Management of the Postal Regulatory Commission's Smartphones

AUDIT REPORT

Report Number 23-024-R23 | June 26, 2023

Table of Contents

Highlights

Background

The Postal Regulatory Commission (Commission) is an independent agency that exercises regulatory oversight of the U.S. Postal Service. With five commissioners, supported by a staff of approximately 70 individuals, the Commission uses smartphones to facilitate greater working efficiencies and operations, making them a core element of the Commission's IT program.

Smartphones help facilitate communications, share on-the-go information, and run various software applications based on individual need. Often, these devices provide access to much of the same data and systems that would be available from an office desktop. Due to their mobile nature, this can present significant cybersecurity issues if the smartphones are not fully protected.

What We Did

Our objective was to assess the management of the inventory, security, and utilization of the Commission's smartphones. We used a combination of data analytics, interviews, and control tests to determine if appropriate controls were in place and functioning as intended.

> "Overall, we identified opportunities for improvement in the Commission's management of inventory, security, and utilization of smartphones."

What We Found

Overall, we identified opportunities for improvement in the Commission's management of inventory, security, and utilization of smartphones. Specifically, the Commission did not have (1) a standardized process for reviewing and maintaining its inventory; (2) key components to effectively manage the security of its smartphones; and (3) a written policy or procedure to review smartphone utilization billing. These issues occurred because the Commission did not follow a standardized process for inventory and utilization reviews, and it prioritized other IT projects over the security of its smartphones.

Recommendations

We made nine recommendations, including performing routine inventory and utilization reviews in compliance with industry best practices, developing a mobile device security policy, and providing end user smartphone security training.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 26, 2023

MEMORANDUM FOR: ERICA A. BARKER
SECRETARY & CHIEF ADMINISTRATIVE OFFICER

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

SUBJECT: Audit Report - Management of the Postal Regulatory Commission's Smartphones (Report Number 23-024-R23)

This report presents the results of our audit of the Management of the Postal Regulatory Commission's Smartphones.

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

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Management of the Postal Regulatory Commission's Smartphones (Project Number 23-024). Our objective was to assess the management of the inventory, security, and utilization of the Postal Regulatory Commission's smartphones. See Appendix A for additional information about this audit.

Background

Commission Organization

The Postal Regulatory Commission (Commission) is an independent agency that exercises regulatory oversight of the United States Postal Service.[1] It is comprised of five commissioners and supported by approximately 70 employees whose mission is to ensure transparency and accountability of the Postal Service and foster a vital and efficient universal mail system.[2] The Commission was created by the Postal Reorganization Act and assumed expanded responsibilities as a result of the Postal Accountability and Enhancement Act of 2006. The Commission regulates and approves postal rates consistent with legal criteria, advises Postal Service decision-makers on strategic decisions that could impact the nation, collects and publishes cost and service performance data, and analyzes and reports on the Postal Service's strategic plans and finances. The Commission's staff operates with an appropriation of $17.5 million.[3] Ninety-five percent of the Commission's budget is for personnel and lease expenditures, with the remainder largely dedicated to employee development and recurring operational expenses, such as telephone expenses.

The Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), both recently hired, oversee the management and security of IT at the Commission. Together, their department consists of seven individuals. The CISO manages the IT security program by overseeing the security posture of IT systems and devices throughout their lifecycle, applying government-wide IT security requirements, along with ensuring enterprise information systems are integrated and interoperable. The CIO provides advice and assistance on IT acquisitions and ensures information resources are managed consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the Commission. The CIO is also responsible for inventory management and monitoring smartphone utilization. These two individuals both report to the Secretary and Chief Administrative Officer, who oversees the day-to-day functions of budgeting and accounting, human resource management, records and data management, contracts and audits, facilities, and IT.

Commission's Priority IT Initiatives

With these recent changes in IT leadership, Commission management prioritized its IT efforts and limited budget on two distinct, but intertwined, projects that are intended to provide both external and internal data management solutions and enhanced workflow that are critical to the Commission's mission. These projects include replacing its high value assets (electronic docketing system and external website) and increasing its security compliance. The docketing system allows the Postal Service and other parties to file motions, pleadings, comments, and data for review and decisions by the Commission. The external website (PRC.GOV) gives the public access to the docketing system. The security portion of the project will implement best practices to secure the docketing system and website.

Another IT project that the Commission rated as a high priority is a telecommunication enhancements initiative, which includes parts of a mobile device security program. Due to limited resources dedicated to this project, the Commission is in the initial phases of implementation as of April 2023.

1 About the Postal Regulatory Commission (PRC) (prc.gov/about).
2 Mission, Vision, Guiding Principles, and Strategy (prc.gov/mission).
3 Commission's enacted budget for fiscal year 2022.

Smartphones at the Commission

The Commission uses smartphones[4] to facilitate greater working efficiencies and operations, making them a core element of the Commission's IT program. Often, these devices provide access to much of the same data and systems that would be available from an office desktop computer.

Best Practices for Smartphone Security

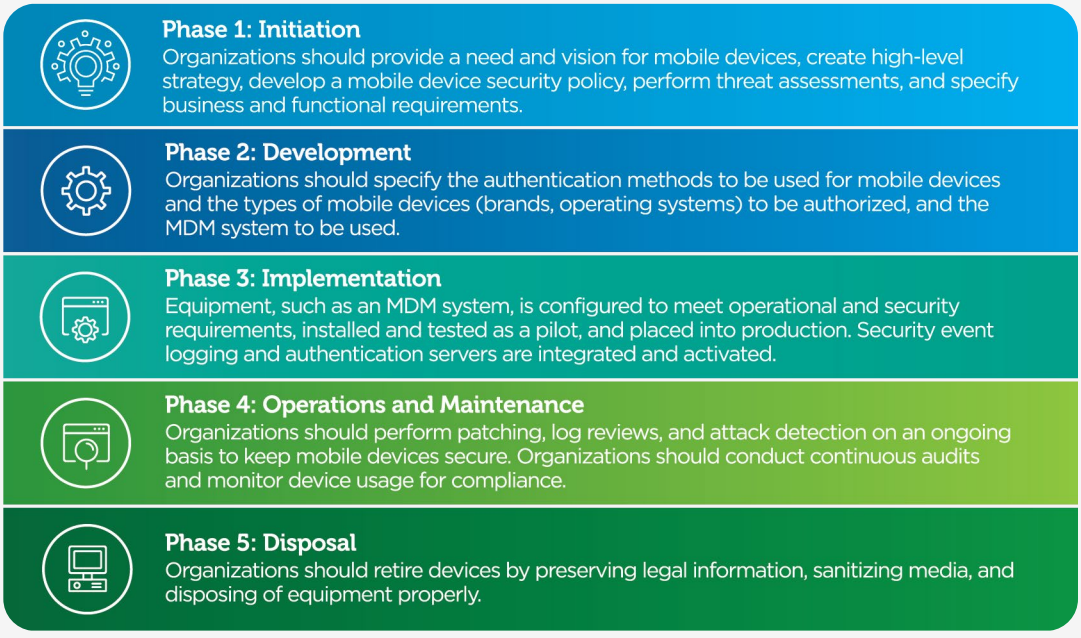
Due to their mobile nature, smartphones can present significant cybersecurity issues if they are not fully protected. For example, insecure configurations, unauthorized access, loss of sensitive data, and device loss or theft are common threats to smartphones. Zimperium, a mobile cybersecurity company, analyzed over 500,000 phishing sites and found that in 2021, 75 percent of those phishing sites specifically targeted smartphones.[5] To overcome these threats, there is an array of federal agencies tasked with providing guidance to minimize cybersecurity issues, such as the Cybersecurity Infrastructure Security Agency (CISA), forum of Federal Chief Information Officers (CIOs), and the National Institute of Standards and Technology (NIST). These organizations recommend implementing a mobile device security program that includes (1) mobile device inventory oversight, (2) a mobile device management (MDM) system, and (3) policies and procedures relating to mobile device security.

> "Due to their mobile nature, smartphones can present significant cybersecurity issues if they are not fully protected."

Before implementing a mobile device security program, an organization first must have a clear understanding of its inventory. The process of tracking an agency's IT assets is critical because it provides a foundation for asset accountability and protection, risk assessment, and timely incident responses. When an agency can accurately account for its assets, it can then assess the threats specific to its mobile devices. Next, an agency can begin to implement an MDM system that allows for further security, configuration settings and restrictions, and can implement policies to protect end users and the organization. (See Figure 1.)

Figure 1. Components of a Mobile Device Security Program

Source: U.S. Postal Service Office of Inspector General (OIG) analysis of NIST Special Publication 800-124, Revision 1 - *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, dated June 2013.[6]



4 A smartphone is a high-end mobile phone built on a mobile computing platform, with more advanced computing ability and connectivity than a contemporary feature phone.
5 *2022 Global Mobile Threat Report, Zimperium*, 2022.
6 As of May 2023, NIST is revising Special Publication 800-124.

Oversight of the Commission

The Postal Service Reform Act of 2022 granted oversight authority of the Commission to the U.S. Postal Service Office of Inspector General. We conducted this audit to examine the management of inventory, security, and utilization of smartphones, and to assess the risk posed by these assets at the Commission. We used a combination of data analytics, interviews, and control tests to determine if appropriate controls were in place and functioning as intended.

Findings Summary

While the Commission was aware of the shortfalls in its smartphone management and has plans to utilize third party tools to strengthen the security of its smartphones, we identified opportunities for further improvement in the Commission's management of inventory, security, and utilization of its smartphones. Specifically, the Commission did not have a standardized process for reviewing and maintaining its inventory. Further, while the Commission was aware it was vulnerable to security risks and is currently working with a contractor to implement an MDM system to mitigate this risk, it did not have key components in place to effectively manage the security of its smartphones. Lastly, the Commission did not have a written policy or procedure to review smartphone utilization billing.

Finding #1: Inventory of Smartphones

While the Commission had policies for maintaining inventories for smartphones, we found opportunities for improvement. Specifically, the Commission did not perform quarterly inventories in accordance with its internal policy. Additionally, the Commission did not include key device characteristics and dispositions to properly account for smartphone inventory. Further, the Commission did not perform asset discovery scans on its mobile devices, which could assist in maintaining an accurate inventory.

Lack of Quarterly Inventories

During our audit, we found the Commission did not conduct inventories of smartphones every quarter. According to internal policy,[7] the Commission will establish appropriate controls to ensure equipment is used appropriately, to include quarterly inventories. Specifically, we requested the Commission's quarterly inventories of its smartphones, however, Commission management responded they did not conduct them.

> "We found the Commission did not conduct inventories of smartphones every quarter in accordance with its internal policy."

Inaccurate Key Device Characteristics and Dispositions

During our review of the Commission's inventory, dated November 2022, we found 64 of 73 smartphones (87 percent) had one or more missing or incorrect key elements in the inventory data, such as the smartphone's serial number, location, Commission identification number, or phone number. For example, 17 (23 percent) of smartphone disposition entries were inaccurate, causing users to appear to be assigned multiple devices when they only had one device in use. Table 1 shows our analysis of the Commission's smartphone inventory.

Table 1. Smartphone Inventory Analysis

Inventory Categories	Number of Inaccurate Data Points	Percent of Total
Commission ID	45	62%
Assigned Date	40	55%
Serial Number	17	23%
Disposition	17	23%
Location	4	5%
Model	2	3%
Phone Number	1	1%
Manufacturer	1	1%

Source: OIG analysis of the Commission's phone inventory as of 11/21/2022.

7 PRC IT-004 Policy: *Acceptable Use of Commission Equipment and Systems*, dated September 2016.

Industry best practices[8] state that organizations should regularly maintain smartphone security by keeping an active inventory of each smartphone. One way to accomplish this is by ensuring fields are correctly recorded to provide a foundation to support internal controls, such as ensuring the correct phone is assigned to the correct employee.

Insufficient Asset Discovery Scans

While the Commission was performing asset discovery scans[9] on most IT equipment, it excluded smartphones from these scans. According to CISA's Binding Operational Directive 23-01, dated October 3, 2022, agencies (including the Commission) are required to safeguard federal information and IT systems by performing automatic asset discoveries every seven days and looking for vulnerabilities across all discovered assets every 14 days by April 3, 2023. The directive includes smartphones in its definition of assets.

> "Performing asset discovery scans would allow the Commission to identify smartphones accessing its network and to verify the accuracy of its inventory by comparing it against the scans."

These three inventory-related issues occurred because management did not focus its resources on completing quarterly device inventories in accordance with written policy. Further, the Commission did not have a standard operating procedure documenting how to conduct these inventories and the key elements to record for each smartphone in its inventory. Lastly, the Commission did not include smartphones in its asset discovery scans because not all its phones were registered in its MDM solution. However, once the Commission registers its remaining phones in its MDM solution, it will then include smartphones in its scans.

Without an accurate inventory list:

- Management is not able to fully implement a mobile device security program because it would not have the information required to apply the same security configurations across its mobile computing landscape. This gap in security coverage leads to a heightened risk of cyberattacks.
- Smartphones are subject to loss, misplacement, or theft.
- Mobile phone bills cannot be accurately analyzed, which could lead to excess payments.

In addition, performing asset discovery scans would allow the Commission to identify smartphones accessing its network and to verify the accuracy of its inventory by comparing it against the scans.

Recommendation #1

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Officer**, develop a standard operating procedure for smartphones, documenting how inventories should be performed and outlining the key elements to record for each smartphone.

Recommendation #2

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, include smartphones in its automated asset discovery and vulnerability enumeration scans to comply with the Cybersecurity and Infrastructure Security Agency Binding Operational Directive 23-01.

Finding #2: Security of Smartphones

We found the Commission was missing key components to effectively manage the security of its smartphones. Specifically, the Commission's mobile device security program did not have: (1) an adequate smartphone security policy, (2) smartphone security awareness training, (3) threat assessments and security log practices, and (4) documented standards and required configuration settings to protect the security of its smartphones. However, the Commission is currently making strides to improve its smartphone security by implementing

8 Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise.
9 Software that identifies IT hardware such as laptops, printers, and mobile devices, which are connected to an agency's network.

multifactor authentication[10] before users can access Commission information on Microsoft Office 365 applications and piloting an MDM system.

This occurred due to several factors, including prioritization of other projects, limited staffing and funding resources, and critical infrastructure issues. For instance, the Commission prioritized the replacement of the Commission's legacy docketing system and a modernization refresh to the PRC.GOV public website over the security of its smartphones. Additionally, the Commission's limited staff did not have the bandwidth to prioritize policy creation and reviews. Given these other initiatives, the Commission planned to complete the implementation of its MDM system by the fourth quarter of fiscal year 2023. However, if the Commission continues to delay efforts on the security of its smartphones, it could be subject to data loss and cybersecurity attacks.

Inadequate Smartphone User Security Policies

While the Commission had policies covering the management of smartphones, it lacked a mobile device security policy. In a meeting with Commission personnel, they explained they strive to follow NIST standards as an industry best practice yet did not align their policies with the NIST guidance[11] regarding mobile device security. Specifically, we found that the Commission's *Acceptable Use Policy* and *Rules of Behavior* did not include what data would be accessible to smartphones, supported models/operating systems and configuration, minimum security requirements, or how smartphones are provisioned[12] to Commission employees. According to NIST, these elements should be included in an organization's mobile device security policy. In April 2023, management acknowledged its lack of policy and stated they intended to create a mobile device security policy by July 2023.

The missing aspects of the Commission's policy are a critical foundation in the development of a mobile device security program because they orient the organization to protect sensitive information, safeguard against cybersecurity threats, and ensure assets are used properly. Without updated, comprehensive policies covering smartphone security, vulnerabilities are at a high risk to be unaddressed, increasing the likelihood that the Commission would fall victim to data loss and cybersecurity attacks.

"Without updated, comprehensive policies covering smartphone security, vulnerabilities are at a high risk to be unaddressed, increasing the likelihood that the Commission would fall victim to data loss and cybersecurity attacks."

Recommendation #3

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, develop and implement a smartphone security policy that aligns with National Institute of Standards and Technology Special Publication 800-124.

Minimal Smartphone Security Awareness Training

We found the Commission did not have adequate smartphone security training. NIST[13] recommends that organizations provide training and awareness activities for smartphone users on threats and recommended security practices. NIST provides a *Mobile Threat Catalogue*[14] that could assist the Commission in identifying which threats and security practices users should be trained on, such as phishing attacks, malicious applications, and the importance of rapidly performing operating system and application updates. Additionally, according to the Commission's *Rules of Behavior*, which covers the use of IT resources, including smartphones, all users must complete mandatory security and privacy awareness training within designated timeframes.

10 A mechanism to verify a user's identity by requiring them to provide more than just a username and password. For example, in addition to entering a password, a user may be required to provide a code that was sent to their phone or email account.
11 Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.
12 Providing telecommunications service to a user, including everything necessary to set up the service, such as equipment, wiring, and transmission.
13 Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.
14 NIST *Mobile Threat Catalogue*, https://pages.nist.gov/mobile-threat-catalogue/.

In our review of the Commission's mandatory Information Security Awareness training, the one section pertaining to mobile security stated that users should keep their devices on them when traveling internationally and not connect to public Wi-Fi. In its training, however, there was no information related to cybersecurity threats specific to smartphones, such as downloading malicious applications, mitigating phishing attacks, and limiting data loss prevention.

The Commission acknowledged it does not have mobile device-specific training; however, we found that it has access to a catalog[15] with on-demand, mobile device security training. Without a robust training program, end users will not be properly educated on the security threats or on how to secure their smartphones and cannot employ tactics to effectively mitigate these risks. This could endanger enterprise and user information at the Commission.

Recommendation #4

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, develop and provide training and awareness activities for smartphone users on smartphone threats, recommended security practices, and policies.

Lack of Threat Assessment and Security Log Practices

The Commission did not conduct threat profile modeling[16] to identify possible cybersecurity risks posed to smartphones. Further, while the Commission was piloting an MDM system as of April 2023, there were no procedures or types of events to capture and examine in its MDM logs[17] pertaining to smartphone security and policy violations.

According to NIST best practices,[18] before designing and deploying an MDM system and other mobile security solutions, organizations should conduct a threat assessment for managing and using smartphones and mobile applications to access and process sensitive data. Further, organizations should develop system threat models for mobile devices because their very nature places them at a higher risk for exposure to threats, so they often need additional protection. Threat modeling should include feasible threats, vulnerability and security controls, quantifying the possibility of successful attacks and impacts, and identifying where security controls are needed.

> "Threat modeling should include feasible threats, vulnerability and security controls, quantifying the possibility of successful attacks and impacts, and identifying where security controls are needed."

Further, NIST guidance[19] states that organizations should establish policies and procedures for log management; create and maintain a log management infrastructure; and establish standard log management operational processes.

Without conducting threat assessments, the Commission is not able to implement effective controls to mitigate potential security threats to smartphones. In addition, without having procedures or use cases in security logs for review, it cannot properly identify, investigate, or respond to cybersecurity attacks.

Recommendation #5

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, perform threat profile modeling for smartphones to identify cybersecurity risks specific to smartphones at the Postal Regulatory Commission.

Recommendation #6

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, develop and implement a standardized process for capturing and reviewing security logs that includes specific use cases to monitor for smartphones.

15 HERO is the U.S. Postal Service's online professional course site that offers 3,200 self-development courses.
16 Involves identifying security requirements, pinpointing threats, and potential vulnerabilities, then quantifying the likelihood of successful attacks and their impacts, and lastly, analyzing this information to determine where security controls need to be improved or added.
17 A log is a record of the events occurring within an organization's system and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.
18 Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.
19 Special Publication 800-92, *Guide to Computer Security Log Management*, dated September 2006.

No Defined or Implemented Standards and Configuration Settings

Although the Commission has taken actions to enhance smartphone security and protect user data, there are opportunities for improvement. We found that the Commission did not fully configure security settings and hardening[20] standards onto its smartphones. Further, the Commission did not have written policies for these standards.

NIST best practices[21] state that organizations should implement an MDM solution that includes the ability to monitor smartphone connectivity and provide protection, authentication, and application functionality. Additionally, the Government Accountability Office recommends organizations implement an MDM solution with the ability to perform configuration control (logging and the ability to disable a device) and management practices (such as setting policies based on a user's role).[22]

Further, during our on-site testing, we found that the Commission did not have the ability to enforce strong password credentials, restrict application downloads, or ensure Commission emails were used to create iCloud[23] profiles. Specifically, we were able to download 16 applications that were considered high risk[24] or in violation of the Commission's *Rules of Behavior*. Also, we were able to exfiltrate data from the Commission's email system through five different methods, including copy and pasting, external storage devices, iTunes backup[25], AirDrop[26], and via texting. Additionally, we identified four of 16 iPhone[27] users (25 percent) had their personal email addresses for their Apple IDs.[28]

While we identified these issues, the Commission took the following steps during our audit:

- Established multifactor authentication on its agency-issued smartphones to access Office 365 applications, such as Outlook, Teams, and SharePoint.
- Implemented Apple Business Manager,[29] which requires the use of Managed Apple IDs that allow for role-based administration, provide the ability to assign content to smartphones, and reset passwords remotely. Managed Apple IDs are owned and managed by an organization for business purposes only, so certain features are disabled to protect the organization.
- Started a pilot of Microsoft Intune[30] that would work in conjunction with Apple Business Manager to address security risks. As of March 2023, the Commission included 10 smartphones in its MDM pilot with Microsoft Intune. This MDM recommends nine security configuration settings[31] for devices that access work data. However, for the smartphones enrolled in the MDM Intune pilot, only two of the nine recommended security configurations were applied to the devices (blocking jailbroken devices[32] and requiring a minimum operating system[33] version). (See Table 2.)

20 A process intended to eliminate a means of cyberattack by patching vulnerabilities and turning off nonessential services.
21 Special Publication 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.
22 GAO Report 12-757 *Better Implementation of Controls for Mobile Devices Should Be Encouraged*, dated September 18, 2012.
23 A service from Apple that securely stores photos, files, notes, passwords, and other data in the cloud and automatically updates across devices.
24 USPS OIG CISO provided a list of applications that are deemed risky due to permissions, such as the ability to read and send text messages, and access phone camera, microphone, and address book.
25 Copying certain files and settings from an iPhone to a computer using iTunes, a software application for downloading, playing, and managing audio and visual files.
26 Uses Wi-Fi and Bluetooth to wirelessly send encrypted photos, videos, websites, locations to other nearby devices.
27 We reviewed a total of 17 smartphones – 16 iPhones and one Android. We are only including iPhones in this statistic because only iPhones can have Apple IDs.
28 The account used to authenticate a user's identity and required whenever a user logs into Apple services.
29 Apple Business Manager is a web-based portal for IT administrators that works with an organization's MDM solution and allows for organizations to better manage devices, including automated device enrollment, Managed Apple IDs, and authentication to Microsoft's active directory domain.
30 Microsoft's MDM software.
31 Microsoft Learn Knowledge Base: *iOS/iPadOS device compliance security configurations*, dated March 2, 2023.
32 The process of removing software restrictions that are intentionally put in place by the device manufacturer.
33 Provides an interface between a smartphone's hardware components and software functions that allows it to run applications and programs. Smartphone manufacturers release operating system versions periodically to update new features, security updates, and other system standards.

Table 2. Microsoft's Recommended Intune Security Configurations

Microsoft Intune Recommended Security Configurations	Included in Intune Pilot as 3/14/2023
Blocking Jailbroken Devices	
Requiring a Minimum Operating System Version	
Requiring a Password to Unlock Mobile Devices	
Blocking Simple Passcodes	
Requiring a Minimum Password Length	
Requiring a Password Type	
Requiring the Phone to Lock After a Period of Inactivity	
Marking Devices Noncompliant Immediately	
Requiring a Maximum Number of Minutes After Screen Lock before Password is Required	

Source: OIG analysis of the Commission's smartphones included in their Microsoft Intune pilot.

Operating without smartphone hardening standards and configuration settings puts the Commission at risk of non-standardized smartphones accessing its network. Additionally, by only installing a subset of recommended configurations in its pilot program, the Commission will continue to be exposed to cybersecurity risks such as malware, phishing, and data exfiltration attempts.

Recommendation #7

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, identify and document hardening standards and configuration settings for smartphones before issuing to end users.

Recommendation #8

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Security Officer** and the **Chief Information Officer**, enroll all smartphones in a mobile device management program and enforce established configuration settings to include strong password credentials, restricted application downloads, automatic operating system patches, and data loss prevention measures.

Finding #3: Utilization of Smartphones

The Commission performed high-level, ad-hoc utilization reviews of smartphone billing statements that were not documented, which led to minor issues related to utilization.

According to a federal executive order,[34] agencies should assess current device usage and establish controls to ensure they are not paying for unused or underutilized IT equipment, software, or services. Additionally, each agency should take steps to limit the number of IT devices. Though not required of the Commission, it may voluntarily follow this executive order. In conversations with Commission executives, they informed the audit team that they try to comply with this executive order.

During our audit, we identified five of 51 devices that had zero usage over three consecutive months between October 2020 through September 2022. The Commission was not able to provide reasoning for the zero usage but has recently begun an initiative to reduce the deployment of smartphones to curtail utilization issues and reduce expenditures.

This occurred because the Commission did not have a written policy or standardized procedure to review or monitor its utilization data. While the Commission

34 EO 13589 – *Promoting Efficient Spending*, Section 4 - Employee Information Technology Devices, dated November 9, 2011.

is working to pilot an MDM system that has the capability to require users to periodically check-in on their devices, this would only serve as a secondary measure to review smartphone utilization. Without a standardized process or procedure in place, there is no consistency in how utilization analyses are performed and no continuity of operations in the case of personnel turnover. In addition, without a standardized process to review utilization, there is a risk of overpayment for services.

> "Without a standardized process to review utilization, there is a risk of overpayment for services."

Recommendation #9

We recommend the **Secretary and Chief Administrative Officer**, in coordination with the **Chief Information Officer**, establish a utilization policy and operating procedures to review utilization data that better aligns with Executive Order 13589.

Management's Comments

Management agreed with the report's findings and recommendations.

Regarding recommendation 1, management stated it is drafting a revised policy and standard operating procedure for inventory management for smartphone devices that covers the items in the OIG recommendations. Also, management stated it will conduct a review of the current key device characteristics and dispositions to ensure fields are correctly recorded. The target implementation date is December 31, 2023.

Regarding recommendation 2, management stated it has developed a Plan of Action and Milestones to systemically identify and mitigate risks. To ensure its MDM solution includes sufficient vulnerability scanning capabilities to meet the CISA directive, management noted it will conduct market research to identify the appropriate asset discovery and vulnerability enumeration tool(s) that will meet the requirements. After the scanning tool is identified, management stated it may require additional funding to procure the tool. The target implementation date is March 31, 2024.

Regarding recommendation 3, management stated it will develop a smartphone security policy that aligns with National Institute of Standards and Technology Special Publication 800-124, Revision 1. The target implementation date is December 31, 2023.

Regarding recommendation 4, management stated it will develop and implement an internal mobile device training and awareness program that includes training on smartphone threats, recommended security practices, and policies. Also, management noted it will research and leverage mobile device training provided by the U.S. Postal Service's HERO training system. The target implementation date is December 31, 2023.

Regarding recommendation 5, management stated it will develop criteria and implement threat profile modeling targeted to identify cybersecurity risks for smartphones. The target implementation date is March 31, 2024.

Regarding recommendation 6, management stated it recently entered into an inter-agency agreement with the Department of Justice to develop and implement a standardized process for capturing and reviewing security logs, including specific use cases to monitor for smartphones. The target implementation date is March 31, 2024.

Regarding recommendation 7, management stated it has an updated and documented artifact that includes hardening standards and a configuration profile. Management noted it would make this artifact available for OIG review to support closure of this recommendation by June 15, 2023.

Regarding recommendation 8, management stated it is in the process of enrolling all government-issued mobile devices into its MDM program. According to management, enrollment includes standardized configuration settings such as strong password credentials, restricted application downloads, automatic operating system patches, and data loss prevention measures. The target implementation date is December 31, 2023.

Regarding recommendation 9, management stated it will update its current tracking method that displays monthly utilization and establish a utilization policy and operating procedures in alignment with Executive Order 13589. The target implementation date is December 31, 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, and the corrective actions should resolve the issues identified in the report. Regarding recommendation 7, the Commission provided the hardening standards and configuration profile artifact for review. Therefore, we can close this recommendation prior to issuance of the report. All recommendations require OIG concurrence before closure. Consequently, the OIG requires written confirmation when corrective actions are completed. Recommendations should not be closed until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our audit scope included the review of smartphones at the Commission; specifically, we assessed and evaluated:

- Inventory management processes and procedures.
- Security and application management policies and their enforcement.
- Expense and usage data for FYs 2021 and 2022.

To accomplish our objective, we:

- Assessed Commission policies relating to the management of smartphones.
- Evaluated the effectiveness of the controls over smartphone inventory management processes and procedures and ensured the accuracy of its smartphone inventory.
- Analyzed smartphone expense and usage data to determine if there were opportunities for cost savings and if devices were under/over utilized.
- Reviewed smartphone data to determine compliance with policies and best practices, to include whether devices were timely patched, downloaded applications were authorized, devices remained supported by IT staff, and configurations were aligned with hardening standards.
- Performed on-site testing for 17 Commission smartphones by examining configurations, network access, application permissions, and verifying inventory. To support our on-site testing, we also interviewed Commission employees on their use and knowledge of smartphones.

We conducted this performance audit from November 2022 through June 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 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 May 9, 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 identified no prior audits or reviews related to the objective of this audit.

Appendix B: Management's Comments

U.S. POSTAL REGULATORY COMMISSION
Washington, DC 20268-0001

Office of the Secretary and Administration

June 16, 2023

Wilvia Espinoza
Deputy Assistant Inspector General for Inspection Services, Technology, and Services
U.S. Postal Service Office of Inspector General (USPS OIG)

Dear Deputy Assistant Inspector General,

Thank you for providing the Postal Regulatory Commission ("the Commission") management with the Office of Inspector General's ("OIG") Audit "Management of the Postal Regulatory Commission's Smartphones" Project number 23-024 dated June 2, 2023. Management has reviewed the OIG's Management of the Postal Regulatory Commission's Smartphones Project Number 23-024 DRAFT.

Commission Management agrees with the findings provided by the OIG team and thanks the OIG for the opportunity to provide feedback on the draft audit report. Prior to this audit, as part of the Commission's security and IT modernization efforts, the Commission began implementing its plan for mobile device management (MDM) for its government-issued mobile devices. The Commission agrees with the OIG's findings that by instituting mobile device management, it will be able to keep secure all government-issued mobile devices by applying software, processes, and security policies onto those mobile devices. MDM solutions will include enrollment of all government-issued mobile devices into the Commission's MDM program, management of device inventory and provisioning, collection of unused devices, protection of mobile device applications, data, and content through implementation of controls, policies, and training.

OIG Recommendation #1:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, develop a standard operating procedure for smartphones, documenting how inventories should be performed and outlining the key elements to record for each smartphone.

Management Response:
Management agrees with this recommendation. The Commission is currently drafting a revised policy and standard operating procedure for inventory management for smartphone devices. The policy and standard operating procedure will establish updated inventory requirements, a standardized process for reviewing and maintaining smartphone inventory, and will cover additional items in the OIG recommendations. The Commission will also conduct a review of the current key device characteristics and

dispositions in order to update incomplete or inaccurate inventory items to ensure fields are correctly recorded.

Target Implementation Date:
December 31, 2023
Responsible Official:
Chief Information Officer

OIG Recommendation #2:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, include smartphones in its automated asset discovery and vulnerability enumeration scans to comply with the Cybersecurity and Infrastructure Security Agency Binding Operative Directive 23-01.
Management Response:
Management agrees with this recommendation. In response to this recommendation, Commission has developed a Plan of Action and Milestones (POA&M) to systemically identify and mitigate risks. Although the OIG's report states that "once the Commission registers its remaining phones in its MDM solution, it will then include smartphones in its scans[,]" the Commission is uncertain whether its current MDM solution includes sufficient vulnerability scanning capabilities in order to meet the CISA directive. As a result, the Commission will conduct market research to identify the appropriate asset discovery and vulnerability enumeration tool(s) that will meet the requirements. After the scanning tool is identified, the Commission may require additional funding to procure the tool and plans to implement the solution by Spring 2024.
Target Implementation Date:
March 31, 2024
Responsible Official:
Chief Information Security Officer

OIG Recommendation #3:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, develop and implement a smartphone security policy that aligns with National Institute of Standards and Technology Special Publication 800-124.
Management Response:
Management agrees with this recommendation. The Commission will develop and implement a smartphone security policy that aligns with National Institute of Standards and Technology Special Publication 800-124, Revision 1.
Target Implementation Date:
December 31, 2023
Responsible Official:
Chief Information Security Officer

OIG Recommendation #4:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, develop and provide training

and awareness activities for smartphone users on smartphone threats, recommended security practices, and policies.

Management Response:

The Commission agrees with this recommendation. The Commission will develop and implement an internal mobile device training and awareness program that includes training on smartphone threats, recommended security practices, and policies. As part of its comprehensive policy updates, the Commission will also align its instructions on mobile device security to include information on security threats, securing mobile devices, and tactics to mitigate risks. The Commission will also research and leverage mobile device training provided by the USPS HERO training system.

Target Implementation Date:

December 31, 2023

Responsible Official:

Chief Information Security Officer

OIG Recommendation #5:

We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, perform threat profile modeling for smartphones to identify cybersecurity risks specific to smartphones at the Postal Regulatory Commission.

Management Response:

Management agrees with this recommendation. The Commission will develop criteria and implement threat profile modeling targeted to identify cybersecurity risks specific to smartphones.

Target Implementation Date:

March 31, 2024

Responsible Official:

Chief Information Security Officer

OIG Recommendation #6:

We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, develop and implement a standardized process for capturing and reviewing security logs that includes specific use cases to monitor for smartphones.

Management Response:

Management agrees with this recommendation. The Commission recently entered into an inter-agency agreement with the Department of Justice (DOJ) to receive its Security Operations Services (SOC) and will work with DOJ to develop and implement a standardized process for capturing and reviewing security logs. The Commission will work with DOJ to include specific use cases to monitor smartphones.

Target Implementation Date:

March 31, 2024

Responsible Official:

Chief Information Security Officer

OIG Recommendation #7:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, identify and document hardening standards and configuration settings for smartphones before issuing to end users.
Management Response:
Management agrees with this recommendation. Since the date of the OIG technical assessment, the Commission has an updated and documented artifact that includes hardening standards and a configuration profile. The Commission will make this artifact available for OIG review and closure of this recommendation.
Target Implementation Date:
June 15, 2023
Responsible Official:
Chief Information Security Officer

OIG Recommendation #8:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Security Officer and the Chief Information Officer, enroll all smartphones in a mobile device management program and enforce established configuration settings to include strong password credentials, restricted application downloads, automatic operating system patches, and data loss prevention measures.
Management Response:
Management agrees with this recommendation. The Commission is in the process of enrolling all government-issue mobile devices into its mobile device management program. Enrollment includes standardized configuration settings such as strong password credentials, restricted application downloads, automatic operating system patches, and data loss prevention measures.
Target Implementation Date:
December 31, 2023
Responsible Official:
Chief Information Officer

OIG Recommendation #9:
We recommend the Secretary and Chief Administrative Officer, in coordination with the Chief Information Officer, establish a utilization policy and operating procedures to review utilization data that better aligns with Executive Order 13589.
Management Response:
Management agrees with this recommendation. The Commission will update its current tracking method that displays utilization on a monthly basis and establish a utilization policy and operating procedures in alignment with Executive Order 13589.
Target Implementation Date:
December 31, 2023
Responsible Official:
Chief Information Officer

The Commission thanks the OIG auditors for their professionalism and cooperative spirit throughout the audit process. As indicated by the Commission's response, we agree with the OIG's recommendation of areas for improvement and the Commission takes its compliance areas very seriously.

Sincerely,

ERICA BARKER Digitally signed by ERICA BARKER
Date: 2023.06.16 12:27:37 -04'00'

Erica Barker
Secretary and Chief Administrative Officer

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