OFFICE OF INSPECTOR GENERAL | UNITED STATES POSTAL SERVICE

Technology, Infrastructure, and Site Security Review

AUDIT REPORT

Report Number 24-133-R25 | March 21, 2025

Table of Contents

Highlights

Background

The U.S. Postal Service operates more than 8,500 automated systems and equipment at 313 [redacted] facilities that [redacted] nearly half the world's mail. Its [redacted] network consists of computer systems and equipment that manage, monitor, and control mail [redacted] functions. Without proper technological, physical, and environmental controls, there is an increased risk of adverse impacts to essential equipment, which could result in delays in [redacted].

What We Did

Our objective was to determine whether the Postal Service established and implemented adequate controls at select [redacted] in the [redacted] Division. Our review included an assessment of the effectiveness of information technology, physical, and environmental controls implemented on the approximately $87.7 million of [redacted] at the [redacted].

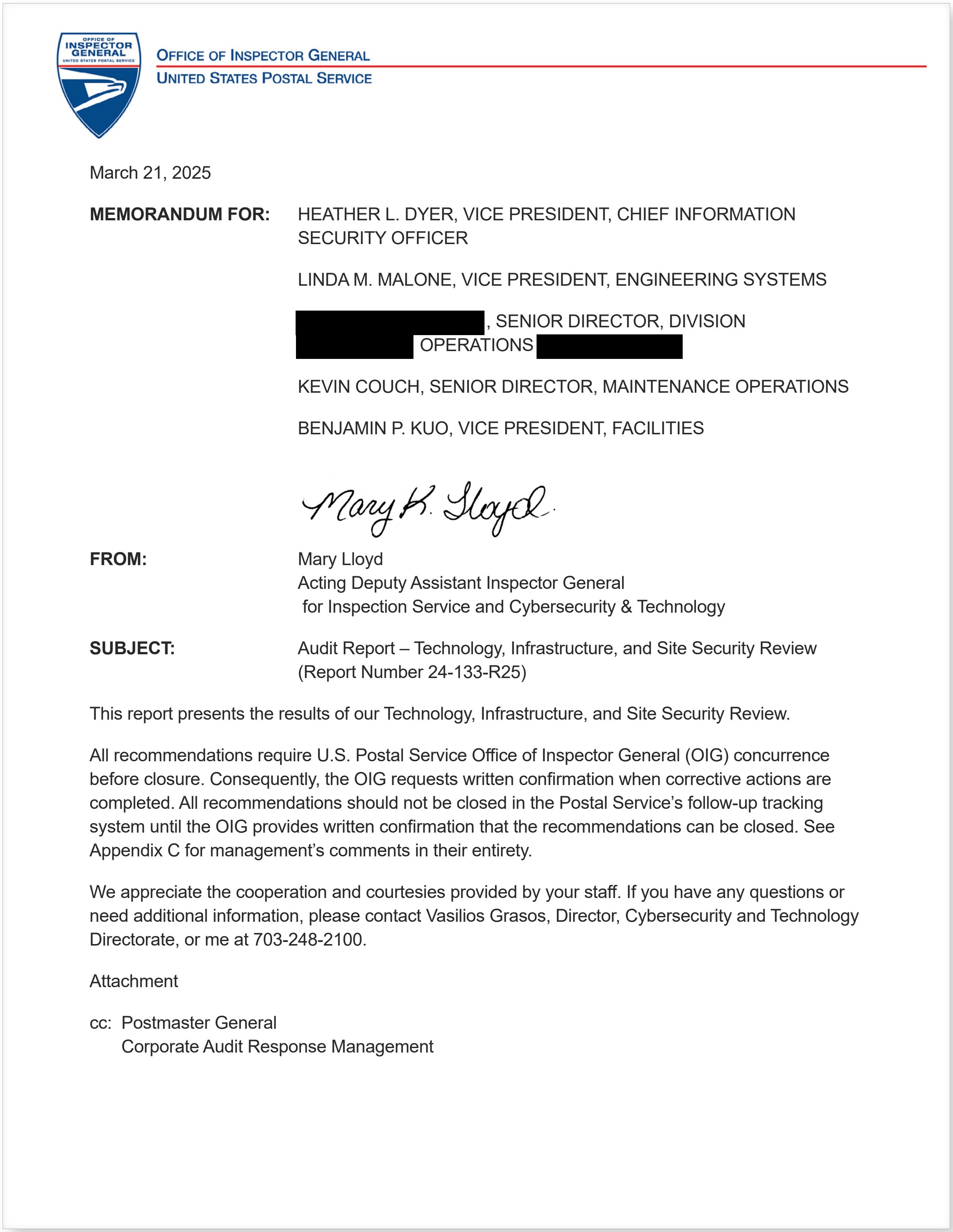
What We Found

The Postal Service did not always establish and implement effective information technology, physical, and environmental controls. Specifically, the Postal Service did not have a process to proactively identify or remediate information technology vulnerabilities on the [redacted] network. According to Engineering Systems, a process to improve vulnerability scanning coverage on the [redacted] network is in the pilot phase. However, unresolved vulnerabilities could be exploited and lead to disruptions to [redacted]. In addition, the [redacted] have physical and environmental security issues that may allow unauthorized access to restricted [redacted] facilities and equipment.

Recommendations and Management's Comments

We made 14 recommendations to address the issues identified in this report. Postal Service management agreed with eight recommendations and disagreed with six. Management's comments and our evaluation are at the end of each finding and recommendation. The U.S. Postal Service Office of Inspector General considers the Postal Service responsive to recommendations one through eight, as corrective actions should resolve these issues. We will work with management through the audit resolution process on the remaining six recommendations. See Appendix C for management's comments in their entirety.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 21, 2025

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

LINDA M. MALONE, VICE PRESIDENT, ENGINEERING SYSTEMS

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

KEVIN COUCH, SENIOR DIRECTOR, MAINTENANCE OPERATIONS

BENJAMIN P. KUO, VICE PRESIDENT, FACILITIES

Mary K. Lloyd

FROM: Mary Lloyd
Acting Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report – Technology, Infrastructure, and Site Security Review (Report Number 24-133-R25)

This report presents the results of our Technology, Infrastructure, and Site Security Review.

All recommendations require U.S. Postal Service Office of Inspector General (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. See Appendix C for management's comments in their entirety.

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 and Technology Directorate, 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 Technology, Infrastructure, and Site Security Review (Project Number 24-133). Our objective was to determine whether the Postal Service established and implemented adequate information technology, physical, and environmental security controls at select [redacted] Division. Specifically, we performed reviews of the [redacted]. Our review assessed the effectiveness of controls protecting [redacted] at the select facilities. See Appendix A for additional information about this audit.

Background

The Postal Service operates more than 8,500 automated systems and equipment that [redacted] nearly half the world's mail.[2] Its [redacted] network consists of computer systems that manage, monitor, and control mail [redacted] functions at each of 313 total [redacted] facilities nationwide. The [redacted] computer systems control functions such as [redacted] For example, the [redacted] are vital for business operations and must be protected based on the risk to the Postal Service if the equipment were disabled or compromised. In addition, the [redacted] at the three sites we selected have a value of approximately $87.7 million.[6] 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 evaluated technical, physical, and environmental security controls at the [redacted], and [redacted] (see Figure 1). We selected these sites based on mail volume, square footage, and the variety of [redacted] used at each site. We also conducted a vulnerability assessment of the information technology systems at the [redacted] (see Table 3) because it had the largest square footage and widest variety of machine types of the three sites.

Figure 1. Sites Visited

[redacted]

Source: OIG created map based on information from the Postal Service.

[1] Our work included the [redacted].
[2] *Postal Facts*. https://facts.usps.com/.
[3] A mailpiece that is not a postcard, letter, or large envelope.
[4] Combines address and other tracking data into a barcode that is used to sort and track parcels, letters, and flats.
[5] Large envelopes, newsletters, and magazines.
[6] This includes $35.8 million at the [redacted], $19.5 million at the [redacted], and $32.5 million at the [redacted].

It is critical that proper controls are in place to reduce the risk of threats to [redacted], which may directly impact the timely [redacted] of mail.

Findings Summary

The Postal Service did not establish and implement effective information technology, physical, and environmental security controls at the [redacted] and [redacted]. Our review of technical security controls consisted of a vulnerability assessment, which identified issues related to misconfiguration of systems, systems with end-of-life products,[7] and out-of-date software[8] at the [redacted]. In addition, we found that opportunities existed for the Postal Service to improve its physical and environmental security controls at the [redacted] and [redacted]. Specifically, we found physical access security controls and account security for [redacted] were not consistently implemented or enforced. Also, we found that [redacted] was not configured according to Postal Service policy and best practices. Finally, we found that the [redacted] did not consistently implement adequate environmental security controls to protect access to controlled areas. See Table 2 for a summary of our findings at each site.

Table 2. Summary of Findings

Control Assessed	[redacted]	[redacted]	[redacted]
Vulnerability Assessment	N/A	N/A	X
Physical Security			
Access to Work Floors	✓	X	X
Access Control List	✓	✓	X
Access to Controlled Areas	✓	X	X
Account Security	X	X	X
Account Configuration	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 September 26, 2024.

[7] A product that is no longer sold, supported, or updated by the vendor.
[8] Applications or operating systems that have not been updated to the latest version released by the software vendor.

Finding #1: Information Technology Vulnerabilities on [redacted]

We determined the Postal Service misconfigured security controls on [redacted] and did not always remove or update end-of-life and out-of-date software installed on [redacted] at the [redacted], as required by internal policy and recommended by industry standards.

Vulnerabilities may be classified differently depending on the tool used. The Postal Service's vulnerability scanning tool classifies vulnerabilities as Low, Medium, High, and Critical based on the risk to the network. We opted to use a different scanning tool that classifies vulnerabilities as Moderate, Severe, or Critical based on the ease of vulnerability exploitation. According to best practices, using more than one scanning tool allows assessors to compare results of the tools and minimize the risk of missed vulnerabilities.[9] Additionally, using more than one scanning tool may be needed to achieve sufficient depth and coverage.[10]

Critical and severe risk vulnerabilities indicate that cybersecurity events could have a severe or catastrophic adverse effect on organizational operations, assets, or individuals. According to Postal Service policy, critical and severe risk vulnerabilities should be remediated within 30 to 90 days.[11] Our vulnerability assessment of the information technology and processing equipment at the [redacted] identified 2,394 critical and 12,400 severe vulnerabilities that existed across 13 of the 14 systems assessed (see Table 3 for amount of each type found and Appendix B for amount by [redacted]). This is similar to the number of vulnerabilities we identified in a prior [redacted] assessment.[12]

Of the vulnerabilities we identified, 12 critical and 67 severe were caused by misconfiguration of the [redacted]. For example, [redacted] were enabled on eight of 14 [redacted]. When [redacted] are enabled to access [redacted], shared accounts are used rather than unique, individual accounts, which prevents accountability.

We also found vulnerabilities from end-of-life operating systems, end-of-life applications, and out-of-date software. For example, [redacted] were using:

- Operating systems that the vendor stopped providing security patches[15] for as long as eight years ago.
- Applications that became end-of-life two and four years ago.
- Software that has been at end-of-life for as long as 14 years.

The identified vulnerabilities were on both the [redacted] and [redacted] networks (see Table 3). The [redacted] can only [redacted]. However, the [redacted] and the internet, increasing the risk of potential adverse impact to the [redacted] and the broader Postal Service network.

[9] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment,* Section 4.3, Vulnerability Scanning, dated September 2008.

[10] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* Section RA-5, Vulnerability Monitoring and Scanning, dated September 2020.

[11] *Patch Management Process,* Implementation Deadline, dated September 10, 2024.

[12] *Site Technical Assessment Review – January 2024* (Report Number 22-199-R24, dated January 25, 2024).

[13] [redacted]

[14] [redacted]

[15] A patch is the immediate solution to an identified problem and is provided to users or downloaded from the software vendor's website.

Table 3. Summary of Vulnerabilities

Vulnerability Type	# of Critical Vulnerabilities		# of Severe Vulnerabilities	
	[redacted]	[redacted]	[redacted]	[redacted]
Misconfiguration	0	12	20	47
End-of-Life Operating Systems	1	3	0	0
End-of-Life Applications	6	7	0	1
Out-of-Date Software	654	1,711	3,787	8,545
Total	**661**	**1,733**	**3,807**	**8,593**

Source: OIG vulnerability assessment results.

Of the vulnerabilities identified, the Cybersecurity and Infrastructure Security Agency (CISA)[16] determined 155 of them to be Known Exploited Vulnerabilities. CISA defined these as actively exploited vulnerabilities that have a clear remediation solution, such as a vendor-provided update or patch. According to CISA, all organizations should prioritize remediating these Known Exploited Vulnerabilities.

Postal Service policy states that all technology applications should be subject to vulnerability assessments, which include conducting scans on a regular basis to identify vulnerabilities.[17] In addition, Postal Service policy states that scan results must be analyzed to proactively secure information resources.[18] Finally, justifications for exceptions to conducting regular vulnerability scans should be documented.[19] However, the Postal Service did not have any exceptions to this policy documented for the 14 systems we assessed.

These issues occurred because the Postal Service did not verify that internal policies were implemented, to include proactively scanning the [redacted] network to identify vulnerabilities. In September 2024, the Postal Service's Chief Information Security Office (CISO) and Engineering Systems — the two offices responsible for oversight of information technology security — implemented a scanning and reporting process for vulnerability identification on [redacted] However, this process passively monitors the network for unusual activity that may be a result of an exploited vulnerability and does not proactively identify vulnerabilities.

A prior audit[20] released in January 2024 identified similar vulnerabilities related to misconfiguration, end-of-life, and out-of-date software on [redacted] in the [redacted]. Engineering Systems stated it is piloting a process to proactively scan the [redacted] network for vulnerabilities. It also stated it plans to implement this process nationwide and scan the [redacted] network for vulnerabilities on a regular basis. However, it had not provided an implementation plan with milestones or a schedule for vulnerability scanning.

Without a process to proactively scan the [redacted] network for vulnerabilities, the Postal Service is unable to identify weaknesses that could potentially allow attackers to cause disruptions to [redacted] and Postal Service operations.

Recommendation #1

We recommend the **Vice President, Engineering Systems**, and **Vice President, Chief Information Security Officer**, develop a plan to prioritize and remediate all identified vulnerabilities on the [redacted] and document all exceptions.

[16] CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.
[17] Handbook AS-805, *Information Security,* Section 11-1.2, Network Infrastructure, dated September 2022.
[18] Handbook AS-805, *Information Security,* Section 8-2.4.4, Patch Management, dated September 2022.
[19] Management Instruction AS 810-2022-14, *Cyber Risk Enterprise Network Scanning: Customer Impact Resolution, Responsibility Section,* dated September 2023.
[20] *Site Technical Assessment Review – January 2024* (Report Number 22-199-R24, dated January 25, 2024).

Recommendation #2

We recommend the **Vice President, Engineering Systems**, in coordination with the **Vice President, Chief Information Security Officer**, implement a process to identify and remediate vulnerabilities on the [redacted] network nationwide.

Postal Service Response

Management agreed with recommendations 1 and 2. For recommendation 1, management stated that Engineering Systems will work with CISO management teams to develop a plan to track and manage remediation of critical and high vulnerabilities identified during the audit, with a target implementation date of April 30, 2026. For recommendation 2, management stated that the Vice President Engineering Systems, in coordination with the Vice President Chief Information Security Officer, will implement a process that can be leveraged nationwide to identify and remediate vulnerabilities on the [redacted] network, with a target implementation date of June 30, 2026.

OIG Evaluation

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

Finding #2: [redacted] Account Security

[redacted] user accounts were not secured in accordance with Postal Service policy.[21] We observed that passwords were stored in locations that are easily accessible to anyone on the workroom floor at the [redacted] and [redacted]. Specifically, we found passwords written down and accessible to unauthorized personnel next to three of ten (30 percent) [redacted] at the [redacted], four of seven (57 percent) [redacted] at the [redacted] and [redacted], and eight of 16 (50 percent) [redacted] at the [redacted].

Employees wrote down passwords because they lacked training and awareness of Postal Service's password management policy. Additionally, there was no oversight to prevent passwords from being written down and posted near [redacted].

According to policy,[22] if a password is written down, it must be stored under an employee's personal control or in a tamper-resistant manner (for example, 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 disclosed to anyone other than the authorized user. 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.

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, leading to potential disruptions to operations.

During the audit, management at all three [redacted] removed written passwords and instructed employees to not write down passwords for [redacted].

Recommendation #3

We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted], conduct security awareness training for employees on password management policy and establish an oversight process to prevent passwords from being written down at the [redacted] and [redacted]

Postal Service Response

Management agreed with recommendation 3 and stated that all employees are required to take annual cyber security training that includes protection of passwords. Further, managers daily walks will include checking for written down passwords. The target implementation date for implementing this recommendation is June 30, 2025.

OIG Evaluation

Management's comments were responsive to recommendations 3 and corrective actions should resolve the issues identified in this finding.

[21] Handbook AS-805, *Information Technology,* Section 9-6 Authentication, dated September 2022.

[22] Handbook AS-805, *Information Technology,* Section 9-6.1.9, Password Protection, dated September 2022.

Finding #3: [redacted] Account Configuration

The Postal Service did not securely configure accounts for [redacted]. Specifically, management did not configure [redacted] so that password policies, account lockout controls, and audit log policies were implemented. Further, technical controls were not in place to prevent the use of [redacted] at the [redacted] (see Table 4).

Password, Account Lockout, and Audit Log Configuration

At all three [redacted], passwords were not changed for privileged accounts[24] on [redacted] workstations. According to policy,[25] passwords for privileged accounts must be set to automatically expire and require a new password every 30 days. However, management at the [redacted] was unaware whether the password for at least one [redacted] had ever been changed.

Additionally, a password was not changed after an unauthorized disclosure at the [redacted]. A [redacted] employee stated an unauthorized employee acquired a maintenance level account password and was using it on the [redacted]. Management at the site attempted to change the password by submitting a ticket to the [redacted] Support Center, but support center personnel denied the password change request. Policy[26] states that when passwords have been disclosed to someone other than the authorized user, the user must immediately change the password and notify CISO.

We also determined that all [redacted] assessed were unlocked and available to access without a password. The [redacted] manager at the [redacted] stated that none of the [redacted] are configured to lock after a set period, as required by policy.[27]

Further, account lockout policies were not set on the [redacted]. According to policy,[28] information resources must generate an alarm after several consecutive incorrect login attempts across multiple accounts. When the threshold for invalid consecutive attempts (normally six) for a given log-on ID is reached, the information resource must deactivate access for the log-on ID for a period of at least five minutes. Although this policy is not currently required for [redacted], it is considered an industry best practice.

Table 4. [redacted] Account Configuration

Account Configuration Control Assessed	[redacted]	[redacted]	[redacted]
Password Configuration	X	X	X
Account Lockout Configuration	X	X	X
Audit Log Configuration	X	X	X
Removeable Media Configuration	N/A	N/A	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 September 26, 2024.

[23] [redacted]

[24] Privileged accounts include administrator or maintenance level accounts that allow entitled users access to change data, alter configuration settings, and run programs, and permits unrestricted access to view data.

[25] Handbook AS-805, *Information Technology,* Section 9-6.1.6, Password Expiration, dated September 2022.

[26] Handbook AS-805, *Information Technology,* Section 9-6.1.9, Password Protection, dated September 2022.

[27] Handbook AS-805, *Information Technology,* Section 9-6.10.3, Time-Out Requirements (Re-authentication), dated September 2022.

[28] Handbook AS-805, *Information Technology,* Section 9-6.10.1, Session Establishment, dated September 2022.

Lastly, audit logs for each [redacted] were set to "no auditing," which means audit logs were not being captured for sessions established, authentication attempts, user access, and failed log-on attempts. According to policy,[29] each [redacted] must be capable of [redacted] so there is a [redacted]

Failure to implement secure configurations on [redacted] increases the risk of disruption to [redacted] by malicious actors or insider attacks. Once compromised, attackers can gain unauthorized access to systems, networks, and sensitive data and cause critical damage in the [redacted] environment.

In response to recommendations from a prior audit,[30] Engineering Systems stated that requiring individual user accounts and account lockout policies would cause delays and impact operations in the [redacted]. Because this prior audit recommendation is in resolution as of February 2025, we will not make an additional recommendation on this matter.

[redacted]

We found that the use of [redacted] on [redacted] is not restricted to authorized users. We tested this by [redacted] We found we could [redacted] on five of six (83 percent) [redacted] we tested in the [redacted].

Per Postal Service policy,[31] [redacted]

[redacted]

Without proper security controls in place to prevent the use of [redacted], such as [redacted], there is an increased risk that unauthorized users could compromise the [redacted] and networks. Once compromised, attackers can gain unauthorized access to systems, networks, and sensitive data and cause critical damage in the [redacted] environment.

Engineering Systems stated that they are installing agents through the endpoint monitoring platform[32] on [redacted] that would be able to detect unauthorized [redacted] and only allow access to approved [redacted].

Recommendation #4

We recommend the **Vice President, Engineering Systems** implement controls on [redacted] to prevent unauthorized personnel from using unauthorized [redacted].

Postal Service Response

Management agreed with recommendation 4 and stated that Engineering Systems is using an endpoint management agent and [redacted] whitelisting policy to prevent the use of unauthorized [redacted]. Management added that current systems that cannot support this technology will require a technology refresh. The target implementation date is January 31, 2027.

OIG Evaluation

Management's comments were responsive to recommendation 4 and corrective actions should resolve the issues identified in this finding.

[29] [redacted]
[30] *Site Technical Assessment Review – January 2024* (Report Number 22-199-R24, dated January 25, 2024).
[31] Handbook AS-805, *Information Security*, Section 5-5 Prohibited Uses of Information Resources, dated September 2022.
[32] Safeguards implemented to protect end-user machines, such as workstations and laptops, against attack.

Finding #4: Physical Security Access Controls for Controlled Areas

While the [redacted] properly implemented access controls, the [redacted] and [redacted] had not properly implemented controls to restrict and record access to work floors and controlled areas.

According to Postal Service policy,[33] a single point of entry to [redacted] should accommodate both visitors and employees. The entryway must be designed to deny customers and other outsiders access into the remainder of the facility and to keep off-duty employees and visitors from having access to the workroom after they enter the building. Management allows or restricts access to these locations using ePhysical Access Control System (ePACS)[34] readers installed at the [redacted]. Employees must scan their badges on ePACS readers to access the facility. Further, access to controlled areas, such as server rooms,[35] must be restricted to personnel whose duties require access to these areas and must be controlled with ePACS readers. If access logs are not captured by ePACS readers for the [redacted] and controlled areas within the [redacted], management cannot restrict and monitor employee access to these areas. Finally, the [redacted] manager is responsible for performing facility security reviews and resolving identified issues. This includes issues with door latches, ePACS readers, and access to controlled areas.

Access to Work Floors

[redacted] management did not always ensure the entrances to the work floor in the [redacted] and [redacted] were secure in accordance with policy.[36]

At the [redacted], maintenance tickets showed the lock on the south dock door had not consistently worked since September 2020. Although the ePACS reader was active, the door was not latching properly; therefore, anyone could access the work floor from outside through this door without the ePACS system authorizing or recording their entrance. This issue reoccurred at least twelve times since September 2020 due to contractors forcing the door open and causing the latch to break. Management repeatedly submitted tickets to the Facilities Single Source Provider (FSSP)[37] to fix the latch, but contractors continued to break the door after FSSP fixed it. On August 29, 2024, [redacted] management submitted a ticket to FSSP to move access control and re-entry hardware to a different door that could be monitored more effectively to prevent contractors from damaging the door.

In the [redacted], the facility used mechanical[38] locks on the doors to the work floor when it should have had ePACS readers installed. Management was not aware of the requirement to have ePACS readers installed and operating on the exterior door of the facility.

During our walkthrough of the [redacted], we identified eight broken ePACS readers. The [redacted] manager stated that they were aware of only four broken readers. The four additional broken ePACS readers were on the work floor. Management was not aware of these four broken ePACS readers because it did not thoroughly complete the yearly assessment of the physical security of the building.

Also, in the [redacted], we observed the facility's high speed garage doors and storm doors on the docks were broken and left open with no employee in the immediate area multiple times during our site visits. In addition, three of the emergency exit doors had been replaced with temporary plywood coverings due to the routing of tubes and wires through the propped open doors for temporary air conditioning units (see Figure 2). These temporary coverings did not prevent access to the facility, and one did not completely cover the doorway. [redacted] management stated this occurred because there was no other option to route the tubes and wires for the temporary air conditioning units.

[33] Handbook RE-5, *Building and Site Security Requirements,* Section 4-3.1, General Security Standards, dated September 2009.
[34] ePACS is a standardized badge access system used to grant access to Postal Services facilities.
[35] Server rooms in [redacted] contain computers that make up the [redacted] network. These computers connect the [redacted] on the work floor.
[36] Handbook RE-5, *Building and Site Security Requirements,* [redacted], General Security Standards.
[37] FSSP is a response line for all facilities construction, repair, alterations and service-related requests.
[38] Includes manual locks and keys, padlocks, and other nonelectric systems.

On November 21, 2024, [redacted] management stated it was working to reinforce the plywood doors to make them more secure until the new air conditioning units are installed in August 2025, at which time they will reinstall the actual doors.

Figure 2. Emergency Exit Temporary Covering and Air Conditioning Tubes

[redacted]

Note: The photos above show two separate doors at the [redacted].
Source: OIG observation at [redacted] on September 24, 2024.

Access to Controlled Areas

Controlled areas, such as computer rooms that store computers and communication equipment, were not secured according to policy.[39]

During our site visit to the [redacted], we found the door to the computer room unlocked because [redacted] personnel did not have a key for the lock. When we identified this issue and brought it to [redacted] management's attention, an onsite maintenance employee installed a new keyed mechanical lock on the door to the computer room.

At the [redacted], we observed that the computer room was not secure. Specifically, the door did not latch, the ePACS reader was broken and not recording employee access, and employees used it as a storage area and unofficial break room. Management submitted tickets for the broken door latch and ePACS reader after we brought it to its attention.

[redacted] management did not address these issues sooner because it was not aware that the computer room was considered a controlled area.

Failure to secure entrances to work floors and controlled areas can allow unauthorized access to facilities or [redacted] and lead to disruption of operations with no ability to determine who caused the disruption.

Recommendation #5

We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted], implement repairs and coordinate with the **Chief Postal Inspector** to verify all doors are secured properly to prevent unauthorized access to work floors and controlled areas at the [redacted] and [redacted] [redacted].

Recommendation #6

We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted], publish an alert to [redacted] managers to explain the requirements for physical security requirements of controlled areas, such as computer rooms.

[39] 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.

Postal Service Response

Management agreed with recommendations 5 and 6. For recommendation 5, management stated that the Security Control Officers at the [redacted] and [redacted] will conduct a Vulnerability and Risk Assessment to assess overall security at each location and ensure security systems are functioning to prevent unauthorized access and notify a Physical Security Specialist of any deficiencies to assist in remediation. The target implementation date is June 30, 2025. For recommendation 6, a physical security policy was issued to all [redacted] division [redacted] on March 10, 2025. While management provided a target implementation date of June 30, 2025, the OIG will validate that the policy was issued to the [redacted] before we close this recommendation.

OIG Evaluation

Management's comments were responsive to recommendations 5 and 6 and corrective actions should resolve the issues identified in this finding.

Access Control Lists

Badge access to the three [redacted] was not always managed effectively. Specifically, management at one facility did not consistently remove access for separated[40] employees to coincide with the employee's termination date, according to policy.[41]

We analyzed access control lists for all three [redacted] for the months of March to September 2024 and found that four of 80 (five percent) terminated employees still retained access to the [redacted] [redacted]. Also, one of the terminated employees successfully gained access to the facility by scanning their badge three months after separation. This occurred because there was no written procedure for offboarding separated employees at any of the facilities assessed.

According to Postal Service policy, a separated employee's manager or supervisor must ensure their computer log-on ID, building-access authorizations, and access to Postal Service information systems are terminated, coinciding with the employee's effective date of departure.

Failure to maintain an accurate access control list for [redacted], including removal of separated employees, can lead to unauthorized access to the work floor and interference with business operations.

Recommendation #7

We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted], deactivate employee badges in the electronic Physical Access Control System at the [redacted] [redacted] for all separated employees.

Recommendation #8

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

Postal Service Response

Management agreed with recommendations 7 and 8. For recommendation 7, management stated it has implemented a process to ensure all separated employees are deactivated from the ePACS system at the [redacted] and for recommendation 8, management stated it has issued an out-processing policy for all [redacted] Division [redacted]. The target implementation date for both recommendations is June 30, 2025.

OIG Evaluation

Management's comments were responsive to recommendations 7 and 8 and corrective actions should resolve the issues identified in this finding.

[40] For the purposes of this report, separated employees include those who were transferred/reassigned, retired, resigned, or terminated.
[41] Handbook AS-805, *Information Security*, Section 6-6, Departing Personnel, dated September 2022.

Finding #5: Protection From Environmental Hazards

The Postal Service did not always implement the necessary controls to protect [redacted] from potential harm that could be caused by environmental factors. [redacted] can be protected from environmental hazards through a variety of methods, including heating, ventilation, and air conditioning (HVAC) systems,[42] undamaged roofing, uninterruptable power supplies[43] with surge protection, and backup generators. However, we found deficiencies with these systems.

HVAC

At the [redacted], the air conditioning system was not fully functional. Specifically, eight of 23 (35 percent) roof top air conditioning units were not working at the time of our site visit. To address the issue, the facility had two temporary air conditioning units installed in June of 2024.

The [redacted] contacted FSSP multiple times within the last two years for air conditioning issues. An FSSP ticket from April 25, 2024, stated that there were heavy roof leaks near the units and that most roof leaks were caused by rotted retainer pans underneath the units.

On November 12, 2024, an architect/engineer from Facilities[44] stated that the small airport located next to the [redacted] increases the degradation of the air conditioning units. They also said the previous units lasted only about five years and that lack of regular maintenance (cleaning coils and filters, replacing belts, and preventing rust) contributed to units failing. Design and Construction is replacing these units with an estimated completion date of August 2025 and applying an anti-corrosion coating to avoid the current issues.

Under Postal Service policy,[45] safeguards must be implemented to monitor and maintain acceptable levels of temperature and humidity, and protection against roof leaks must be implemented.

Persistent HVAC issues pose potential harm to [redacted] from water damage and insufficient protection from the area's humidity and high temperatures, which could impact operations.

Recommendation #9

We recommend the **Senior Director, Division [redacted] Operations,** [redacted], implement controls to verify routine maintenance is performed on air conditioning units at the [redacted]

Postal Service Response

Management disagreed with recommendation 9, stating that HVAC maintenance is contracted for and verified by local maintenance personnel and that it has taken actions to improve the HVAC systems.

OIG Evaluation

Management's comments were not responsive to recommendation 9. The previous HVAC systems only lasted about 5 years and lack of maintenance was documented as contributing to the rapid deterioration. We view management's disagreement with the recommendation as unresolved and will work with management though the formal audit resolution process.

Roofing

The [redacted] had several tarps on the work floor above some [redacted] and a mail staging area to protect the [redacted] from water leaking from the damaged roof into the facility (see Figure 3). Additionally, during our site visit in September of 2024, employees placed empty mail bins on the ground to collect water from roof leaks during a rainstorm.

[42] Used to prevent the overheating or freezing of information systems.
[43] 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.
[44] Provides real estate and construction services for the Postal Service.
[45] Handbook AS-805, *Information Security,* Section 7-5, Environmental Security, dated September 2022.

Figure 3. Tarps for Leaks Above [redacted]

[redacted]

Source: OIG observation at [redacted] on September 23, 2024.

According to policy,[46] plastic sheets are considered protection against water damage from roof leaks. However, protection against weather-related damage was not sufficiently implemented given that we observed water leaking onto the floors that had to be caught in bins during our site visit.

According to maintenance personnel, there is ongoing repair work for the facility's roof. An FSSP ticket dated June 14, 2024, described the roof as being in "poor condition" and indicated that the facility made eight calls related to the roof within the past 12 months and 23 calls within the past six years.

If the [redacted] roof is not sound, then [redacted] is at risk of water damage. During a meeting November 6, 2024, Facilities stated that a roof replacement project began in August 2024 and is scheduled to be completed in 2025.

Recommendation #10

We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] [redacted], complete planned replacement of air conditioning units and roof at the [redacted] [redacted]

Postal Service Response

Management disagreed with recommendation 10, stating that a contract has been awarded for a new HVAC system.

OIG Evaluation

Management's comments were not responsive to recommendation 10. While management stated it has a contract in place to replace the HVAC systems, it did not comment on replacement of the roof. We view management's disagreement with the recommendation as unresolved and will work with management though the formal audit resolution process.

Uninterruptable Power Supplies and Surge Protectors

Uninterruptable power supplies provide battery backup to allow for a proper power down of equipment. This protects from data loss, which can occur in a sudden loss of power. Surge protectors protect equipment from damage caused by a surge of power, such as from a lightning strike. Four [redacted] systems at the [redacted] and [redacted] [redacted] had disabled or missing uninterruptable power supplies and/or surge protectors (see Table 5).

Table 5. Disabled or Missing Uninterruptable Power Supplies and Surge Protectors

[redacted]	[redacted]		[redacted]	
	Uninterruptable Power Supply	Surge Protector	Uninterruptable Power Supply	Surge Protector
[redacted]	Inactive	✓		
[redacted]	✓		Both Missing	
[redacted]	✓		Both Missing	
[redacted]	✓		Both Missing	

Note: ✓ indicates that an uninterruptable power supply and/or surge protector was installed and functioning.
Source: OIG analysis results as of September 26, 2024.

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

Maintenance personnel from each [redacted] stated that there was no process in place for replacing uninterruptable power supplies before they died. Rather, replacement requests are not submitted until after the uninterruptable power supply no longer works. Surge protection and uninterruptable power supplies must be implemented for information resources.[47] Without proper protection from electrical power surges and temporary power outages, [redacted] is at risk of damage, potentially leading to [redacted] outages.

At the [redacted], three ePACS readers were inactive due to an outage caused by a storm prior to our site visit in July 2024. Maintenance personnel stated that the system was not connected to a surge protector to protect against power fluctuations, such as the one caused by that storm. We also found that ePACS readers were not plugged into surge protectors at the [redacted] or [redacted].

Computer rooms for [redacted] are secured via ePACS card access readers, which cannot prevent unauthorized access if they are broken due to insufficient protection from power surges or outages.

During a meeting on November 12, 2024, [redacted] management provided evidence that surge protectors were installed for ePACS readers after our assessment.

Recommendation #11

We recommend the **Senior Director, Maintenance Operations**, install surge protectors for access control systems and [redacted] in the [redacted] and [redacted]

Recommendation #12

We recommend the **Senior Director, Maintenance Operations**, install uninterruptable power supplies for [redacted] in the [redacted] and [redacted], or document exceptions to policy, as appropriate. In addition, implement controls to ensure uninterruptable power supplies are assessed and replaced before they become non-functional.

Postal Service Response

Management disagreed with recommendations 11 and 12. Regarding recommendation 11, management stated that generators are not required and that existing generators are on a contract for repairs, as needed.

For recommendation 12, management stated that systems deployed with uninterruptable power supplies have procedures to validate their operability. For those systems with uninterruptable power supplies that do not have procedures to validate their operability, the procedures will be updated to incorporate the appropriate checks. Finally, management stated the combined sites have only experienced 4 hours of degraded operations in fiscal year 2024 due to power issues.

OIG Evaluation

Management's comments were not responsive to recommendations 11 and 12. Surge protection and uninterruptable power supplies are required for information resources according to Postal Service policy. Further, we found broken access control systems at the [redacted] due to a power surge caused by a storm. We view management's disagreement with the recommendations as unresolved and will work with management though the formal audit resolution process.

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

Backup Generators

We also found two of three (66 percent) backup generators at the [redacted] were non-functional.

Backup generators provide power to continue [redacted] during a power outage. [redacted] management had an open repair ticket for one generator that was submitted on April 23, 2024, and opened another ticket to repair the second generator after we brought the issue to its attention. Maintenance personnel did not identify the issue with the generators because they did not proactively check for non-functional generators and did not follow up on tickets to verify they were repaired.

Postal Service policy states that a long-term alternate power source must be implemented to maintain minimal operational capability in the event of a power outage.[48] Although there were backup generators on site in need of repair at the [redacted] [redacted], Postal Service maintenance personnel stated that it is sufficient to bring in portable generators to support [redacted] operations in the event of a power outage. However, if the onsite generators at the [redacted] were functional, then Postal would not need to incur the additional cost of bringing in portable generators or lose processing time while waiting for the portable generators to arrive.

Failure to implement appropriate short-term and long-term alternate power sources could lead to disruptions in [redacted] during a power outage.

Recommendation #13

We recommend the **Senior Director, Maintenance Operations**, implement a process to regularly verify the operation of backup generators at the [redacted] to include following up on outstanding repair tickets to ensure the generators are operational.

Postal Service Response

Management disagreed with recommendation 13, stating that backup generators are not required, are on a maintenance schedule, and that the generator that is currently not operational has a ticket for repair.

OIG Evaluation

Management's comments were not responsive to recommendation 13. During our site visit, we observed that two of three generators were not functional and that only one had a ticket for repair, submitted in April 2024, that was still open at the time of our audit. We view management's disagreement with the recommendation as unresolved and will work with management though the formal audit resolution process.

Temperature and Water Damage

The [redacted] had issues pertaining to high temperature levels and water damage. Specifically, we found:

- A ceiling vent used to help cool an electrical equipment room was not working.
- Condensation from the temporary air conditioning unit's tubing creating a pool of water on the work floor near high voltage electrical equipment.

Postal Service policy[49] requires that information resources, such as servers, be protected from unacceptable temperature levels and water damage.

An assessment of the facility's HVAC dated November 10, 2023, recommended that the electrical rooms be air conditioned because of the high heat and humidity in this environment. The maintenance manager could not confirm that the areas holding electrical equipment were checked periodically, although there are yearly and five-year inspections performed for the equipment.

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

Undetected environmental hazards could threaten the functionality of both the facility and its [redacted] if they are not mitigated in a timely manner.

Recommendation #14

We recommend the **Senior Director, Division [redacted] Operations, [redacted]**, implement a process to regularly check for environmental hazards on the work floor and in controlled areas at the [redacted]

Postal Service Response

Management disagreed with recommendation 14, stating that abatements were put in place for issues identified during the audit and tickets submitted to repair the issues.

Further, management noted that the 1767 process is in place for employees to report hazards for abatement.

OIG Evaluation

Management's comments were not responsive to recommendation 14. During our site visit, we observed problems with the HVAC, roofing, uninterruptable power supplies, surge protection, and backup generators that did not have tickets submitted for abatement or repair. We view management's disagreement with the recommendation as unresolved and will work with management though the formal audit resolution process.

Appendices

Appendix A: Additional Information

Scope and Methodology

We conducted site work in the [redacted] Division from July 29 to August 1 and September 23 to 26, 2024. We judgmentally selected three [redacted] in this division with the [redacted] and widest variety of [redacted] for our review of physical and environmental controls: [redacted], and [redacted]. We also conducted vulnerability scans on 14 [redacted] that support [redacted] at the [redacted].

To accomplish our objective, we:

- Obtained and reviewed physical security policies, processes, and procedures designed to prevent unauthorized access to facilities and [redacted] to gain an understanding of the environment.
- Observed and evaluated physical and environmental controls that protect [redacted] and 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 personnel to determine the roles and responsibilities for the Postal Service's physical and environmental security program and controls.
- Conducted vulnerability scanning on one of each of the 14 types of [redacted] and performed network data capture of the [redacted] environment to capture vulnerabilities that could be used to disrupt a network or impact operations and reviewed account configurations and security.

We conducted this performance audit from July 2024 through January 2025 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on February 21, 2025, and included its 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, risk assessment, 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 vulnerability assessment, badge access, and site selection data by tracing the data to source documents and through performance testing. We determined that the data were sufficiently reliable for the purposes of this report.

Appendix B: Number of Vulnerabilities by [redacted] [redacted] Type

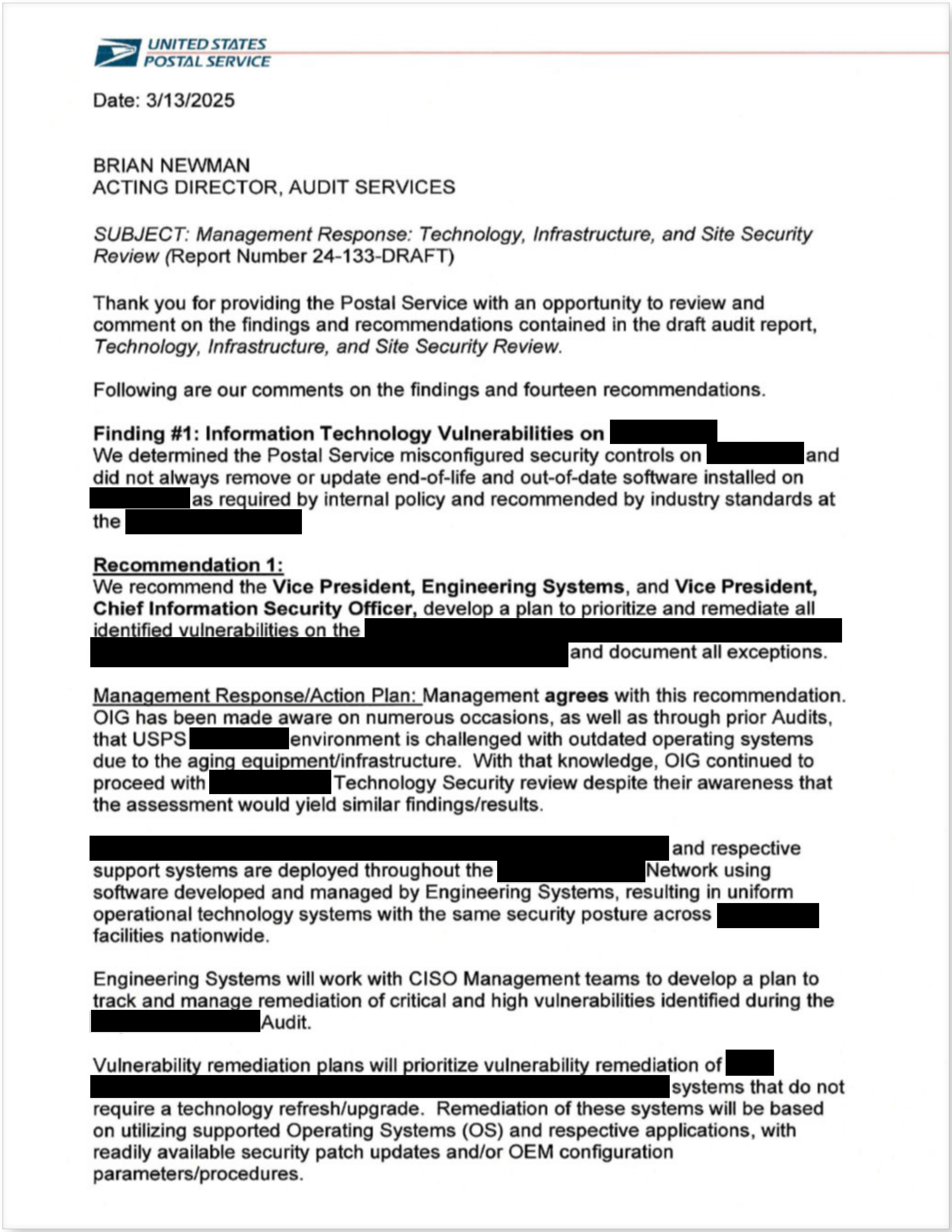
[redacted]	# of Critical Vulnerabilities	# of Severe Vulnerabilities
[redacted]	301	1,345
[redacted]	189	1,253
[redacted]	32	73
[redacted]	1	0
[redacted]	443	2,903
[redacted]	0	0
[redacted]	138	584
[redacted]	137	583
[redacted]	3	1,559
[redacted]	732	1,504
[redacted]	80	618
[redacted]	335	1,971
[redacted]	3	2
[redacted]	0	5
Total	**2,394**	**12,400**

Source: OIG vulnerability assessment results.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Site Technical Assessment Review – January 2024	Our objective is to determine whether the Postal Service has established and implemented adequate controls at selected [redacted] [redacted] in the [redacted] Division.	22-199-R24	January 25, 2024	$0

Appendix C: Management's Comments



UNITED STATES
POSTAL SERVICE

Date: 3/13/2025

BRIAN NEWMAN
ACTING DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Technology, Infrastructure, and Site Security Review (Report Number 24-133-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, *Technology, Infrastructure, and Site Security Review*.

Following are our comments on the findings and fourteen recommendations.

Finding #1: Information Technology Vulnerabilities on [redacted]
We determined the Postal Service misconfigured security controls on [redacted] and did not always remove or update end-of-life and out-of-date software installed on [redacted] as required by internal policy and recommended by industry standards at the [redacted]

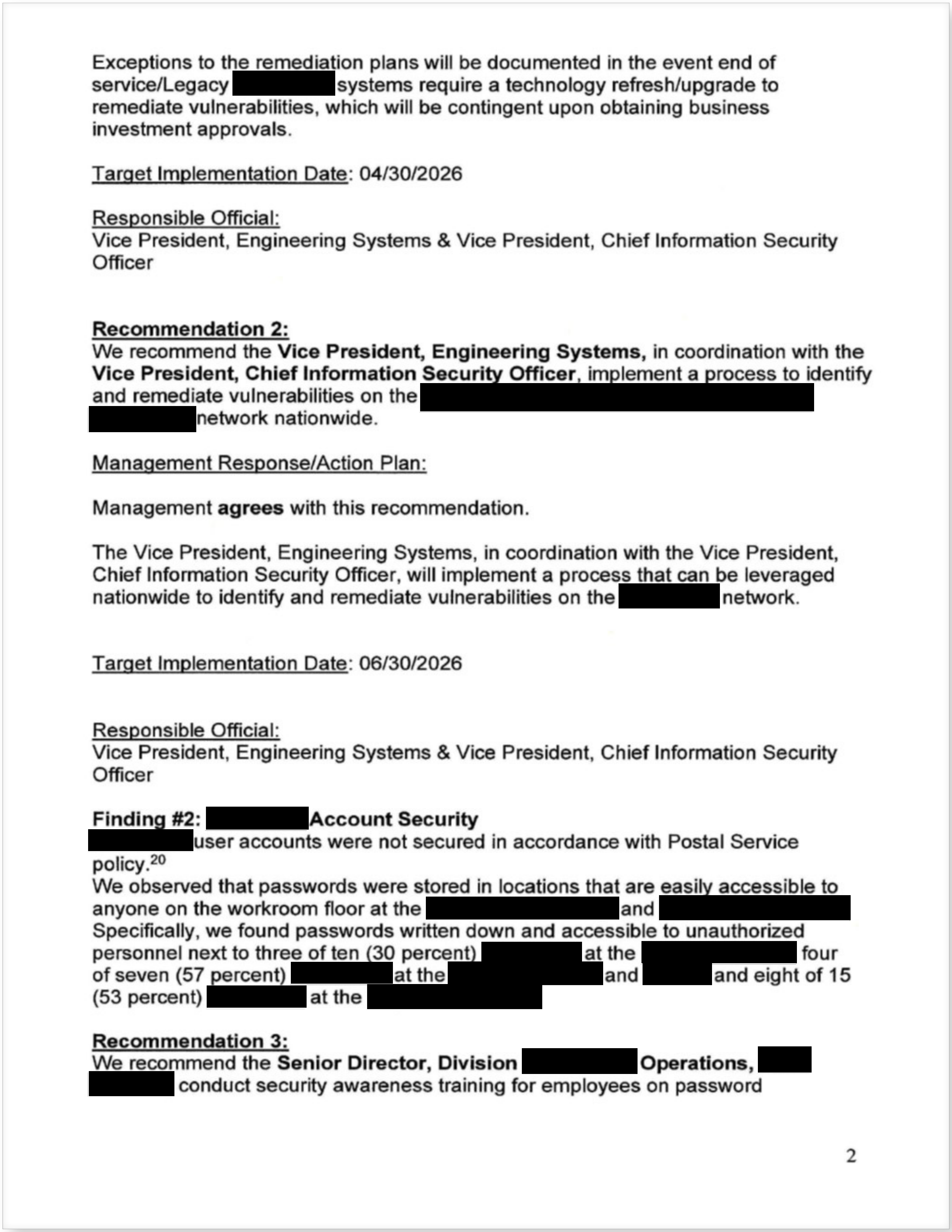
Recommendation 1:
We recommend the **Vice President, Engineering Systems**, and **Vice President, Chief Information Security Officer,** develop a plan to prioritize and remediate all identified vulnerabilities on the [redacted] and document all exceptions.

Management Response/Action Plan: Management **agrees** with this recommendation. OIG has been made aware on numerous occasions, as well as through prior Audits, that USPS [redacted] environment is challenged with outdated operating systems due to the aging equipment/infrastructure. With that knowledge, OIG continued to proceed with [redacted] Technology Security review despite their awareness that the assessment would yield similar findings/results.

[redacted] and respective support systems are deployed throughout the [redacted] Network using software developed and managed by Engineering Systems, resulting in uniform operational technology systems with the same security posture across [redacted] facilities nationwide.

Engineering Systems will work with CISO Management teams to develop a plan to track and manage remediation of critical and high vulnerabilities identified during the [redacted] Audit.

Vulnerability remediation plans will prioritize vulnerability remediation of [redacted] systems that do not require a technology refresh/upgrade. Remediation of these systems will be based on utilizing supported Operating Systems (OS) and respective applications, with readily available security patch updates and/or OEM configuration parameters/procedures.



Exceptions to the remediation plans will be documented in the event end of service/Legacy [redacted] systems require a technology refresh/upgrade to remediate vulnerabilities, which will be contingent upon obtaining business investment approvals.

Target Implementation Date: 04/30/2026

Responsible Official:
Vice President, Engineering Systems & Vice President, Chief Information Security Officer

Recommendation 2:
We recommend the **Vice President, Engineering Systems,** in coordination with the **Vice President, Chief Information Security Officer**, implement a process to identify and remediate vulnerabilities on the [redacted] network nationwide.

Management Response/Action Plan:

Management **agrees** with this recommendation.

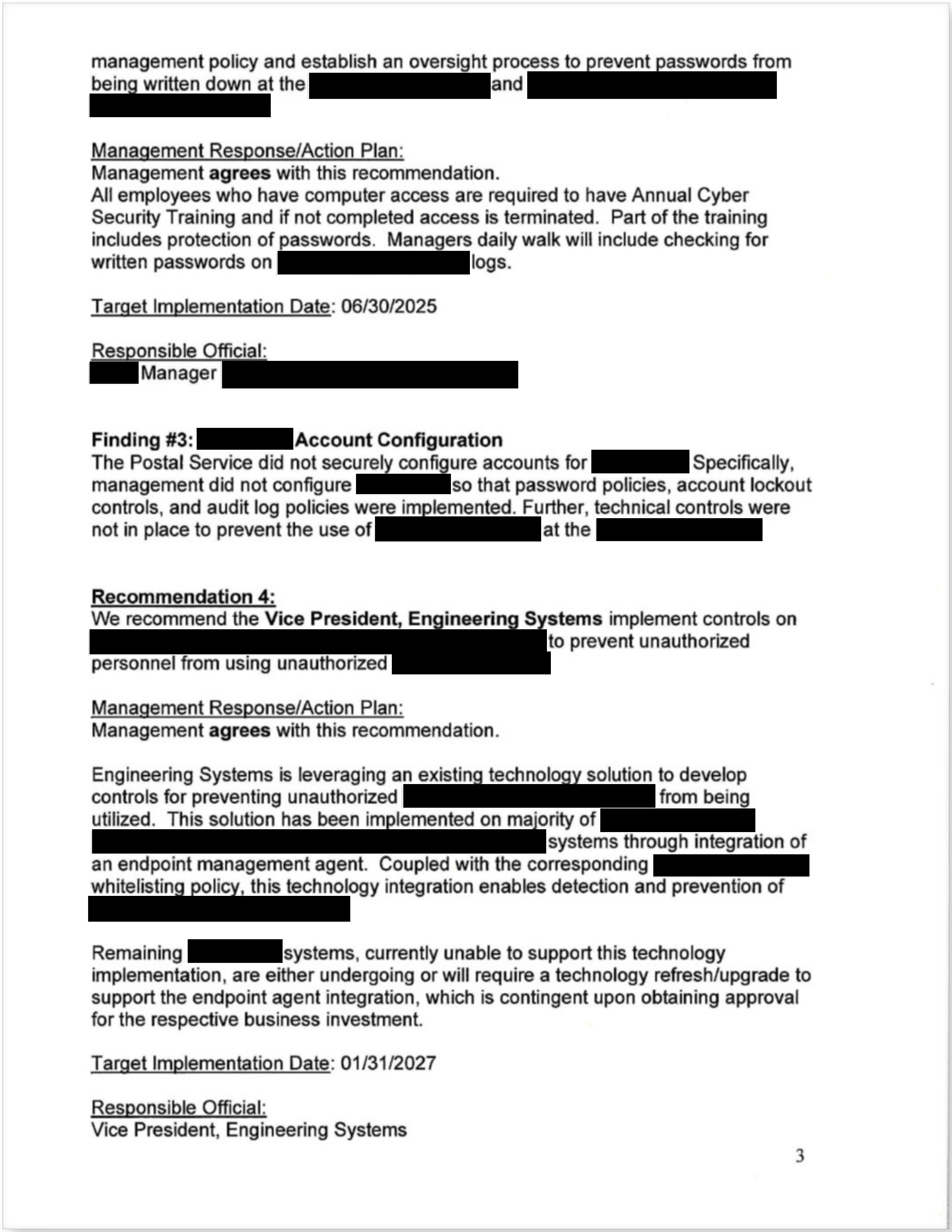
The Vice President, Engineering Systems, in coordination with the Vice President, Chief Information Security Officer, will implement a process that can be leveraged nationwide to identify and remediate vulnerabilities on the [redacted] network.

Target Implementation Date: 06/30/2026

Responsible Official:
Vice President, Engineering Systems & Vice President, Chief Information Security Officer

Finding #2: [redacted] Account Security
[redacted] user accounts were not secured in accordance with Postal Service policy.[20]
We observed that passwords were stored in locations that are easily accessible to anyone on the workroom floor at the [redacted] and [redacted] Specifically, we found passwords written down and accessible to unauthorized personnel next to three of ten (30 percent) [redacted] at the [redacted] four of seven (57 percent) [redacted] at the [redacted] and [redacted] and eight of 15 (53 percent) [redacted] at the [redacted]

Recommendation 3:
We recommend the **Senior Director, Division [redacted] Operations,** [redacted] conduct security awareness training for employees on password



management policy and establish an oversight process to prevent passwords from being written down at the [redacted] and [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.
All employees who have computer access are required to have Annual Cyber Security Training and if not completed access is terminated. Part of the training includes protection of passwords. Managers daily walk will include checking for written passwords on [redacted] logs.

Target Implementation Date: 06/30/2025

Responsible Official:
[redacted] Manager [redacted]

Finding #3: [redacted] Account Configuration
The Postal Service did not securely configure accounts for [redacted] Specifically, management did not configure [redacted] so that password policies, account lockout controls, and audit log policies were implemented. Further, technical controls were not in place to prevent the use of [redacted] at the [redacted]

Recommendation 4:
We recommend the **Vice President, Engineering Systems** implement controls on [redacted] to prevent unauthorized personnel from using unauthorized [redacted]

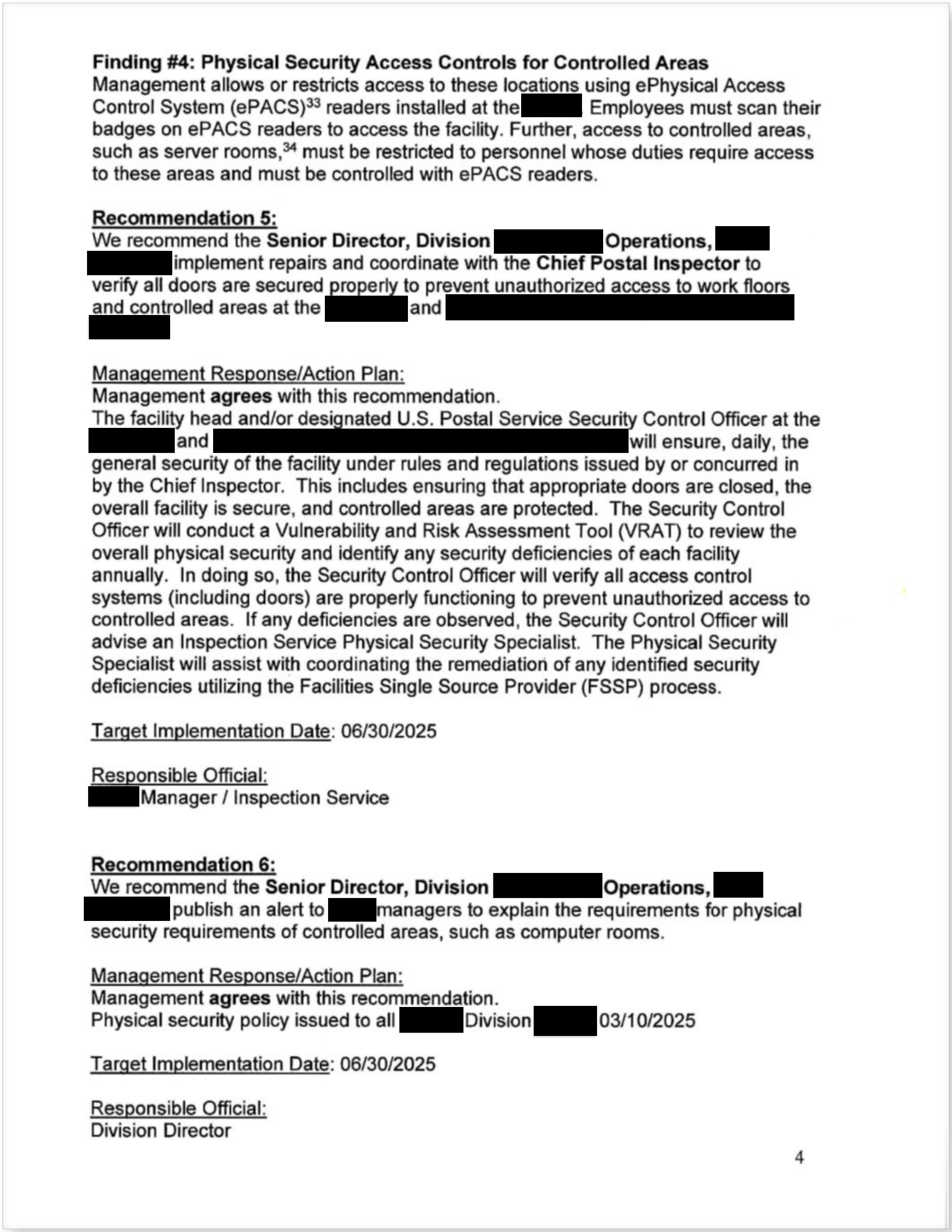
Management Response/Action Plan:
Management **agrees** with this recommendation.

Engineering Systems is leveraging an existing technology solution to develop controls for preventing unauthorized [redacted] from being utilized. This solution has been implemented on majority of [redacted] systems through integration of an endpoint management agent. Coupled with the corresponding [redacted] whitelisting policy, this technology integration enables detection and prevention of [redacted]

Remaining [redacted] systems, currently unable to support this technology implementation, are either undergoing or will require a technology refresh/upgrade to support the endpoint agent integration, which is contingent upon obtaining approval for the respective business investment.

Target Implementation Date: 01/31/2027

Responsible Official:
Vice President, Engineering Systems



Finding #4: Physical Security Access Controls for Controlled Areas
Management allows or restricts access to these locations using ePhysical Access Control System (ePACS)[33] readers installed at the [redacted] Employees must scan their badges on ePACS readers to access the facility. Further, access to controlled areas, such as server rooms,[34] must be restricted to personnel whose duties require access to these areas and must be controlled with ePACS readers.

Recommendation 5:
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] implement repairs and coordinate with the **Chief Postal Inspector** to verify all doors are secured properly to prevent unauthorized access to work floors and controlled areas at the [redacted] and [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.
The facility head and/or designated U.S. Postal Service Security Control Officer at the [redacted] and [redacted] will ensure, daily, the general security of the facility under rules and regulations issued by or concurred in by the Chief Inspector. This includes ensuring that appropriate doors are closed, the overall facility is secure, and controlled areas are protected. The Security Control Officer will conduct a Vulnerability and Risk Assessment Tool (VRAT) to review the overall physical security and identify any security deficiencies of each facility annually. In doing so, the Security Control Officer will verify all access control systems (including doors) are properly functioning to prevent unauthorized access to controlled areas. If any deficiencies are observed, the Security Control Officer will advise an Inspection Service Physical Security Specialist. The Physical Security Specialist will assist with coordinating the remediation of any identified security deficiencies utilizing the Facilities Single Source Provider (FSSP) process.

Target Implementation Date: 06/30/2025

Responsible Official:
[redacted] Manager / Inspection Service

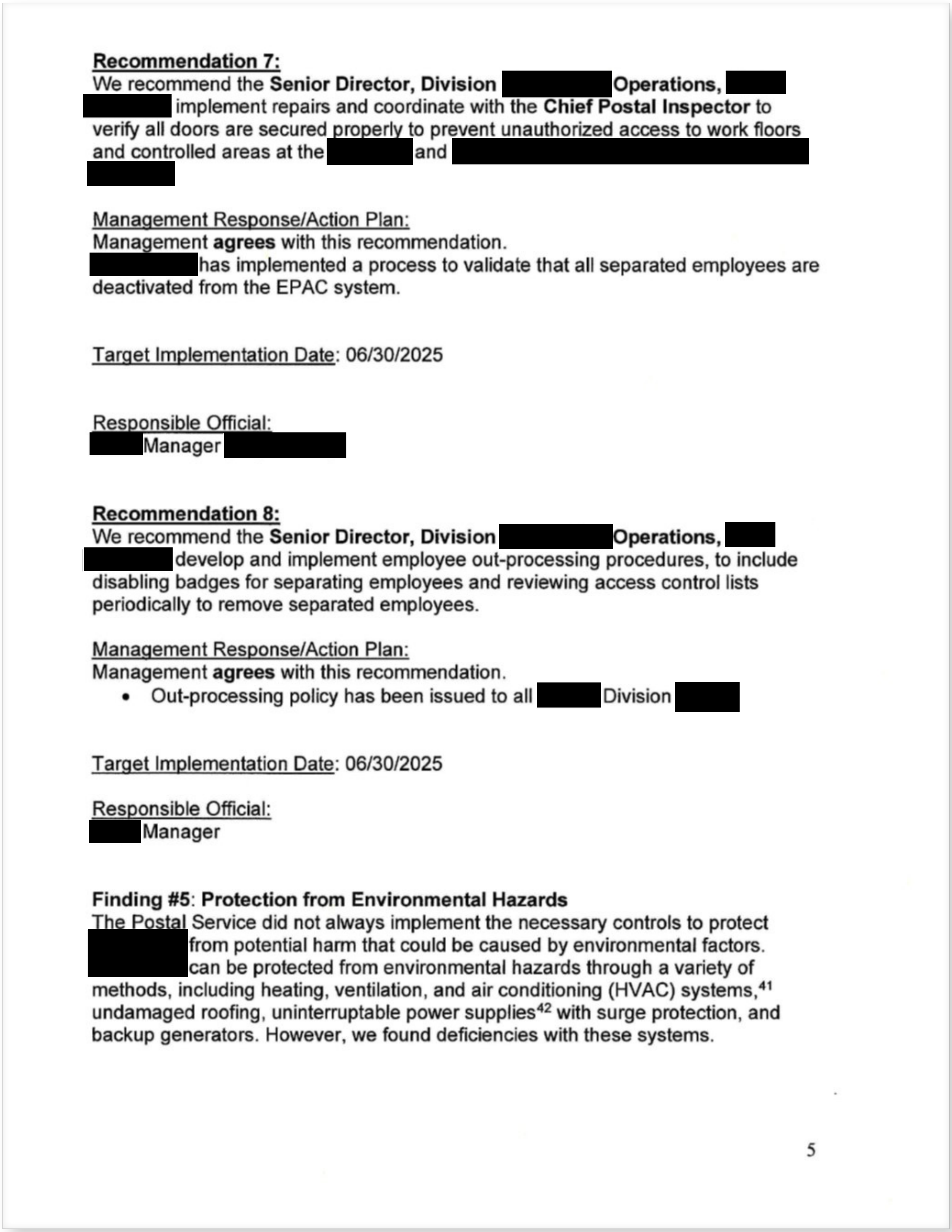
Recommendation 6:
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] publish an alert to [redacted] managers to explain the requirements for physical security requirements of controlled areas, such as computer rooms.

Management Response/Action Plan:
Management **agrees** with this recommendation.
Physical security policy issued to all [redacted] Division [redacted] 03/10/2025

Target Implementation Date: 06/30/2025

Responsible Official:
Division Director

4



Recommendation 7:
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] [redacted] implement repairs and coordinate with the **Chief Postal Inspector** to verify all doors are secured properly to prevent unauthorized access to work floors and controlled areas at the [redacted] and [redacted] [redacted]

Management Response/Action Plan:
Management **agrees** with this recommendation.
[redacted] has implemented a process to validate that all separated employees are deactivated from the EPAC system.

Target Implementation Date: 06/30/2025

Responsible Official:
[redacted] Manager [redacted]

Recommendation 8:
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] [redacted] develop and implement employee out-processing procedures, to include disabling badges for separating employees and reviewing access control lists periodically to remove separated employees.

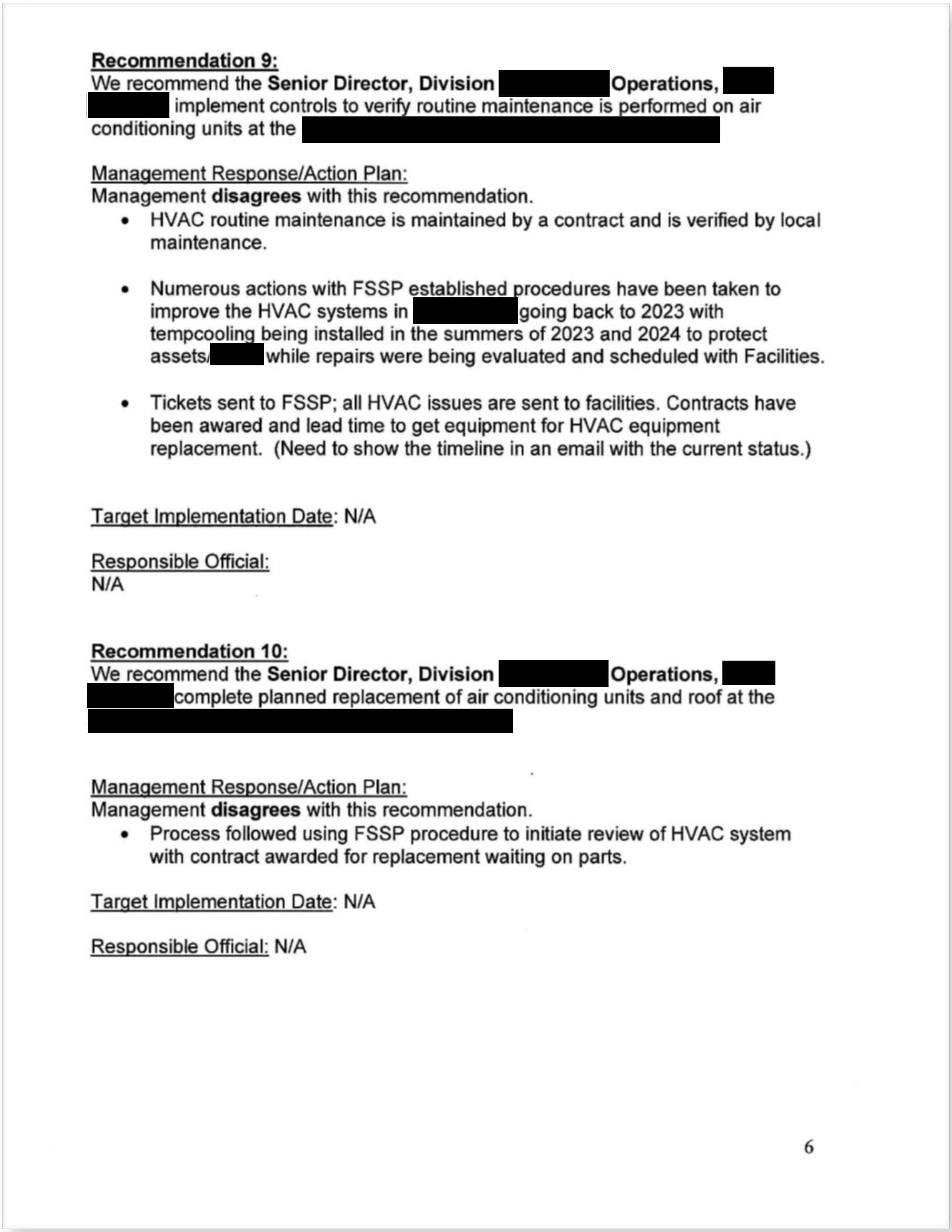
Management Response/Action Plan:
Management **agrees** with this recommendation.

- Out-processing policy has been issued to all [redacted] Division [redacted]

Target Implementation Date: 06/30/2025

Responsible Official:
[redacted] Manager

Finding #5: **Protection from Environmental Hazards**
The Postal Service did not always implement the necessary controls to protect [redacted] from potential harm that could be caused by environmental factors. [redacted] can be protected from environmental hazards through a variety of methods, including heating, ventilation, and air conditioning (HVAC) systems,[41] undamaged roofing, uninterruptable power supplies[42] with surge protection, and backup generators. However, we found deficiencies with these systems.



<u>**Recommendation 9:**</u>
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] [redacted] implement controls to verify routine maintenance is performed on air conditioning units at the [redacted]

<u>Management Response/Action Plan:</u>
Management **disagrees** with this recommendation.

- HVAC routine maintenance is maintained by a contract and is verified by local maintenance.

- Numerous actions with FSSP established procedures have been taken to improve the HVAC systems in [redacted] going back to 2023 with tempcooling being installed in the summers of 2023 and 2024 to protect assets/[redacted] while repairs were being evaluated and scheduled with Facilities.

- Tickets sent to FSSP; all HVAC issues are sent to facilities. Contracts have been awared and lead time to get equipment for HVAC equipment replacement. (Need to show the timeline in an email with the current status.)

<u>Target Implementation Date</u>: N/A

<u>Responsible Official:</u>
N/A

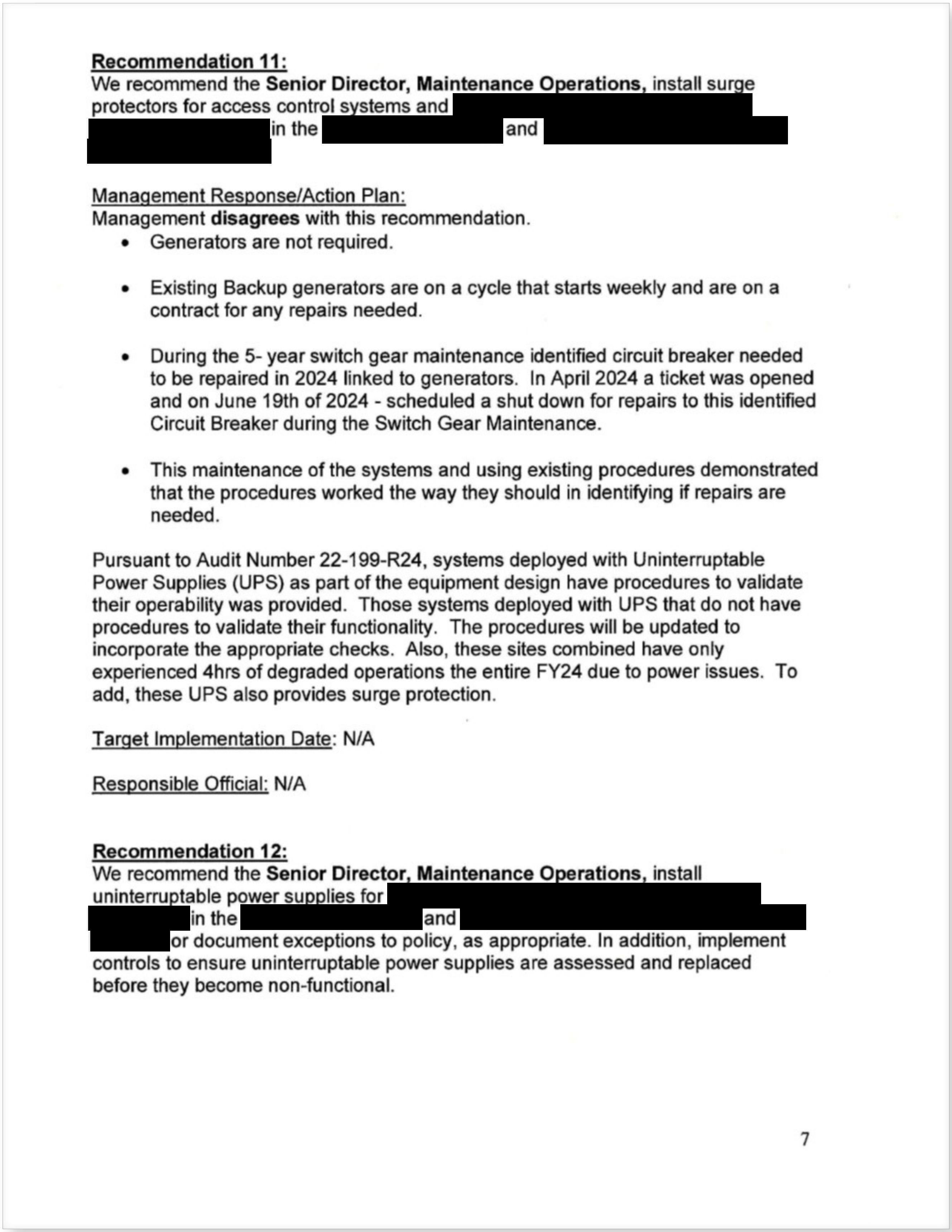
<u>**Recommendation 10:**</u>
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] [redacted] complete planned replacement of air conditioning units and roof at the [redacted]

<u>Management Response/Action Plan:</u>
Management **disagrees** with this recommendation.

- Process followed using FSSP procedure to initiate review of HVAC system with contract awarded for replacement waiting on parts.

<u>Target Implementation Date</u>: N/A

<u>Responsible Official:</u> N/A



Recommendation 11:
We recommend the **Senior Director, Maintenance Operations,** install surge protectors for access control systems and [redacted] in the [redacted] and [redacted]

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

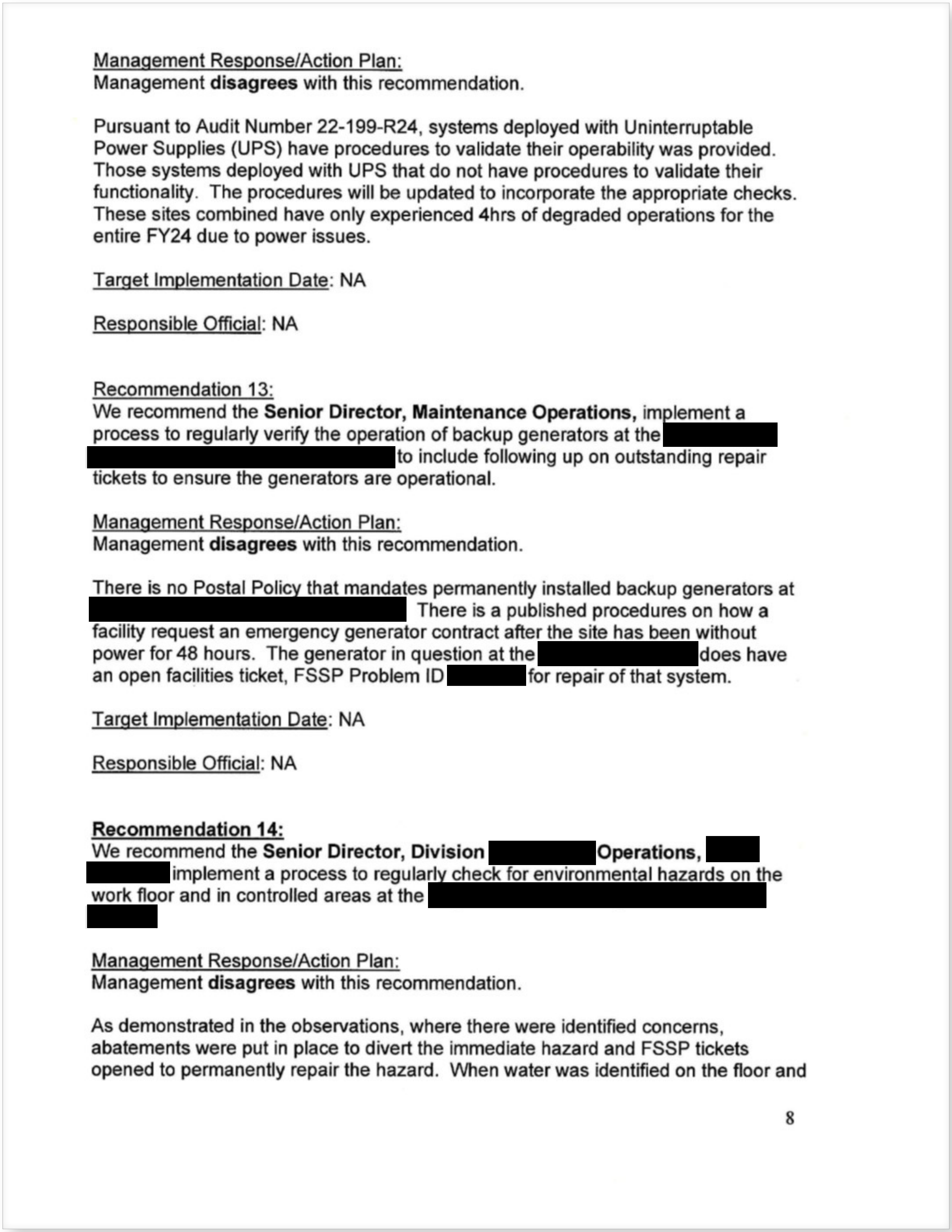
- Generators are not required.
- Existing Backup generators are on a cycle that starts weekly and are on a contract for any repairs needed.
- During the 5- year switch gear maintenance identified circuit breaker needed to be repaired in 2024 linked to generators. In April 2024 a ticket was opened and on June 19th of 2024 - scheduled a shut down for repairs to this identified Circuit Breaker during the Switch Gear Maintenance.
- This maintenance of the systems and using existing procedures demonstrated that the procedures worked the way they should in identifying if repairs are needed.

Pursuant to Audit Number 22-199-R24, systems deployed with Uninterruptable Power Supplies (UPS) as part of the equipment design have procedures to validate their operability was provided. Those systems deployed with UPS that do not have procedures to validate their functionality. The procedures will be updated to incorporate the appropriate checks. Also, these sites combined have only experienced 4hrs of degraded operations the entire FY24 due to power issues. To add, these UPS also provides surge protection.

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 12:
We recommend the **Senior Director, Maintenance Operations,** install uninterruptable power supplies for [redacted] in the [redacted] and [redacted] or document exceptions to policy, as appropriate. In addition, implement controls to ensure uninterruptable power supplies are assessed and replaced before they become non-functional.



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

Pursuant to Audit Number 22-199-R24, systems deployed with Uninterruptable Power Supplies (UPS) have procedures to validate their operability was provided. Those systems deployed with UPS that do not have procedures to validate their functionality. The procedures will be updated to incorporate the appropriate checks. These sites combined have only experienced 4hrs of degraded operations for the entire FY24 due to power issues.

Target Implementation Date: NA

Responsible Official: NA

Recommendation 13:
We recommend the **Senior Director, Maintenance Operations,** implement a process to regularly verify the operation of backup generators at the [redacted] to include following up on outstanding repair tickets to ensure the generators are operational.

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

There is no Postal Policy that mandates permanently installed backup generators at [redacted] There is a published procedures on how a facility request an emergency generator contract after the site has been without power for 48 hours. The generator in question at the [redacted] does have an open facilities ticket, FSSP Problem ID [redacted] for repair of that system.

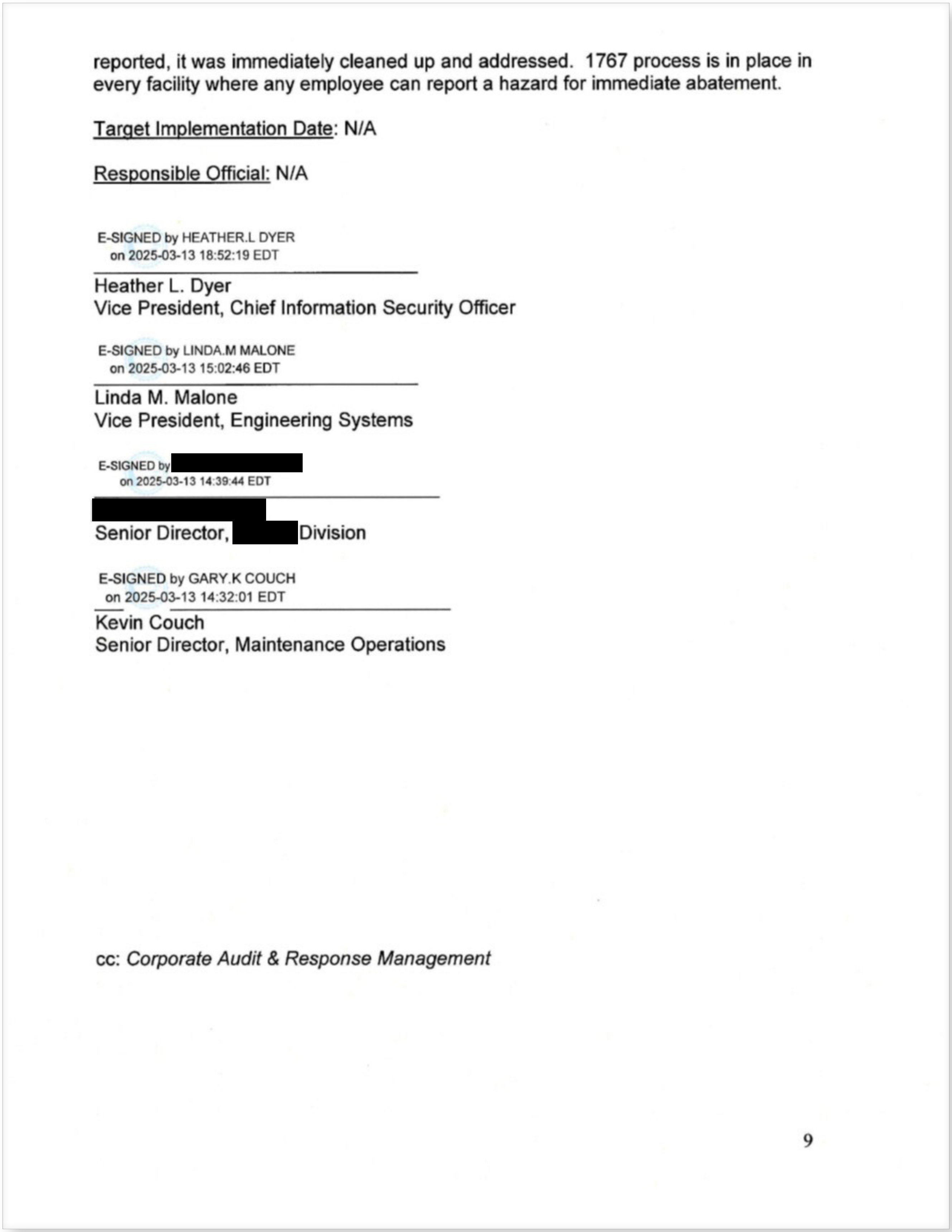
Target Implementation Date: NA

Responsible Official: NA

Recommendation 14:
We recommend the **Senior Director, Division** [redacted] **Operations,** [redacted] implement a process to regularly check for environmental hazards on the work floor and in controlled areas at the [redacted]

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

As demonstrated in the observations, where there were identified concerns, abatements were put in place to divert the immediate hazard and FSSP tickets opened to permanently repair the hazard. When water was identified on the floor and



reported, it was immediately cleaned up and addressed. 1767 process is in place in every facility where any employee can report a hazard for immediate abatement.

Target Implementation Date: N/A

Responsible Official: N/A

E-SIGNED by HEATHER.L DYER
on 2025-03-13 18:52:19 EDT

Heather L. Dyer
Vice President, Chief Information Security Officer

E-SIGNED by LINDA.M MALONE
on 2025-03-13 15:02:46 EDT

Linda M. Malone
Vice President, Engineering Systems

E-SIGNED by [redacted]
on 2025-03-13 14:39:44 EDT

[redacted]
Senior Director, [redacted] Division

E-SIGNED by GARY.K COUCH
on 2025-03-13 14:32:01 EDT

Kevin Couch
Senior Director, Maintenance Operations

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

This document contains sensitive information that has been redacted for public release. These redactions were coordinated with USPS and agreed to by the OIG.