OFFICE OF INSPECTOR GENERAL | UNITED STATES POSTAL SERVICE

Site Technical Assessment Review - January 2024

AUDIT REPORT

Report Number 22-199-R24 | January 25, 2024

Table of Contents

Highlights

Background

The U.S. Postal Service operates more than 8,500 automated systems and equipment that [redacted] nearly half the world's mail. [redacted] network consists of computer systems and equipment that manage, monitor, and control mail [redacted] functions. Without proper controls, there is an increased risk of damage to essential equipment, which could result in delays in mail delivery or injury to Postal Service personnel. Whether it's important documents — such as passports or bank statements — packages, or vital communications, the reliable processing of Postal Service mail is essential to ensure timely delivery.

What We Did

Our objective was to determine whether the Postal Service established and implemented adequate controls at selected [redacted] in the [redacted] Division. Our review included an assessment of the effectiveness of physical, environmental, and security controls implemented on [redacted] at the selected facilities.

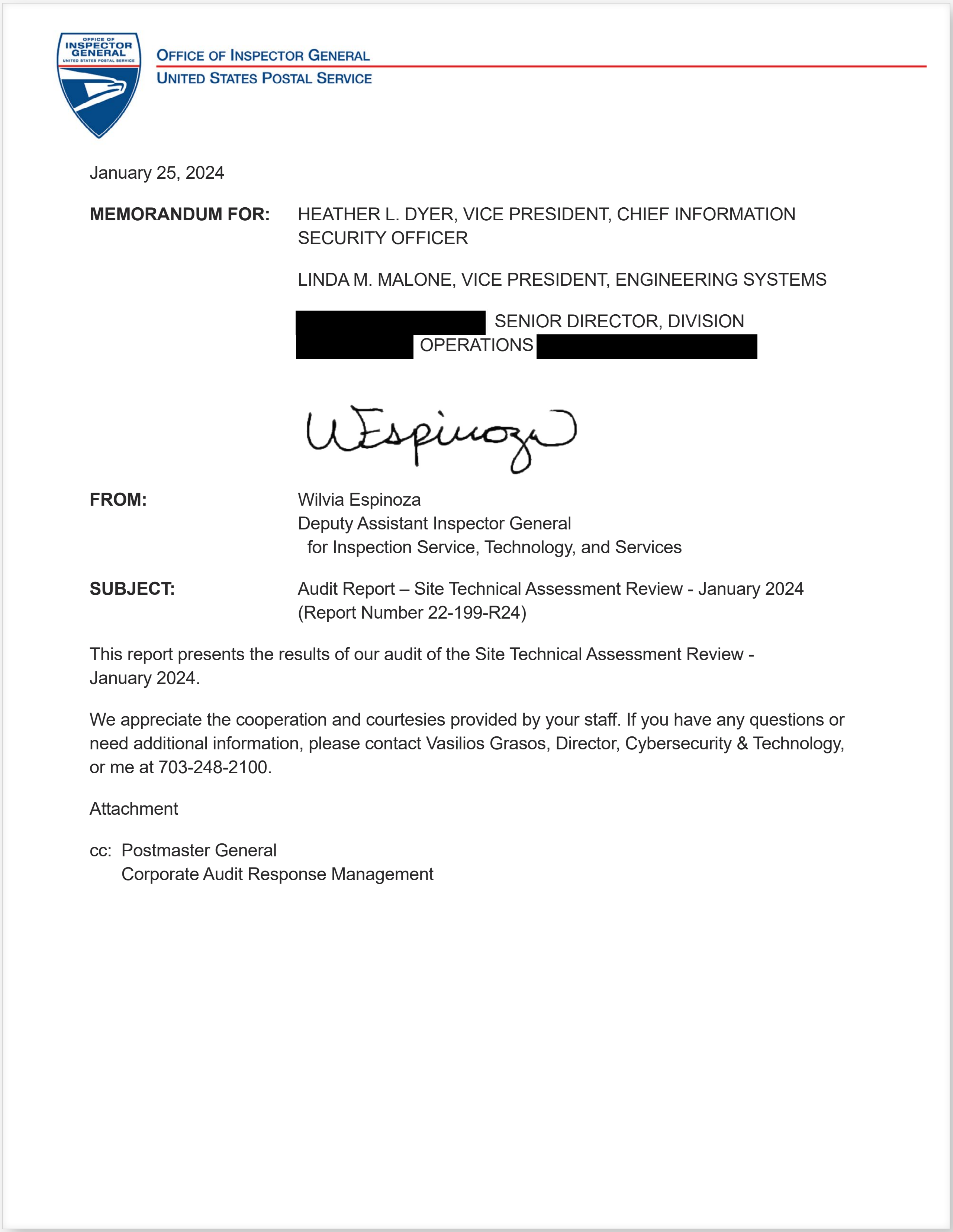
What We Found

We found issues with security controls implemented on [redacted] at the [redacted]. Specifically, we identified vulnerabilities related to system misconfigurations, end-of-life products, and out-of-date software across 52 [redacted] we evaluated. In addition, while the three [redacted] in the [redacted] Division documented their continuity of operations plans, we found that opportunities exist to establish and implement security and environmental controls at the [redacted]. For example, we found that the [redacted] did not consistently implement adequate physical access and account security controls. Further, accounts for [redacted] were not properly configured and the three [redacted] did not consistently implement adequate security controls to prevent harm from environmental hazards in controlled areas. These issues occurred due to limitations of the [redacted] non-standard practices among the facilities, and a lack of documented exceptions to policy.

Recommendations

We made 14 recommendations, including for management to address vulnerabilities identified on the [redacted] and to develop and enforce security controls for doors and badge readers, implement and enforce secure account configuration and management for [redacted], regularly check controlled areas for environmental hazards, and install uninterruptable power supplies in all server racks or document exceptions to policy.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 25, 2024

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

LINDA M. MALONE, VICE PRESIDENT, ENGINEERING SYSTEMS

[redacted] SENIOR DIRECTOR, DIVISION
[redacted] OPERATIONS [redacted]

WEspinoza

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

SUBJECT: Audit Report – Site Technical Assessment Review - January 2024
(Report Number 22-199-R24)

This report presents the results of our audit of the Site Technical Assessment Review - January 2024.

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

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Site Technical Assessment Review - January 2024 (Project Number 22-199). Our objective was to determine whether the U.S. Postal Service established and implemented adequate controls at selected [redacted] in the [redacted] Division. Our review included an assessment of the effectiveness of the physical, environmental, and security controls implemented on [redacted] at the selected facilities. See Appendix A for additional information about this audit.

Background

[redacted] Network Infrastructure

The Postal Service operates more than 8,500 automated systems and equipment that [redacted] nearly half the world's mail.[1] The [redacted] network consists of computer systems that manage, monitor, and control mail [redacted] functions at each [redacted]. The [redacted] computer systems control such functions as [redacted] For example, the [redacted] are vital for business operations and must be protected based on the impact to the Postal Service if the equipment was disabled or compromised. See Table 1 for other examples of [redacted] and their functions.

Table 1. [redacted] Examples

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Source: Postal Service Enterprise Information Repository.

We conducted audit work at three [redacted] Specifically, we evaluated security controls at all facilities and conducted a vulnerability assessment at the [redacted]. The [redacted] was selected for the vulnerability assessment because it processed the fourth highest volume of mail of all [redacted], and it used a wide variety of [redacted]. Our comprehensive review included:

- Vulnerability Assessment – identifies exposures, weaknesses, or flaws in systems that malicious users can manipulate to harm a network and impact operations. The Postal Service performs vulnerability assessments on certain systems, networks, and applications to determine the adequacy of security measures and identify security deficiencies. Vulnerabilities are ranked as critical, high, medium, or low based on the feasibility and impact of an attacker exploiting the

[1] *Postal Facts*. https://facts.usps.com/.
[2] A mailpiece that is not a postcard, letter, or large envelope.
[3] Large envelopes, newsletters, and magazines.

vulnerability. A prior Office of Inspector General (OIG) report[4] identified that there was no process for the Corporate Information Security Office (CISO) [redacted]. We recommended implementing [redacted]

Postal Service management agreed with the finding and recommendation and stated they would implement an ongoing vulnerability assessment process for the [redacted]. They provided documentation to close this recommendation by the target implementation date of October 31, 2023. [redacted] therefore, this recommendation remains open.

- Physical Security Access Controls Assessment – security mechanisms designed to deter unauthorized access to facilities. These vary by facility according to policy based on their square footage, function, and number of employees. For example, an electronic badge system is required to access [redacted] facilities.[5] Additionally, access lists to controlled areas within facilities must be restricted to personnel whose duties require access and who possess appropriate security clearances or background investigations. Examples of controlled areas include, but are not limited to, computer rooms, telecommunications rooms, and wiring closets.
- Environmental Security Controls Assessment – designed to reduce the risk of infrastructure failure and damage from natural or fabricated environmental hazards. These controls safeguard personnel, equipment, hardware, software, and networks from unintentional loss and impairment of data, system availability, or long-term facility loss. Examples of environmental hazards include power outages, roof leaks, flooding, and excessive heat. Examples of environmental controls include uninterruptable power supplies and cooling systems for server rooms. Additionally, a continuity of operations[6] plan must be developed by the facility manager to ensure all Postal Service employees respond safely and quickly to any emergency or situation that may disrupt normal operations.[7]

The reliability of the Postal Service's [redacted] operations is critical to ensure timely and safe delivery of mail to its customers. Without proper security, physical, and environmental controls, there is an increased risk of damage to essential equipment, which could result in delays in mail delivery or injury to Postal Service personnel.

> “The reliability of the Postal Service's [redacted] operations is critical to ensure timely and safe delivery of mail to its customers.”

Roles and Responsibilities

The Vice President, Regional [redacted] Operations oversees [redacted] operations in the [redacted]. The Senior Director, Division [redacted] Operations in [redacted] is responsible for, among other things, preparing for and responding to emergencies at the [redacted] managers at these three locations report to the Senior Director of Division [redacted] Operations, and each facility has a physical security specialist responsible for physical access controls who reports to the Postal Inspector in Charge for their division.

The Chief Postal Inspector is responsible for establishing policies, procedures, standards, and requirements for personnel, physical, and environmental security controls, such as controlled

[4] *State of Cybersecurity*, 21-205-R22, dated August 15, 2022.
[5] Handbook RE-5, *Building and Site Security Requirements*, Section 2-5.3, Access Control System, dated September 2009.
[6] Instructions or procedures that describe how an organization's mission-essential functions will be sustained due to a disaster event before returning to normal operations.
[7] Management Instruction AS-280-2021-7, *Integrated Emergency Management Supporting Field Business Continuity*, dated November 2021.

areas, access lists,[8] access control systems,[9] and identification badges.

The CISO is responsible for performing vulnerability assessments on Postal Service systems, networks, and applications and deciding if the risks identified from those vulnerability assessments are acceptable.[10] If the CISO deems the risks acceptable, then it needs to document the exceptions in the Conditional Authorization to Operate[11] for that particular system being used in the production environment.

Engineering Systems is responsible for ensuring the security of information resources used in support of the [redacted] environment, including acquisition, development, maintenance, and updates. In addition, Engineering Systems is responsible for the remediation of vulnerabilities identified on the network, managing the overall structure and placement of equipment on the network, and ensuring it is consistent for each [redacted].

Findings Summary

Our vulnerability assessment identified issues related to misconfiguration of systems, systems with end-of-life products,[12] and out-of-date software at the [redacted]. In addition, while all three [redacted] we visited in the [redacted] Division documented their continuity of operations plans, we found that opportunities exist for the Postal Service to improve its physical and environmental security controls at the [redacted]. Specifically, we found physical access security controls and account security for the [redacted] were not consistently implemented or enforced. We also found that the [redacted] was not configured according to Postal Service policy and best practices. Finally, we found that [redacted] did not consistently implement adequate environmental controls in controlled areas. See Table 2 for a summary of our findings at each site related to the vulnerability assessment (Finding #1), access controls (Finding #2), account security (Findings #3 and #4), and protection from environmental hazards (Finding #5).

Table 2. Summary of Site-Specific Findings

Control Assessed	[redacted]	[redacted]	[redacted]
Vulnerability Assessment	N/A	N/A	X
Continuity of Operations	✓	✓	✓
Access Controls			
• Access to Work Floors	✓	X	X
• Access Control List	✓	X	X
• Access to Controlled Areas	✓	X	X
Account Security	X	N/A	X
Account Configuration			
• Unrestricted Admin Access	X	X	X
• Removable Media	X	X	X
• Shared Accounts	X	X	X
• Account Lockout	X	X	X
• Audit Logging	X	X	X
Protection from Environmental Hazards	X	X	X

Note: ✓ indicates that adequate controls were implemented.
X indicates that there was a deficiency in the assessed control.
"N/A" indicates that the OIG did not assess this control at this site.
Source: OIG analysis results as of April 20, 2023.

Finding #1: Vulnerability Assessment

The Postal Service did not always adequately configure the [redacted], remove end-of-life software, and update out-of-date operating systems running on [redacted] as required by internal policy and standards at the [redacted]. Specifically, we conducted a vulnerability assessment across 52 [redacted] and found 562 critical and 1,308 high vulnerabilities.

[8] A list of permissions associated with a system resource (object or facility) that specifies which users or system processes are granted access to resources, as well as what operations are allowed on given resources.

[9] System used to control who enters a location and when, using an identifier such as an access card or biometric.

[10] Management Instruction AS-800-2022-7, *Authorization to Operate*, dated June 2022.

[11] *Conditional Authorization to Operate* provides a description of any specific limitations or restrictions placed on the operation of the system or the controls that must be followed by the system owner.

[12] A product at the end of the product lifecycle that prevents users from receiving updates, indicating that the product is at the end of its useful life (from the vendor's point of view).

Misconfiguration

We identified 12 critical and 85 high vulnerabilities related to misconfiguration on 44 out of 52 [redacted] Postal Service policy requires the use of updated encryption standards.[13] However, we found [redacted] which can allow an attacker to intercept and tamper with sensitive data. We also found IP forwarding was enabled on [redacted] According to policy, IP forwarding should be disabled by default because it can allow two separate networks to communicate.[16]

> “Information resources must use only hardware and software products that enable regular updates to address emerging security requirements.”

[redacted]

Engineering Systems stated that due to the age of the systems, the misconfigurations were intentional because if secure configurations were applied, critical functionality of the equipment would be impacted. Additionally, Engineering Systems stated that IP forwarding is enabled for remote monitoring and remote access by technical support personnel to [redacted] and that some vulnerabilities can only be resolved by the original equipment manufacturer.

End-of-Life Operating Systems and Applications

We identified 17 critical vulnerabilities related to end-of-life operating systems that are no longer maintained or receiving updates from the vendor on 17 out of 52 [redacted]. For example, 12 [redacted] are using older versions of [redacted] that stopped being maintained from three to as long as nine years ago.

We also identified 44 critical and two high vulnerabilities related to end-of-life applications on a separate 17 out of 52 [redacted]. For example, four [redacted] have [redacted] installed, which became unsupported three years ago.

Postal Service officials stated that the software required to run the [redacted] is only compatible with the older operating systems and applications. However, policy states that [redacted] information resources must use only hardware and software products that enable regular updates to address emerging security requirements.[17] Additionally, National Institute of Standards and Technology (NIST) best practices state that vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches may never be available.[18]

Out-of-Date Software

We identified 539 critical and 1,293 high vulnerabilities associated with software that the Postal Service did not update in accordance with internal policy. Specifically, we found 33 out of 52 [redacted] in which updates were available from the vendors as long as 21 years ago but were not applied.[19] [redacted] information resources must use only hardware and software products that enable regular updates to address emerging security requirements.[20]

Engineering Systems stated that the audit team identified out-of-date software vulnerabilities because patches were not rolled out at the time of scanning or because a patch was deployed, but not installed on a system. Engineering Systems further stated that this is because monthly patches are not done on these older systems, and updates are only rolled out when necessary. Failure to update software can make systems vulnerable to known security

[13] Handbook AS-805, *Information Security*, Section 9-7.1.1 Minimum Encryption Standards, dated September 2022.
[14] [redacted]
[15] [redacted]
[16] Handbook AS-805, *Information Security*, Section 11-1 Policy, dated September 2022.
[17] [redacted]
[18] NIST Special Publication (SP) 800-82r3, *Guide to OT Security*, Section C.2.2 System Vulnerabilities and Predisposing Conditions, dated September 2023.
[19] For example, [redacted], which is a database used to store data in an electronic format.
[20] [redacted]

exploits and could allow attackers to access sensitive data or other systems on the network.

Overall, the vulnerability assessment team did not identify these three vulnerabilities because management did not want to potentially break critical functionality on [redacted] while performing vulnerability scans. However, Postal Service policy states that all technology applications should be subject to ongoing vulnerability assessments, which includes vulnerability scans,[21] and maintain a vulnerability remediation program.[22] In addition, justifications for exceptions to conducting regular vulnerability scans should be documented.[23] Without full visibility into the [redacted] network, the Postal Service is unable to identify potential weaknesses that could be exploited on the network, potentially resulting in disruptions to mail operations. Additionally, the intentional IP forwarding configuration [redacted] puts the Postal Service at risk of being impacted by unidentified and unaddressed vulnerabilities of [redacted].

Recommendation #1

We recommend the **Vice President, Engineering Systems** and **Vice President, Chief Information Security Officer,** develop a plan to address all critical and high vulnerabilities on the [redacted] at the [redacted] and document exceptions for any vulnerabilities that are deemed acceptable.

Recommendation #2

We recommend the **Vice President, Chief Information Security Officer,** conduct recurring vulnerability scan and remediation procedures for all [redacted] Additionally, document any devices excluded from scanning with justification for those exclusions.

Finding #2: Access Controls

While the [redacted] adequately implemented access controls, the [redacted] did not properly or consistently secure entrances to work floors and controlled areas.

Additionally, the audit team found discrepancies in access control lists at the [redacted]

Access to Work Floors

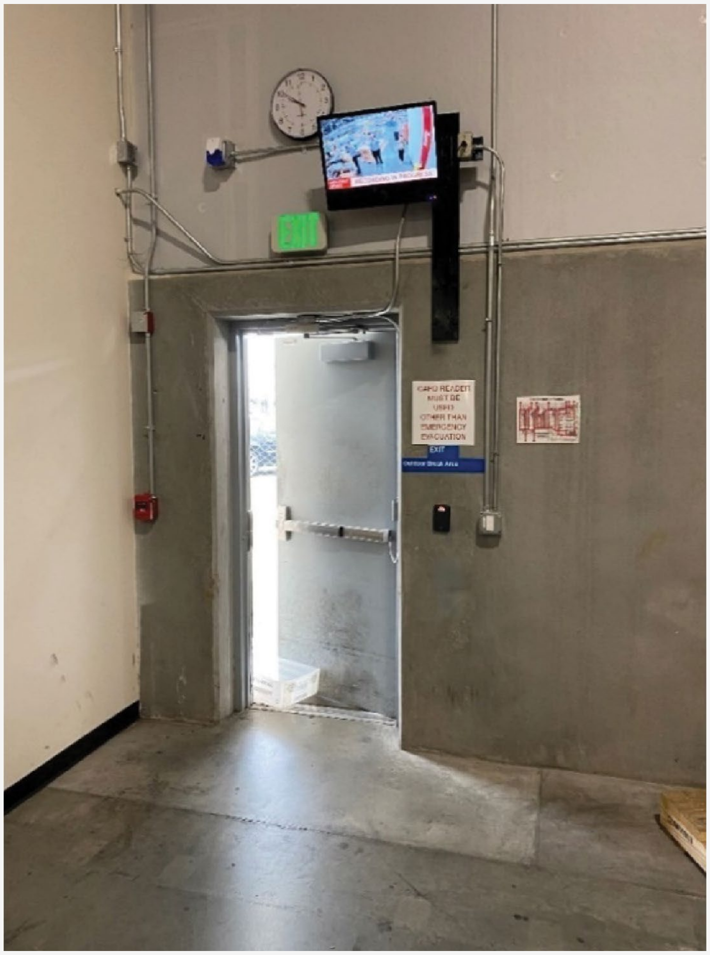
We found [redacted] employees did not always secure entrances to the work floor at the [redacted] according to policy.[24] The audit team entered both facilities without scanning their badges or being stopped by [redacted] employees. Specifically, we:

- Accessed the [redacted] work floor from both unlocked dock and employee parking lot doors. Upon gaining entry to the facility, the audit team had unrestricted access to equipment and vehicles. [redacted] management stated this occurred because carriers use the dock door to move equipment from the dock to the work floor. Also, management stated they do not enforce closure of the parking lot door because it does not have a badge reader, and someone would have to unlock the door whenever carriers enter or exit.
- Entered the [redacted] work floor through an emergency exit door that was propped open, providing unrestricted access to the [redacted] (see Figure 1). From April 17 through April 20, 2023, we closed the door each time we observed it was propped open and reported the issue to management on multiple occasions. Each time the audit team reported this issue, management stated that they were aware, but no immediate preventative action was taken resulting in a persistent failure to maintain physical security. Management stated that the door was propped open to provide contractors faster access to the parking lot and did not communicate physical security requirements to secure the door leading to the work floor. On July 7, 2023, management stated that they assigned a limited duty[25] employee to watch the door and ensure that it was secure. On August 10, 2023, the physical security specialist at the [redacted] performed an unannounced visit to confirm

[21] Handbook AS-805, *Information Security*, Section 11-1.2, Network Infrastructure, dated September 2022.
[22] Handbook AS-805, *Information Security*, Section 2-2.5.3, Director, Cybersecurity Risk Management, dated September 2022.
[23] Management Instruction AS 810-2022-14, *Cyber Risk Enterprise Network Scanning: Customer Impact Resolution, Responsibility Section*, dated September 2023.
[24] Handbook RE-5, *Building and Site Security Requirements*, Section 4-3.1, General Security Standards, dated September 2009.
[25] Limited duty is provided to an employee who has physical limitations identified by a qualified treating physician stemming from an on-the-job injury or illness. The limited duty program is designed to accommodate injured employees who are temporarily unable to perform their regular functions.

that the door was not being propped open and provided photos showing that the door was closed that day.

Figure 1. Unsecured Door at [redacted]



Source: OIG observation at [redacted] on April 17, 2023.

Failure to secure entrances to the work floor can lead to unauthorized access to facilities or [redacted] and disruption of operations.

Recommendation #3

We recommend the **Senior Director Division [redacted] Operations, [redacted],** implement a badge reader to secure all doors surrounding the [redacted] at the [redacted]

Recommendation #4

We recommend the **Senior Director Division [redacted] Operations, [redacted],** issue formal communication to employees stating the requirement to secure all doors leading to the work floor at the [redacted]

Access Control Lists

We found badge access to [redacted] was not always managed effectively. Specifically, management did not consistently remove access to the facility for separated[26] employees to coincide with the employee's termination date according to policy.[27] We compared access control lists for each site to lists of separated personnel from November 2022 through May 2023 and identified 77 of 198 (39 percent) separated employees at the [redacted] and 133 of 302 (44 percent) separated employees at the [redacted] that retained access to their respective facilities. On August 21, 2023, the [redacted] performed a one-time removal of separated employees from their access control list.

We did not find any separated employee badges that were still being used to access the [redacted]. However, we judgmentally selected a sample of 15 out of the 133 (11 percent) employee badges that should have been deactivated at the [redacted] and found three badges that were scanned electronically to access the facility up to nine months after the badges should have been deactivated. After further analysis, we found a total of 30 employee badges that were scanned electronically at the facility after the badges should have been deactivated. During our audit, the [redacted] deactivated the three badges found from our original sample.

These access control issues occurred because employees at [redacted] who were responsible for managing ePhysical Access Control System (ePACS) access stated they were not aware of the standardized guidelines[28] regarding the removal of separated personnel and did not receive training on how to use the system. Additionally, they stated that ePACS support personnel did not have a

[26] For the purposes of this report, separated employees include those who were transferred/reassigned, retired, resigned, or terminated.

[27] Handbook AS-805, *Information Security*, Section 6-6, Departing Personnel, dated September 2022.

[28] ePhysical Access Control System Data Entry Guidelines, dated December 4, 2019. The Postal Service implemented ePACS in 2009. This badge access system was designed to ensure standardized identification protocols (e.g., badge access cards) for granting access to facilities. Access logs from this system must be uploaded to a centralized USPS managed database.

process in place to reconcile separated employees with the badge access control list. However, ePACS support personnel stated they distribute the system guidelines to responsible personnel when they are given access to the ePACS system.

Failure to remove badge access for employees who are no longer employed or do not have a business need at [redacted] can lead to unauthorized access to the work floor and interference with business operations.

Recommendation #5

We recommend the **Senior Director Division** [redacted] **Operations,** [redacted]**,** deactivate the badges in the electronic Physical Access Control System at the [redacted] where the expiration dates were beyond the effective dates for separated employees.

Recommendation #6

We recommend the **Senior Director Division** [redacted] **Operations,** [redacted]**,** Inspector provide training to [redacted] personnel responsible for the ePhysical Access Control System to make sure they can remove and update badge access at the [redacted]

Recommendation #7

We recommend the **Senior Director Division** [redacted] **Operations,** [redacted]**,** publish and implement employee out-processing procedures, to include disabling badges for separating employees and reviewing access control lists periodically to remove separated employees.

Access to Controlled Areas

We found access to controlled areas was not secure according to policy.[29] Additionally, the methods used to secure controlled areas at the [redacted] were unique to their respective sites. Specifically:

- The [redacted] badge readers installed on the controlled areas containing sensitive [redacted] were managed using a standalone system that was not connected to the centralized ePACS readers. As a result, the group responsible for managing the ePACS readers did not have visibility to this system and access logs were not uploaded to the same servers. This occurred because the [redacted] did not receive the resources required to implement a full badge access system. [redacted] management could not produce any written communication regarding the standalone readers and stated that discussions about their implementation were not documented. The ePACS badge reader system was assessed by Facilities and the Inspection Service in January 2023 and is part of a planned upgrade. On May 12, 2023, Facilities stated that the estimated completion date for this upgrade is November 2023.
- Access to the [redacted] controlled area containing [redacted] servers used a physical lock and key with a visitor access log. The badge reader for this room was not in use due to the age of the system, which prevented new employees from being added to the reader. Access to this area required the key to be signed out from the maintenance office. [redacted] management stated that there were no work orders submitted regarding the ePACS reader on this door. They also stated the ePACS readers could have been non-functional for five years or more and are part of a planned upgrade that has been in progress for three years. However, a report received from the Inspection Service, dated July 2020, listed an estimated project completion date to upgrade the badge readers of October 2021. Facilities stated that there were many factors that caused delays to this upgrade, including most projects being put "on hold" for a significant portion of 2021 and requests for project scoping changes from local stakeholders. The physical security specialist for the [redacted] documented these issues in a security assessment that was completed September 27, 2022, but [redacted] management did not respond to the assessment. The physical security specialist stated that [redacted] management sometimes does not respond to requests for action regarding physical security issues.

By using a locally managed badge reader system, it can be difficult to remove separated employees and follow proper procedures for adding access for

[29] Handbook RE-5, *Building and Site Security Requirements*, Section 3-2.5, Access Control System, dated September 2009 and Handbook AS-805, *Information Security*, Section 7-3.1, Access to Controlled Areas, dated September 2022.

employees. Further, if access logs are not uploaded to centralized servers, management cannot monitor employee access to controlled areas. Without oversight of the addition or removal of personnel or retention of access logs, unauthorized personnel could gain access to sensitive equipment leading to damage or theft and the Postal Service would not be able to identify the individual(s) responsible.

Recommendation #8

We recommend the **Senior Director Division [redacted] Operations, [redacted],** install centrally managed badge access panels for controlled areas at the [redacted] and implement access controls in accordance with policy.

Finding #3: Account Security for [redacted] Equipment

[redacted] user accounts were not secured according to Postal Service policy.[30] The audit team observed many written passwords at the [redacted] and other account security issues, such as unauthorized disclosure of passwords and equipment logged into maintenance accounts, which are different from accounts used for basic operation. Specifically, we found passwords written down next to seven of 24 (29 percent) [redacted] observed at the [redacted] and seven of 34 (21 percent) [redacted] observed at the [redacted]. Additionally, a contractor working in the [redacted] disclosed the maintenance password to the [redacted] to the OIG unprompted. This occurred because there was no oversight to prevent passwords from being shared or from being written and posted near [redacted].

We also found three machines at the [redacted] that were logged into accounts with higher privileges than "operator" when no employees were present. This occurred because there was not sufficient oversight for ensuring that employees with higher privileges logged out when they completed their work on the machine. Additionally, Engineering Systems stated that [redacted] does not exist in the [redacted] environment because it would interfere with daily operations but could not provide a documented exception to policy. While Handbook [redacted], does not address the [redacted] standard, Handbook AS-805, *Information Technology* states that the [redacted] standard for Postal Service information resources is a [redacted].[31]

Accounts for Postal Service information technology equipment are intended to associate any action with a single user, process, or other information resource, and are essential for maintaining minimum levels of information security. On typical information systems, users have a single account so an organization can maintain audit logs[32] to track activities conducted on the system. Systems offer different account privileges[33] for users depending on their business need. Shared accounts[34] are allowed in qualifying circumstances defined by CISO but are highly discouraged.

According to policy, if a password is written down, it must be stored under an employee's personal control or in tamper-resistant manner (e.g., an envelope with a registry seal, time stamped, and signed) to ensure that any disclosure or removal of the written password is clearly recognizable. Passwords used to connect to Postal Service information resources must be treated as sensitive information and not be disclosed to anyone other than the authorized user, including system administrators and technical support staff. If there is reason to believe that a password has been disclosed to someone other than the authorized user or has been otherwise compromised, the user must immediately change the password and notify CISO.[35]

[redacted] management's responses to these issues were indicative of differences in standardization between [redacted]. For example, [redacted] management at the [redacted] stated they originally only changed passwords for accounts after they discovered they

[30] Handbook AS-805, *Information Technology* Section 9-6 Authentication, dated September 2022.
[31] Handbook AS-805, *Information Technology,* Section 9-6.10.3, Time-Out Requirements (Re-authentication), dated September 2022.
[32] A record of events occurring on an information system.
[33] A right or authorization granted to an individual, a program, or a process.
[34] Shared accounts have a single log-on ID and password that are used by more than one individual.
[35] Handbook AS-805, *Information Technology*, Section 9-6.1.9, Password Protection, dated September 2022.

were compromised. When [redacted] management discovers that passwords have been compromised, they can change passwords locally to prevent unauthorized use of accounts. After our site visit, management at the [redacted] conducted stand-up talks for account security and started to develop a process for changing [redacted] passwords quarterly while management at the [redacted] took no immediate action to resolve the issue. [redacted] management at the [redacted] stated they do not change their [redacted] passwords, even when they are compromised, because if they change the passwords, it is only a matter of time before everyone in the [redacted] knows it.

If passwords are written down and stored insecurely, they become vulnerable to theft or unauthorized access. This can lead to compromised accounts with access to sensitive data, as well as unauthorized access to machines. Depending on the machine, failure to log out of sessions with elevated privileges can allow employees to change permissions and configurations on operating systems, reset the machine when they are not supposed to, or change [redacted].

Recommendation #9

We recommend the **Senior Director Division [redacted] Operations, [redacted],** provide training and establish an oversight process to prevent [redacted] personnel from writing down and sharing passwords at the [redacted]

Recommendation #10

We recommend the **Senior Director Division [redacted] Operations, [redacted],** develop and implement a standard operating procedure for managing passwords that includes changing passwords and monitoring them for unauthorized disclosure at the [redacted]

Finding #4: Account Configuration of [redacted] Equipment

The Postal Service did not securely configure accounts for the [redacted]. Specifically, we found:

- The [redacted] only has an administrative account for the [redacted] operating system used to operate the machine. This allows any employee with the [redacted] password unrestricted access to alter configuration settings. Engineering Systems stated that maintenance personnel may require administrative access to the [redacted] to install software, updates, and to make system configuration changes. However, Engineering Systems was not able to provide an explanation for why there was only one account created for this machine and stated that accounts with privileges lower than administrative are being included in updates to the [redacted], which are expected to be deployed in fiscal year 2024.
- [redacted]
- Accounts for [redacted] use the same logon identification (ID) for the same types of [redacted] in different [redacted]. For example, the logon ID and password for a [redacted] in the [redacted] had the same logon ID and password as a [redacted] in the [redacted]. The same passwords are used across multiple sites because the login information is a standard image[39] distributed to

[36] [redacted]

[37] Handbook AS-805, *Information Technology*, Section 5-5, Prohibited Uses of Information Resources, dated September 2022.

[38] [redacted]

[39] An exact copy of all electronic data on a device, performed in a manner that ensures the information is not altered.

each [redacted]. Additionally, shared accounts are used on the [redacted] to simplify the operation of the machines and to prevent interruptions in operations from occurring when employees forget passwords. Engineering Systems stated that the risk for using shared accounts was low because the [redacted] machines are programmed to access only the application used to operate the machines and the system does not allow users to perform other unauthorized functions. However, a maintenance manager at the [redacted] stated that employees responsible for the operation of the machine could [redacted] when they are not supposed to if they have access to a maintenance level account in the application used to operate the machine. Additionally, the audit team observed that on the [redacted] it was possible to access system settings, which could allow users to change account privileges.

> “Centralized account management could ensure that users have access to the functions they need without making it possible for them to access information they do not need.”

- Account lockout[40] and audit logging[41] policies were not defined on the [redacted] operating system level on most machines observed. Engineering Systems stated that requiring account lockout policies would cause delays and impact operations in the [redacted] because users would have to log on in the middle of performing tasks. Audit logging was enabled for the application used to operate the [redacted]; however, individual users cannot be identified in the logs because accounts are shared among users.
- Default or simple logins were used at most machines where we found the passwords written or were provided by [redacted] employees. Default and simple logins were used for elevated accounts on [redacted] because in the past, Engineering Systems did not require complex passwords for [redacted] accounts, and some machines could not support complex passwords. Further, approval for special password criteria was not formally documented by the CISO and Engineering Systems. Engineering Systems stated they try to follow CISO criteria for setting passwords but could not provide evidence that they consulted with CISO about password criteria when standards could not be met.

These issues could be resolved by using a centralized account management system. Best practices state that centralized account management could ensure that users have access to the functions they need without making it possible for them to access information they do not need.[42] This would allow Engineering Systems to restrict access to only users who need that access to perform their duties.

Engineering Systems generally adheres to its own policy for information security on the [redacted].[43] This policy provides Engineering Systems with the authority to define password criteria for any device that cannot meet the password requirements in Handbook AS-805. The criteria can include selection characteristics, storage, and transmission requirements. The Vice President, Chief Information Security Officer, and Vice President, Engineering Systems, review and approve the special password criteria.[44] [redacted][45] Additionally, Postal Service policy states that logon IDs should be dependent on an individual’s responsibilities related

[40] Settings that control the threshold for locking an account after incorrect login attempts and the actions to be taken after the threshold is reached.
[41] Audit logs include operating system logs, application system logs, database system logs, event logs, and error logs. Information systems must support audit log capabilities including the actions of any user currently logged on and automatic lockout of that user if necessary.
[42] Microsoft, *What is Identify and Access Management?* https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam.
[43] [redacted]
[44] [redacted].
[45] Handbook AS-805, *Information Security*, Section 5-5, Prohibited Uses of Information Resources, dated September 2022.

to the [redacted], such as troubleshooting, running diagnostics, adjusting, and repairing [redacted].[46]

Failure to implement secure configurations on [redacted] can lead to disruption of [redacted] by malicious actors or insider attacks.[47] Simple, default logins make user accounts more susceptible to password attacks. Once compromised, attackers can gain unauthorized access to systems, networks, and sensitive data and cause critical damage in the mail [redacted] environment.

Recommendation #11

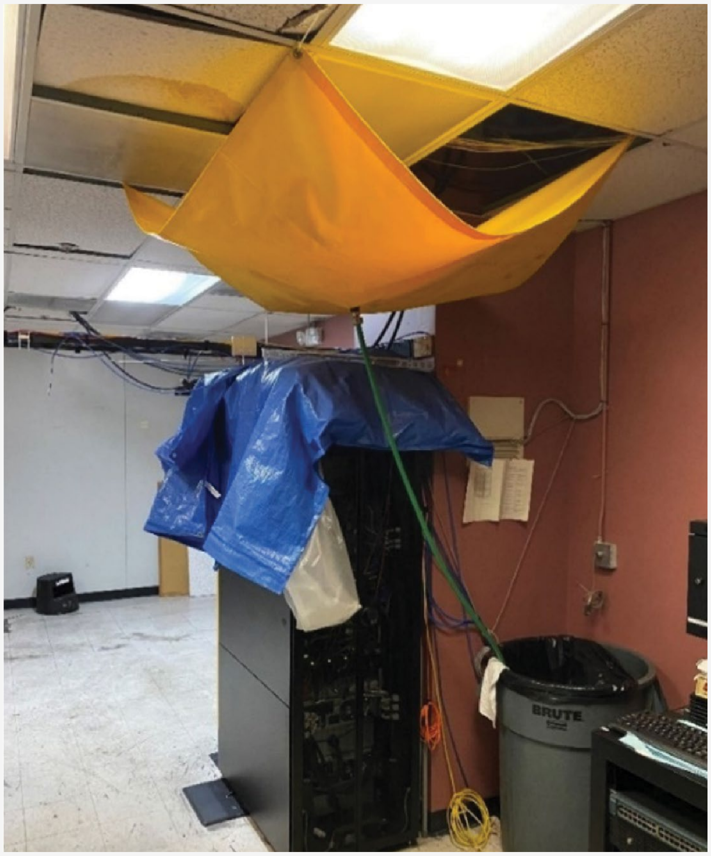
We recommend the **Vice President, Engineering Systems,** implement secure account management and configuration for [redacted] through centralized account management systems or document exceptions to policy, as appropriate.

Finding #5: Protection From Environmental Hazards

The Postal Service did not always implement the necessary precautions to protect [redacted] from potential harm caused by environmental factors. [redacted] can be protected from environmental hazards through a variety of methods, including uninterruptable power supplies[48] and heating, ventilation, and air conditioning systems.[49] However, we found controlled areas were not appropriately protected from water damage, unexpected shutdown, and overheating. During our site walkthroughs, we observed the following deficiencies:

- A tarp protecting the [redacted] from a roof leak at the [redacted] server room (see Figure 2). Maintenance personnel stated the tarp was in place from January 2023 to at least May 2023 and [redacted] management was not able to provide a work order or other evidence of communication with Facilities requesting repair of the roof leak. On July 7, 2023, [redacted] management stated that the tarp was no longer in place, but the roof was still in the process of being repaired.

Figure 2. Tarp Protecting [redacted] From Roof Leak



Source: OIG observation at [redacted] on April 19, 2023.

- Missing or disabled uninterruptable power supplies for [redacted] systems at all three [redacted]. See Table 3 for a list of disabled or missing uninterruptable power supplies.

Table 3. Disabled or Missing Uninterruptable Power Supplies

[redacted] Systems	[redacted]	[redacted]	[redacted]
[redacted]	Missing	Missing	Not Observed
[redacted]	Missing	Not Observed	Missing
[redacted]	✓	✓	Disabled

Source: OIG analysis results as of April 20, 2023.

[46] [redacted]
[47] The threat that an insider will use their authorized access to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.
[48] A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.
[49] Used to prevent the overheating or freezing of information systems.

Maintenance personnel at the [redacted] stated that the [redacted] server racks were configured by Engineering Systems. Engineering Systems stated that the server racks and cabinet did not include uninterruptable power supplies as part of their design and could not provide documentation for why they were not included on these systems. The [redacted] team provided the same explanation for the [redacted] server rack but confirmed that the [redacted] server rack should have had an uninterruptable power supply installed. Maintenance personnel from each [redacted] stated that there was no process in place for replacing them before they died, and that they wait until they die to request replacements.

- The cooling system in a server room was not functioning at the [redacted]. We observed one server room with a temperature between 82 – and 83-degrees Fahrenheit. We found management did not direct employees to check the temperature of the server room, and it was not connected to the cooling system for the building. The maintenance personnel turned on the mobile air conditioning units when the audit team brought the temperature to their attention. On June 25, 2023, the [redacted] submitted a maintenance request for the cooling in this room. On July 6, 2023, Facilities contractors diagnosed the cause of the failure and repaired the cooling system on August 3, 2023. The unit failed again on August 17, 2023, and as of October 24, 2023, the new ticket remained open because parts were not available.

According to policy, environmental security controls must be implemented at the facility, room, and information resource level to protect servers and critical information resources. Protection against water damage from water supply lines, sewer systems, and roof leaks must be implemented. Additional temperature and humidity safeguards must be implemented to monitor and maintain acceptable levels. A short-term alternate power supply must be implemented to ensure proper shutdown in the event of a power interruption.[50]

Failure to implement and maintain environmental security controls surrounding the [redacted] can lead to a loss of functionality for the [redacted] and disruption of operations. For example, [redacted] management from the [redacted] stated that if the [redacted] lost functionality, the [redacted] would not be able to function.

Recommendation #12

We recommend the **Senior Director Division [redacted] Operations, [redacted]**, develop a process to regularly check for environmental hazards in controlled areas at the [redacted] and take action to remediate them, if necessary.

Recommendation #13

We recommend the **Senior Director Division [redacted] Operations, [redacted]**, develop a process to proactively replace uninterruptable power supplies before they become non-functional at the [redacted].

Recommendation #14

We recommend the **Vice President, Engineering Systems,** configure the [redacted] server racks at the [redacted] to include uninterruptable power supplies or document exceptions to policy, as appropriate.

Management's Comments

Management agreed with recommendations 1 through 10 and recommendation 12, but disagreed with recommendations 11, 13, and 14. See Appendix B for management's comments in their entirety.

Regarding recommendation 1, management stated they will track and manage the remediation of the critical and high vulnerabilities found in the [redacted] by implementing available operating system security patches and recommended equipment manufacturer configurations for systems that are not at end-of-life. Management further stated that, pending approval for required funding, it will upgrade [redacted] that contain end-of-life components and document any exceptions for systems that cannot be patched, securely configured, or upgraded. The target implementation date is September 30, 2026.

[50] Handbook AS-805, *Information Security*, Section 7-5, Environmental Security, dated September 2022.

Regarding recommendation 2, management stated they will leverage the data from the [redacted] to define the specific remediation procedures that fall within the enterprise remediation process and document exclusions including a justification for why they cannot be remediated. The target implementation date is September 30, 2024.

Regarding recommendation 3, management stated they will work with the Postal Inspection Service and Facilities to request a security assessment of the sites and explore what options are available to enhance the security of facilities based on current policies within the two groups. The target implementation date is December 31, 2024.

Regarding recommendation 4, management stated they will issue formal communication to employees stating the requirement to secure all doors leading to the work floor at the [redacted] The target implementation date is March 31, 2024.

Regarding recommendation 5, management stated they will deactivate the badges in ePACS at the [redacted] where the expiration dates were beyond the effective dates for separated employees. The target implementation date is June 30, 2024.

Regarding recommendation 6, management stated they agree training could add value and therefore, local management will conduct a standup talk with ePACS users at the [redacted] to ensure there is an understanding of how to remove and update badge access. The target implementation date is December 31, 2024.

Regarding recommendation 7, management stated they will publish and implement employee out-processing procedures, to include disabling badges for separating employees and reviewing access control lists periodically to remove separated employees. The target implementation date is December 31, 2024.

Regarding recommendation 8, management stated they will work with the Postal Inspection Service and Facilities to request a security assessment of the sites and explore what options are available to enhance the badge access panels based on current policies within the two groups. The target implementation date is December 31, 2024.

Regarding recommendation 9, management stated they will provide standup talks to inform [redacted] employees of machine account security and the importance of preventing accounts from being compromised or disclosed at mentioned sites. The target implementation date is February 29, 2024.

Regarding recommendation 10, management stated they will provide standup talks to inform [redacted] employees of machine account security and the importance of preventing accounts from being compromised or disclosed. Additionally, management stated they will monitor work areas for evidence of potential password disclosure on a regular frequency and change passwords if applicable based on system requirements. The target implementation date is September 30, 2024.

Regarding recommendation 11, management stated that the recommendation was impractical and poses challenges because systems connected to the non-routable [redacted] network are isolated and not reachable from a centralized management system. Management also stated that any legacy equipment which may be based on an unsupported operating system poses additional challenges to incorporate a centralized account management uniformly into a standardized solution. However, management stated that secure account management and configuration through a centralized account management system is possible for limited [redacted] systems, which are connected to the routable network and will require further assessment.

Regarding recommendation 12, management stated they will regularly check for environmental hazards in controlled areas at the [redacted] and take action to remediate them, if necessary. The target implementation date is December 31, 2024.

Regarding recommendation 13, management stated that if an uninterruptable power supply fails, risk of an impact to mail [redacted] operations is minimal because the uninterruptable power supply is a secondary back up system which is only activated if other backup systems fail. Additionally, management stated that per normal practice, uninterruptable power supplies are replaced as needed and will continue to be.

Regarding recommendation 14, management stated that the list of systems that OIG identified as not being equipped with uninterruptable power supplies, including the [redacted], are [redacted] that are not within the scope of the respective policy. Additionally, management stated that the legacy design of the [redacted] never included an uninterruptable power supply. Management further stated that the [redacted] is not adversely impacted during a power outage since the system is robust enough to recover quickly after resumption from power loss and can become fully operational after an unexpected shutdown.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1 through 8. The actions planned to address these recommendations should resolve the issues identified in the report. We consider management's comments nonresponsive to recommendations 9 through 14 and will work with management through the formal audit resolution process.

Regarding recommendation 9, while we consider stand-up talks a form of training, management did not explain what process it would follow to ensure password security would be addressed on a long-term basis. Without an oversight process, management has no assurance that personnel won't continue to write down or share passwords.

Regarding recommendation 10, although management stated they will monitor the use of passwords, developing and documenting this oversight process in a standard operating procedure will provide a stronger position from which to implement and oversee password security.

Regarding recommendation 11, if [redacted] systems are not able to support centralized account management, which allows Postal Service to restrict access to only users who need that access to perform their duties, exceptions should be documented with justification.

Regarding recommendation 12, although management stated they will regularly check for environmental hazards in controlled areas at the [redacted], the sites did not have an existing process in place to check for environmental hazards in controlled areas. Developing a standard operating procedure will provide management with a documented process for conducting these checks and verifying that environmental hazards in controlled areas are mitigated timely.

Regarding recommendation 13, Postal Service policy states that both a short – and long-term alternate power supply must be implemented at the facility, room, and information resource level to protect servers and ensure proper shutdown in the event of an interruption. Therefore, proactive replacement should be implemented to ensure that servers requiring uninterruptable power supplies always shut down properly in the event of an interruption.

Regarding recommendation 14, Postal Service policy specific to the [redacted] does not include policy for environmental controls; therefore, we referenced Postal Service information security policy as justification for the recommendation. If certain [redacted] do not require backup power supplies, exceptions should be documented with justification.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Appendix A: Additional Information

Scope and Methodology

We conducted site work in the [redacted] Division in the [redacted] Region for [redacted] Operations from April 10 to 21, 2023. We judgmentally selected three [redacted] in this division with the highest mail volume and widest variety of [redacted] machines for our review of physical and environmental controls: [redacted]. We also conducted vulnerability scans on 52 [redacted] that support mail operations at the [redacted].

To accomplish our objective, we:

- Obtained and reviewed physical security policies, processes, and procedures to gain an understanding of the environment.
- Conducted a site survey to identify any unsecure building doors that allowed unrestricted access to the work floor.
- Observed and evaluated physical and environmental controls that protect [redacted] and its server rooms to determine compliance with Postal Service policy and industry best practices.
- Obtained and reviewed access control lists received from sites to ensure separated personnel badges were inactive.
- Interviewed Postal Service and Postal Inspection Service personnel to determine the roles and responsibilities for the Postal Service's physical and environmental security program and controls.

We also engaged a contractor with subject matter expertise to assist in the vulnerability assessment and provide observations regarding the overall cybersecurity posture of the [redacted] environment. The contractor performed the following:

- Network architecture review of network diagrams, configurations, segmentation architecture, and wireless network architecture and configuration.
- System configuration review ensuring baseline configuration and security settings for assets that comprise the infrastructure align with industry-standard security recommendations and hardening practices.
- Vulnerability scanning.
- Information security standard control assessment using the practices and controls documented in Postal Service policy and industry best practices, frameworks, and standards.

We conducted this performance audit from November 2022 through January 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 November 29, 2023, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of [redacted] 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 five components were significant to our audit objective: control environment, risk assessment, control activities, information and communication, and monitoring.

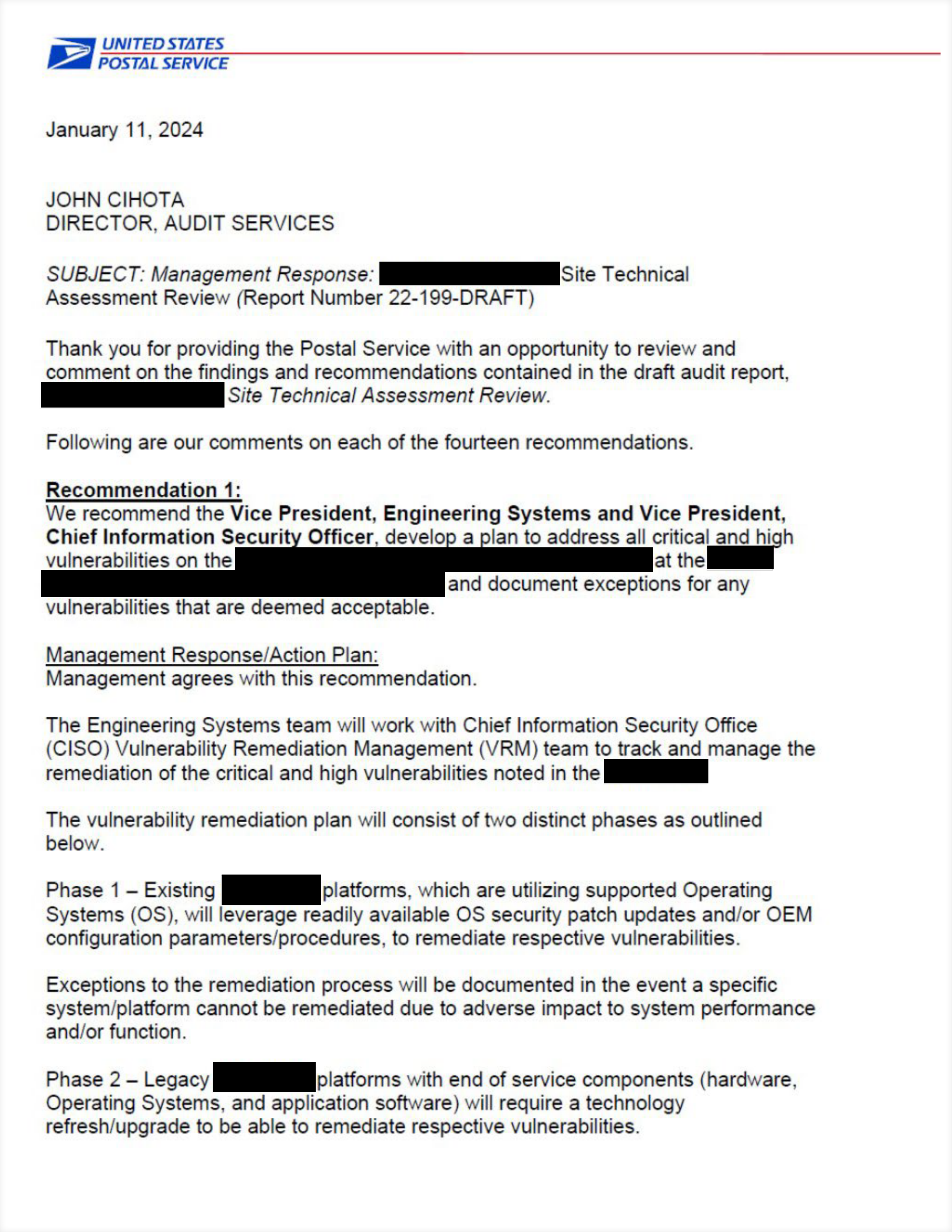
We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to control environment, control activities, information and communication, and monitoring that were significant within the context of our objectives. Our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

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

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Pacific Area Processing and Distribution Center Physical and Environmental Security Controls	Determine whether the Postal Service has adequate and effective physical and environmental security controls at the Margaret L. Sellers P&DC.	IT-AR-17-005	May 3, 2017	N/A
Western Area Physical Security and Environmental Controls	Determine whether the Postal Service has implemented effective physical security and environmental and wireless access controls according to policy and industry best practices at the [redacted] P&DC.	IT-AR-18-002	March 19, 2018	N/A
Physical and Environmental Controls Site Security Review – Summary Report	Identify and summarize the findings and recommendations in four issued area physical and environmental controls site security reports. The objective of those four audits was to determine whether the Postal Service established effective physical and environmental security controls at P&DCs.	IT-AR-19-004	August 15, 2019	N/A

Appendix B: Management's Comments



UNITED STATES
POSTAL SERVICE

January 11, 2024

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: [redacted] Site Technical Assessment Review (Report Number 22-199-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, [redacted] *Site Technical Assessment Review.*

Following are our comments on each of the fourteen recommendations.

Recommendation 1:
We recommend the **Vice President, Engineering Systems and Vice President, Chief Information Security Officer**, develop a plan to address all critical and high vulnerabilities on the [redacted] at the [redacted] and document exceptions for any vulnerabilities that are deemed acceptable.

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

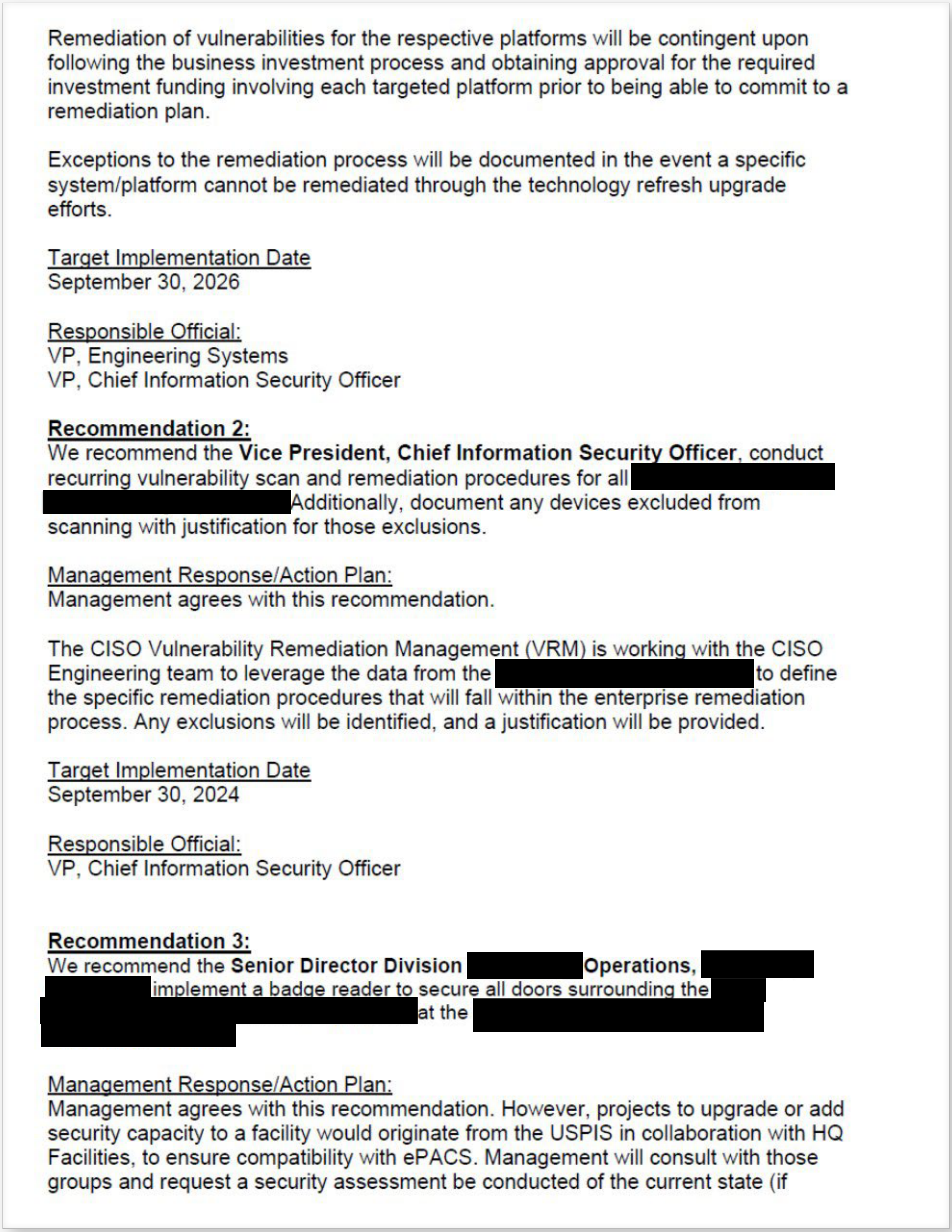
The Engineering Systems team will work with Chief Information Security Office (CISO) Vulnerability Remediation Management (VRM) team to track and manage the remediation of the critical and high vulnerabilities noted in the [redacted]

The vulnerability remediation plan will consist of two distinct phases as outlined below.

Phase 1 – Existing [redacted] platforms, which are utilizing supported Operating Systems (OS), will leverage readily available OS security patch updates and/or OEM configuration parameters/procedures, to remediate respective vulnerabilities.

Exceptions to the remediation process will be documented in the event a specific system/platform cannot be remediated due to adverse impact to system performance and/or function.

Phase 2 – Legacy [redacted] platforms with end of service components (hardware, Operating Systems, and application software) will require a technology refresh/upgrade to be able to remediate respective vulnerabilities.



Remediation of vulnerabilities for the respective platforms will be contingent upon following the business investment process and obtaining approval for the required investment funding involving each targeted platform prior to being able to commit to a remediation plan.

Exceptions to the remediation process will be documented in the event a specific system/platform cannot be remediated through the technology refresh upgrade efforts.

Target Implementation Date
September 30, 2026

Responsible Official:
VP, Engineering Systems
VP, Chief Information Security Officer

Recommendation 2:
We recommend the **Vice President, Chief Information Security Officer**, conduct recurring vulnerability scan and remediation procedures for all [redacted] Additionally, document any devices excluded from scanning with justification for those exclusions.

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

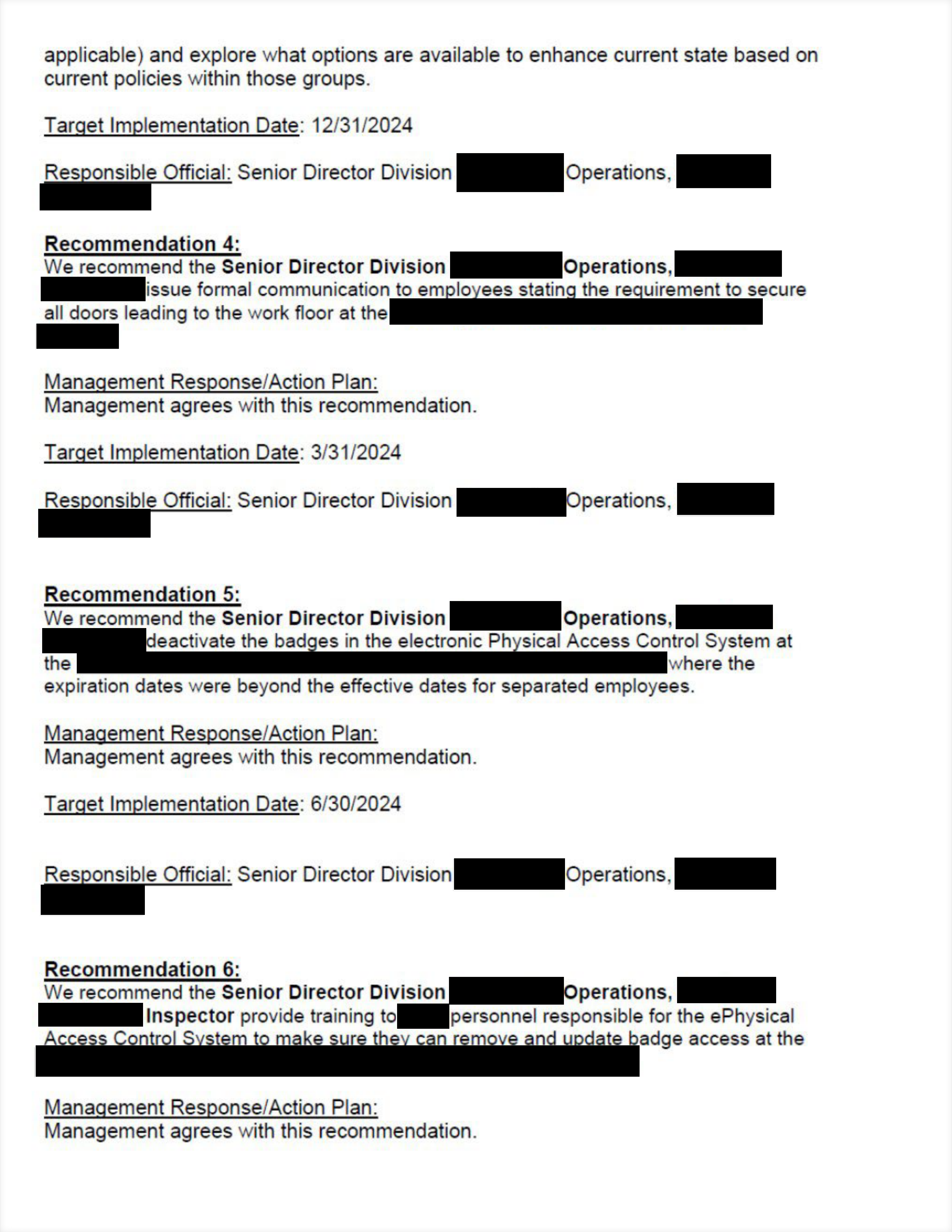
The CISO Vulnerability Remediation Management (VRM) is working with the CISO Engineering team to leverage the data from the [redacted] to define the specific remediation procedures that will fall within the enterprise remediation process. Any exclusions will be identified, and a justification will be provided.

Target Implementation Date
September 30, 2024

Responsible Official:
VP, Chief Information Security Officer

Recommendation 3:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] implement a badge reader to secure all doors surrounding the [redacted] at the [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. However, projects to upgrade or add security capacity to a facility would originate from the USPIS in collaboration with HQ Facilities, to ensure compatibility with ePACS. Management will consult with those groups and request a security assessment be conducted of the current state (if



applicable) and explore what options are available to enhance current state based on current policies within those groups.

Target Implementation Date: 12/31/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted] [redacted]

Recommendation 4:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] issue formal communication to employees stating the requirement to secure all doors leading to the work floor at the [redacted] [redacted]

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

Target Implementation Date: 3/31/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted] [redacted]

Recommendation 5:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] deactivate the badges in the electronic Physical Access Control System at the [redacted] where the expiration dates were beyond the effective dates for separated employees.

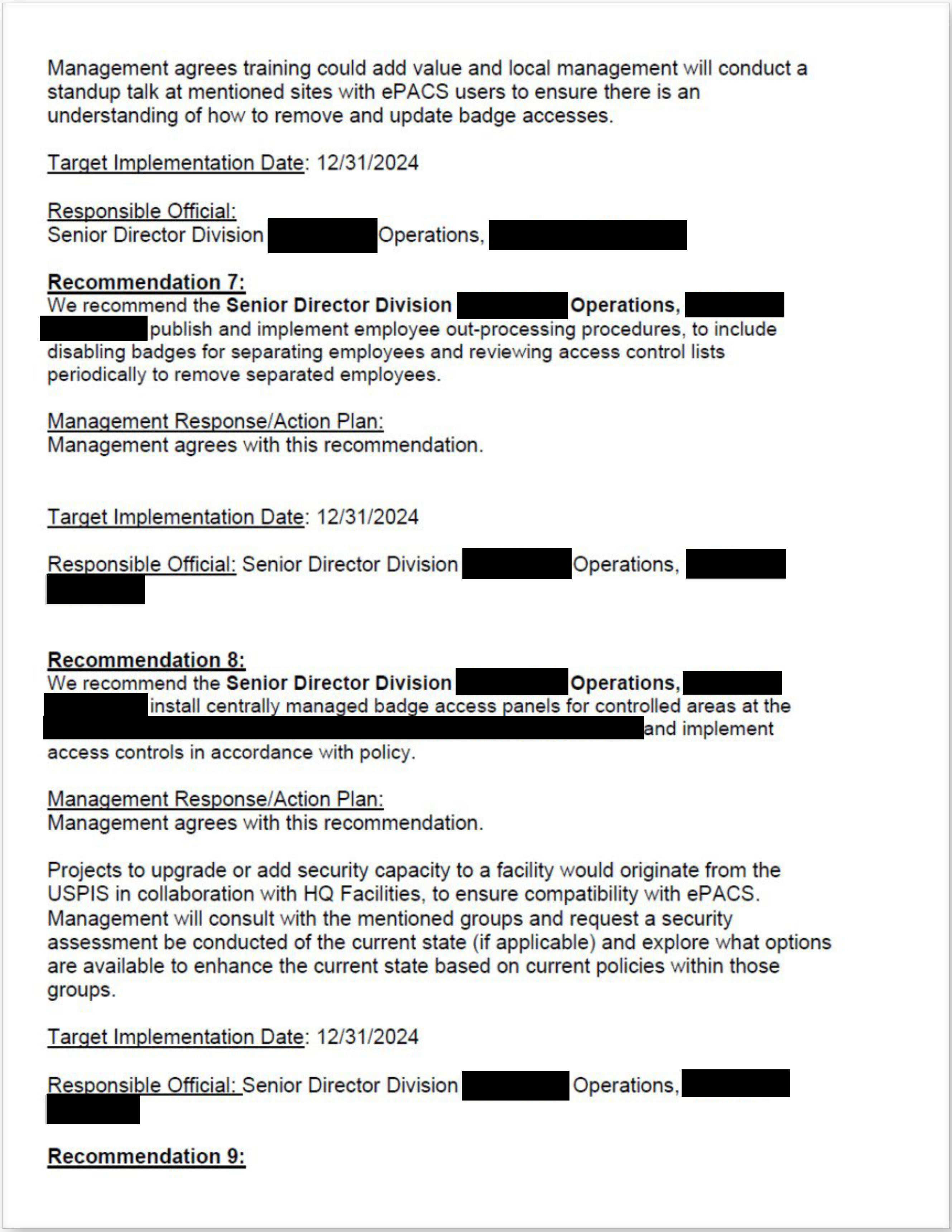
Management Response/Action Plan:
Management agrees with this recommendation.

Target Implementation Date: 6/30/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted] [redacted]

Recommendation 6:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] **Inspector** provide training to [redacted] personnel responsible for the ePhysical Access Control System to make sure they can remove and update badge access at the [redacted]

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



Management agrees training could add value and local management will conduct a standup talk at mentioned sites with ePACS users to ensure there is an understanding of how to remove and update badge accesses.

Target Implementation Date: 12/31/2024

Responsible Official:
Senior Director Division [redacted] Operations, [redacted]

Recommendation 7:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] publish and implement employee out-processing procedures, to include disabling badges for separating employees and reviewing access control lists periodically to remove separated employees.

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

Target Implementation Date: 12/31/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted] [redacted]

Recommendation 8:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] install centrally managed badge access panels for controlled areas at the [redacted] and implement access controls in accordance with policy.

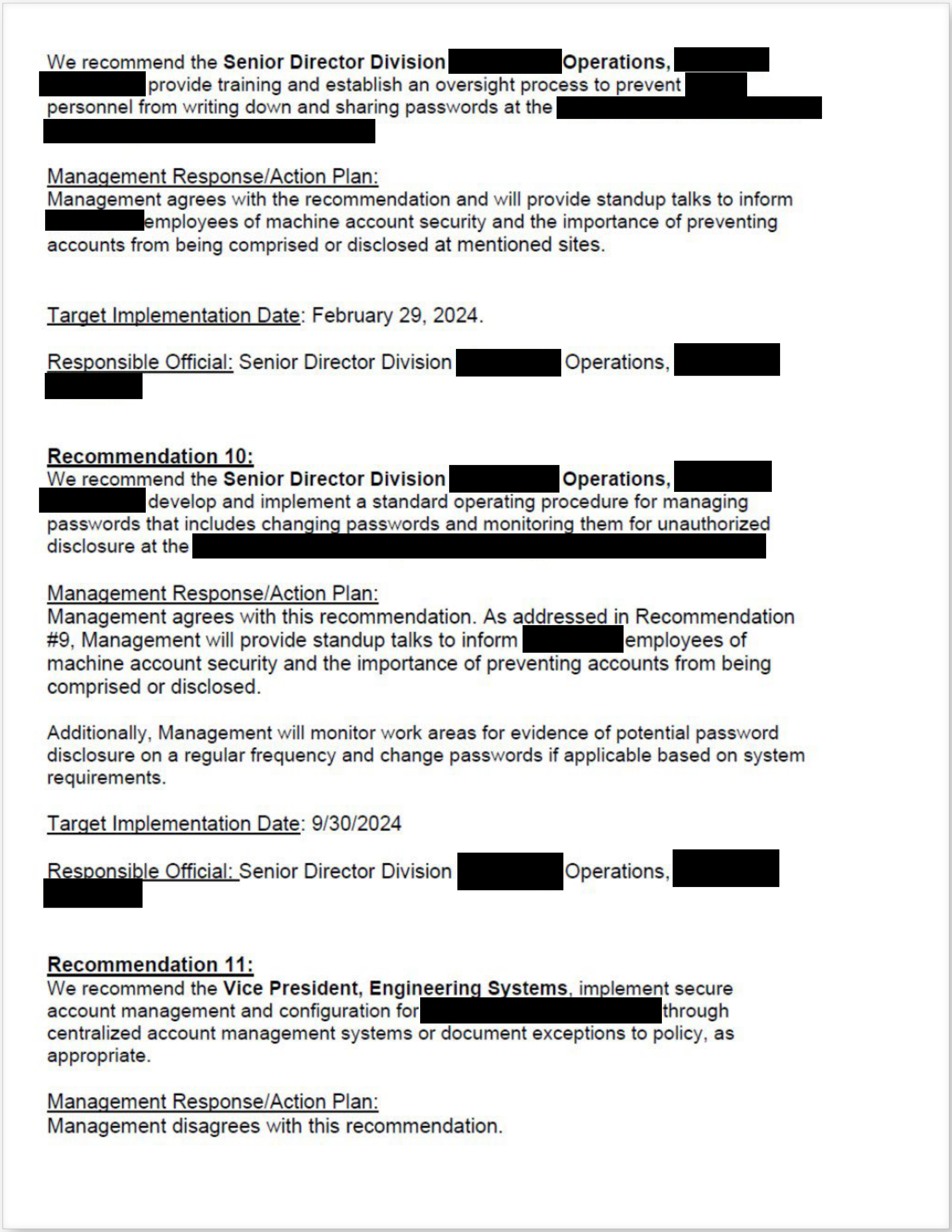
Management Response/Action Plan:
Management agrees with this recommendation.

Projects to upgrade or add security capacity to a facility would originate from the USPIS in collaboration with HQ Facilities, to ensure compatibility with ePACS. Management will consult with the mentioned groups and request a security assessment be conducted of the current state (if applicable) and explore what options are available to enhance the current state based on current policies within those groups.

Target Implementation Date: 12/31/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted] [redacted]

Recommendation 9:



We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] provide training and establish an oversight process to prevent [redacted] personnel from writing down and sharing passwords at the [redacted]

Management Response/Action Plan:
Management agrees with the recommendation and will provide standup talks to inform [redacted] employees of machine account security and the importance of preventing accounts from being comprised or disclosed at mentioned sites.

Target Implementation Date: February 29, 2024.

Responsible Official: Senior Director Division [redacted] Operations, [redacted]

Recommendation 10:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] develop and implement a standard operating procedure for managing passwords that includes changing passwords and monitoring them for unauthorized disclosure at the [redacted]

Management Response/Action Plan:
Management agrees with this recommendation. As addressed in Recommendation #9, Management will provide standup talks to inform [redacted] employees of machine account security and the importance of preventing accounts from being comprised or disclosed.

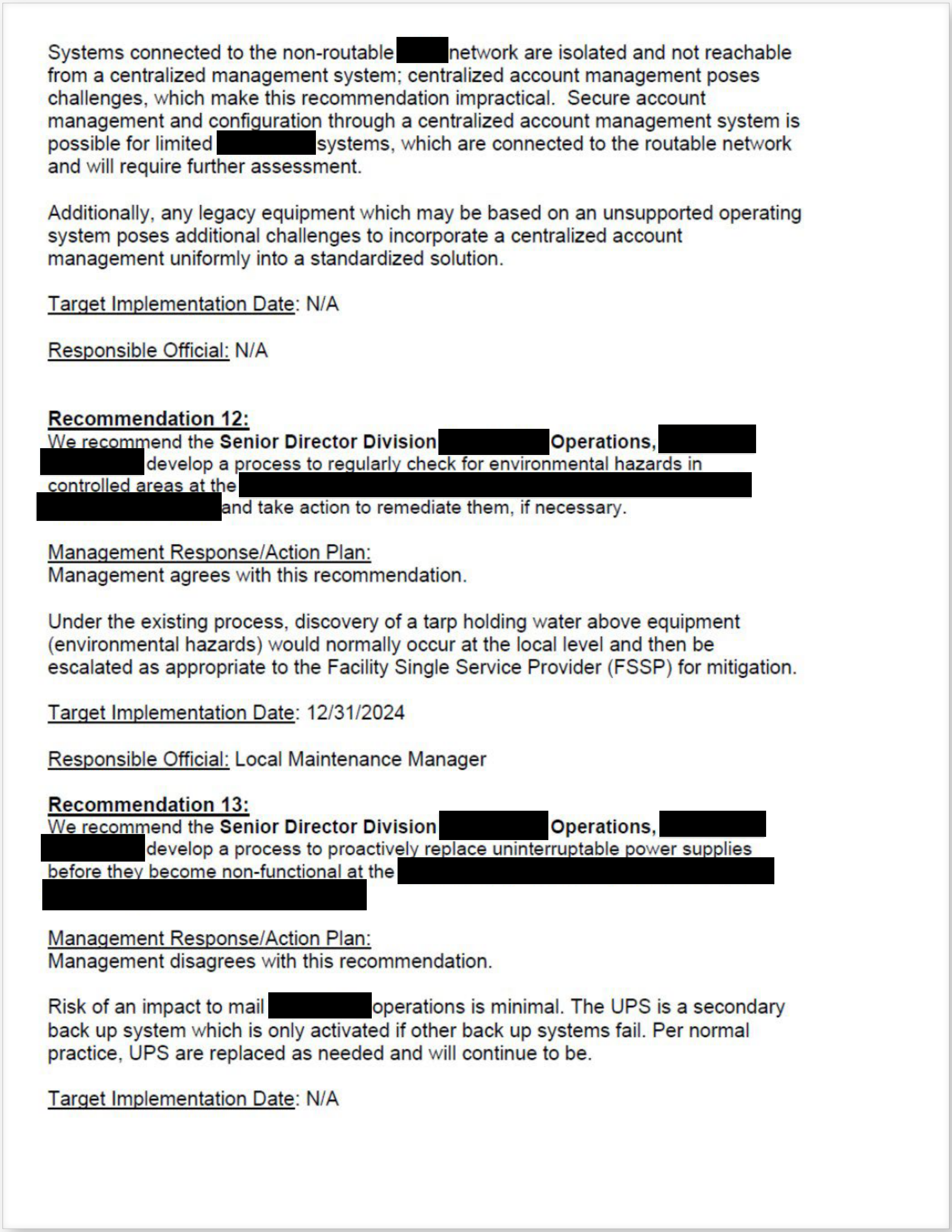
Additionally, Management will monitor work areas for evidence of potential password disclosure on a regular frequency and change passwords if applicable based on system requirements.

Target Implementation Date: 9/30/2024

Responsible Official: Senior Director Division [redacted] Operations, [redacted]

Recommendation 11:
We recommend the **Vice President, Engineering Systems**, implement secure account management and configuration for [redacted] through centralized account management systems or document exceptions to policy, as appropriate.

Management Response/Action Plan:
Management disagrees with this recommendation.



Systems connected to the non-routable [redacted] network are isolated and not reachable from a centralized management system; centralized account management poses challenges, which make this recommendation impractical. Secure account management and configuration through a centralized account management system is possible for limited [redacted] systems, which are connected to the routable network and will require further assessment.

Additionally, any legacy equipment which may be based on an unsupported operating system poses additional challenges to incorporate a centralized account management uniformly into a standardized solution.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 12:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] develop a process to regularly check for environmental hazards in controlled areas at the [redacted] [redacted] and take action to remediate them, if necessary.

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

Under the existing process, discovery of a tarp holding water above equipment (environmental hazards) would normally occur at the local level and then be escalated as appropriate to the Facility Single Service Provider (FSSP) for mitigation.

Target Implementation Date: 12/31/2024

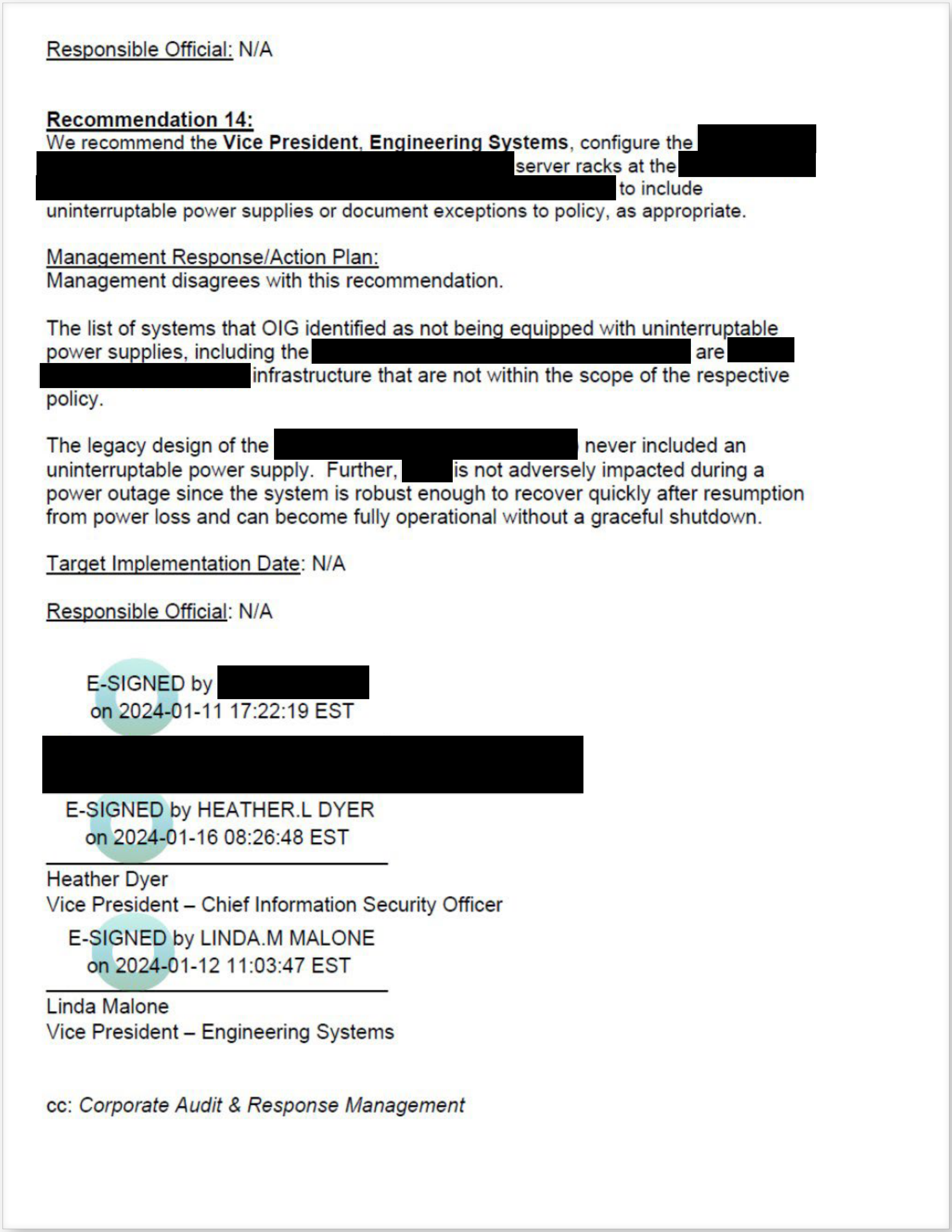
Responsible Official: Local Maintenance Manager

Recommendation 13:
We recommend the **Senior Director Division** [redacted] **Operations,** [redacted] [redacted] develop a process to proactively replace uninterruptable power supplies before they become non-functional at the [redacted] [redacted]

Management Response/Action Plan:
Management disagrees with this recommendation.

Risk of an impact to mail [redacted] operations is minimal. The UPS is a secondary back up system which is only activated if other back up systems fail. Per normal practice, UPS are replaced as needed and will continue to be.

Target Implementation Date: N/A



Responsible Official: N/A

Recommendation 14:
We recommend the **Vice President, Engineering Systems**, configure the [redacted] server racks at the [redacted] to include uninterruptable power supplies or document exceptions to policy, as appropriate.

Management Response/Action Plan:
Management disagrees with this recommendation.

The list of systems that OIG identified as not being equipped with uninterruptable power supplies, including the [redacted] are [redacted] infrastructure that are not within the scope of the respective policy.

The legacy design of the [redacted] never included an uninterruptable power supply. Further, [redacted] is not adversely impacted during a power outage since the system is robust enough to recover quickly after resumption from power loss and can become fully operational without a graceful shutdown.

Target Implementation Date: N/A

Responsible Official: N/A

E-SIGNED by [redacted]
on 2024-01-11 17:22:19 EST

[redacted]

E-SIGNED by HEATHER.L DYER
on 2024-01-16 08:26:48 EST

Heather Dyer
Vice President – Chief Information Security Officer

E-SIGNED by LINDA.M MALONE
on 2024-01-12 11:03:47 EST

Linda Malone
Vice President – Engineering Systems

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