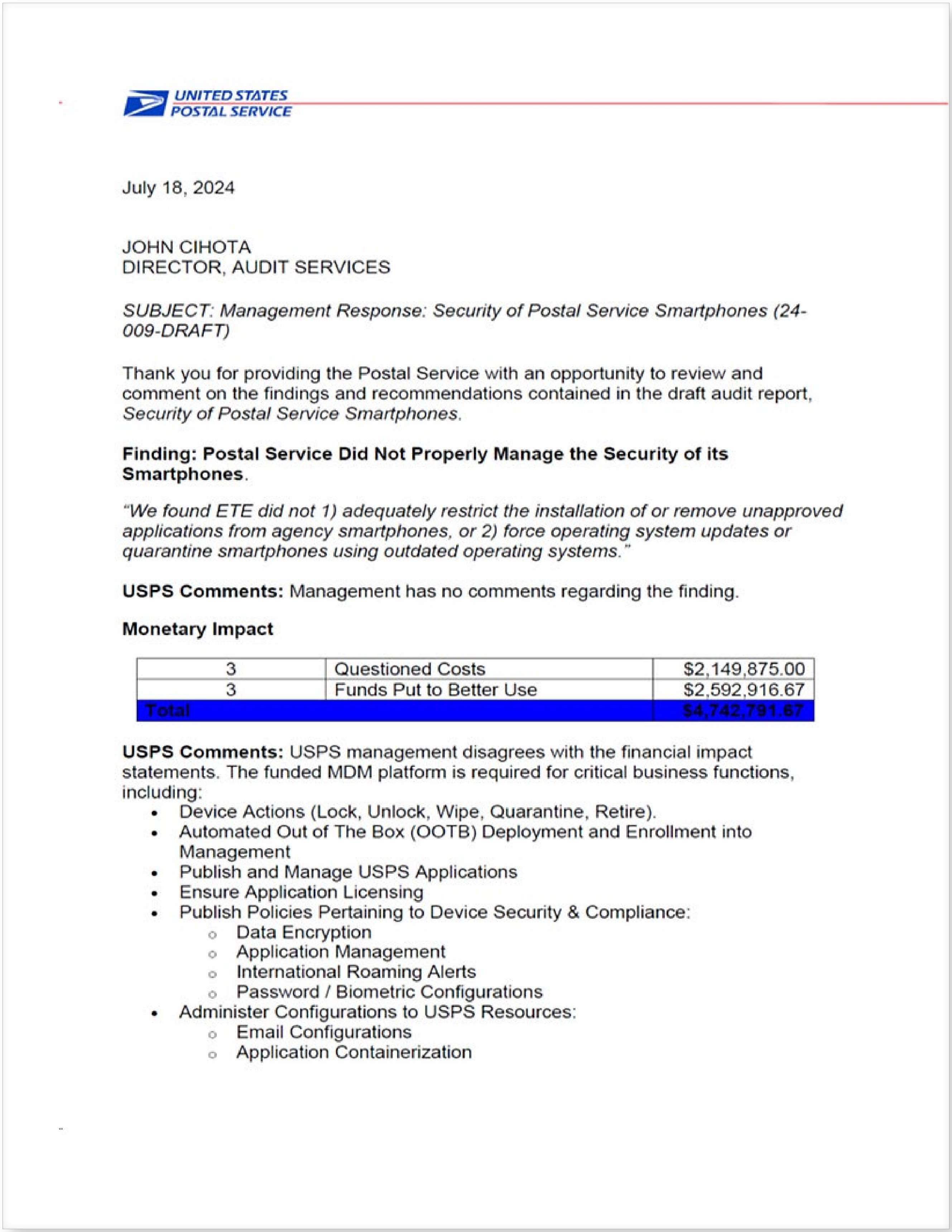
We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to monitoring of the smartphones in the MDM platform that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of computer-generated data by reviewing system controls and the automated processes where data is maintained, and performance testing data using logical tests. We determined that the data was sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Management of the Postal Service's Smartphones	To assess management of the inventory, lifecycle, and utilization of the Postal Service's smartphones.	FR-22-177-R23	August 03, 2023	[redacted]
Mobile Delivery Device Security Controls Assessment	To assess the security controls of the Mobile Device Delivery Tech Refresh deployed at U.S. Postal Service facilities.	FR-22-175-R23	July 07, 2023	[redacted]
Management of the Postal Regulatory Commission's Smartphones	To assess the management of the security, inventory, and utilization of the Postal Regulatory Commission's smartphones.	FR-23-024-R23	June 26, 2023	N/A

Appendix B: Management’s Comments



UNITED STATES POSTAL SERVICE

July 18, 2024

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Security of Postal Service Smartphones (24-009-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, *Security of Postal Service Smartphones.*

Finding: Postal Service Did Not Properly Manage the Security of its Smartphones.

“We found ETE did not 1) adequately restrict the installation of or remove unapproved applications from agency smartphones, or 2) force operating system updates or quarantine smartphones using outdated operating systems.”

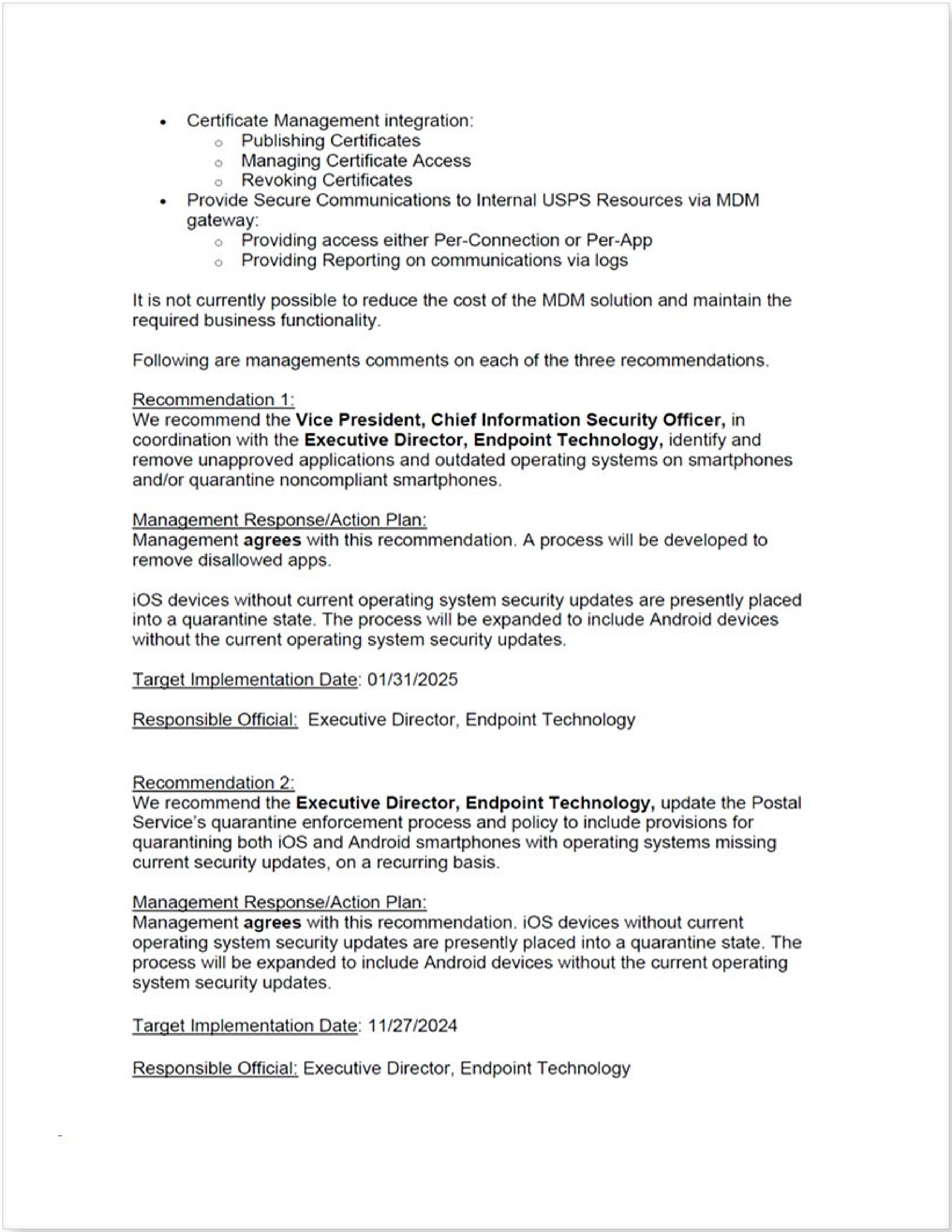
USPS Comments: Management has no comments regarding the finding.

Monetary Impact

3	Questioned Costs	$2,149,875.00
3	Funds Put to Better Use	$2,592,916.67
Total		$4,742,791.67

USPS Comments: USPS management disagrees with the financial impact statements. The funded MDM platform is required for critical business functions, including:

- Device Actions (Lock, Unlock, Wipe, Quarantine, Retire).
- Automated Out of The Box (OOTB) Deployment and Enrollment into Management
- Publish and Manage USPS Applications
- Ensure Application Licensing
- Publish Policies Pertaining to Device Security & Compliance:
  - Data Encryption
  - Application Management
  - International Roaming Alerts
  - Password / Biometric Configurations
- Administer Configurations to USPS Resources:
  - Email Configurations
  - Application Containerization



- Certificate Management integration:
  - Publishing Certificates
  - Managing Certificate Access
  - Revoking Certificates
- Provide Secure Communications to Internal USPS Resources via MDM gateway:
  - Providing access either Per-Connection or Per-App
  - Providing Reporting on communications via logs

It is not currently possible to reduce the cost of the MDM solution and maintain the required business functionality.

Following are managements comments on each of the three recommendations.

Recommendation 1:
We recommend the **Vice President, Chief Information Security Officer,** in coordination with the **Executive Director, Endpoint Technology,** identify and remove unapproved applications and outdated operating systems on smartphones and/or quarantine noncompliant smartphones.

Management Response/Action Plan:
Management **agrees** with this recommendation. A process will be developed to remove disallowed apps.

iOS devices without current operating system security updates are presently placed into a quarantine state. The process will be expanded to include Android devices without the current operating system security updates.

Target Implementation Date: 01/31/2025

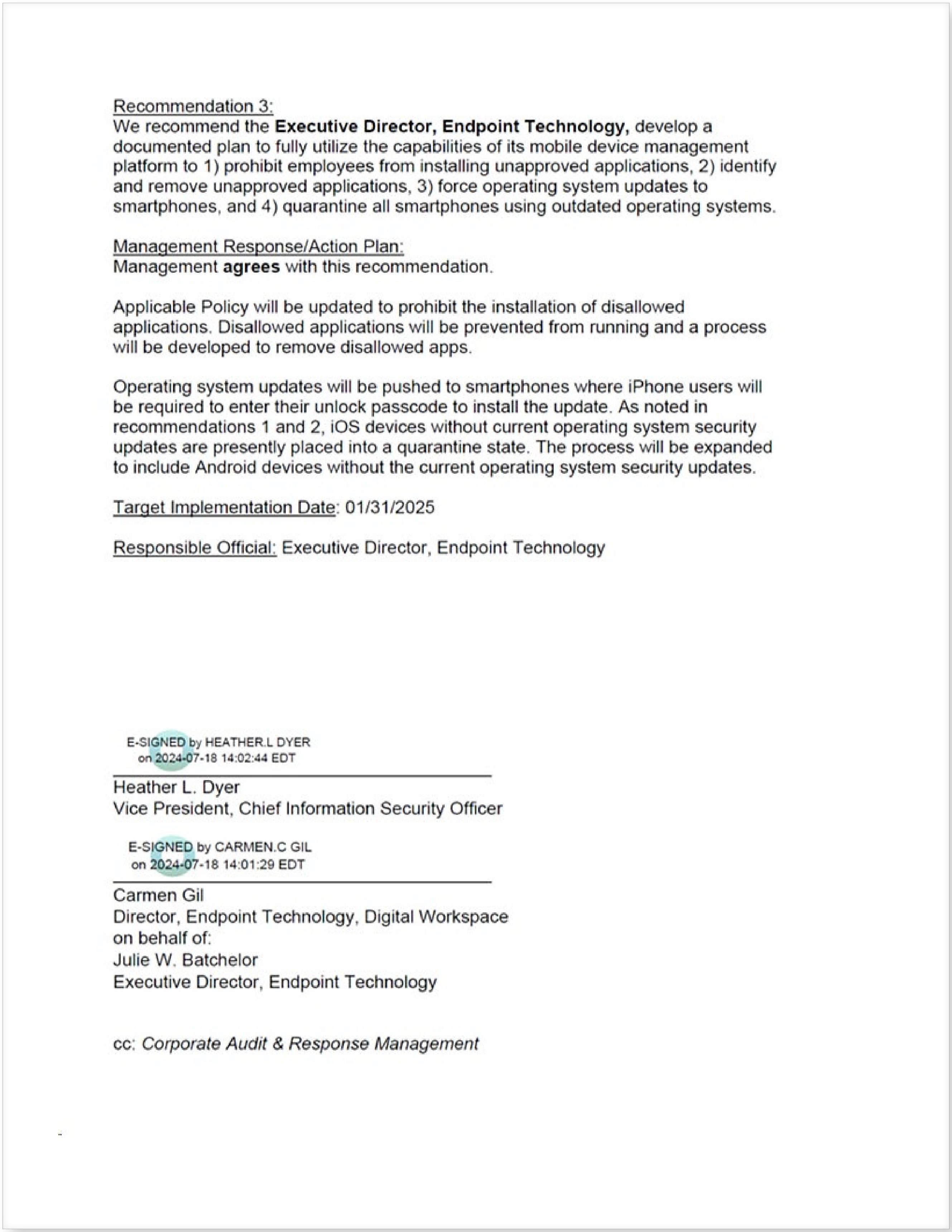
Responsible Official: Executive Director, Endpoint Technology

Recommendation 2:
We recommend the **Executive Director, Endpoint Technology,** update the Postal Service's quarantine enforcement process and policy to include provisions for quarantining both iOS and Android smartphones with operating systems missing current security updates, on a recurring basis.

Management Response/Action Plan:
Management **agrees** with this recommendation. iOS devices without current operating system security updates are presently placed into a quarantine state. The process will be expanded to include Android devices without the current operating system security updates.

Target Implementation Date: 11/27/2024

Responsible Official: Executive Director, Endpoint Technology



Recommendation 3:
We recommend the **Executive Director, Endpoint Technology,** develop a documented plan to fully utilize the capabilities of its mobile device management platform to 1) prohibit employees from installing unapproved applications, 2) identify and remove unapproved applications, 3) force operating system updates to smartphones, and 4) quarantine all smartphones using outdated operating systems.

Management Response/Action Plan:
Management **agrees** with this recommendation.

Applicable Policy will be updated to prohibit the installation of disallowed applications. Disallowed applications will be prevented from running and a process will be developed to remove disallowed apps.

Operating system updates will be pushed to smartphones where iPhone users will be required to enter their unlock passcode to install the update. As noted in recommendations 1 and 2, iOS devices without current operating system security updates are presently placed into a quarantine state. The process will be expanded to include Android devices without the current operating system security updates.

Target Implementation Date: 01/31/2025

Responsible Official: Executive Director, Endpoint Technology

E-SIGNED by HEATHER.L DYER
on 2024-07-18 14:02:44 EDT

Heather L. Dyer
Vice President, Chief Information Security Officer

E-SIGNED by CARMEN.C GIL
on 2024-07-18 14:01:29 EDT

Carmen Gil
Director, Endpoint Technology, Digital Workspace
on behalf of:
Julie W. Batchelor
Executive Director, Endpoint Technology

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