Legacy Systems at the U.S. Postal Service

AUDIT REPORT

Report Number 24-010-R24 | June 3, 2024

Table of Contents

Highlights

Background

The U.S. Postal Service performs a variety of operations, dependent on its vast information technology infrastructure. This infrastructure encompasses 761 systems that the Postal Service strives to maintain and secure from network attacks. In support of the Delivering for America plan, the Postal Service plans to invest in modernizing and enhancing cybersecurity technologies, but it is still managing outdated computing system hardware and software (legacy systems). At least [redacted] of the Postal Service's 761 systems were considered legacy as of December 2023. Secure systems are imperative to uninterrupted operations and protecting Postal Service data.

What We Did

Our objective was to assess legacy systems at the Postal Service and address Postal Service's mitigation of risks for these systems. For this audit, we reviewed Postal Service's 1) legacy system inventory and processes for managing legacy systems; 2) guidance for risk mitigation and compliance with vulnerability remediation; and 3) inventory of systems using unsupported operating systems.

What We Found

We found the Postal Service did not effectively manage its legacy systems and associated risks. Specifically, the Postal Service had documented risks related to legacy systems for over [redacted]. Additionally, prior audits identified issues with the Postal Service's risk management process and highlighted risks associated with some legacy systems. During this audit, the Corporate Information Security Office documented a plan to mitigate the risks in the Postal Service environment; however, the plan did not include completion dates. The ineffective management of legacy systems occurred because the Postal Service did not: sufficiently define legacy systems; identify all systems using legacy operating systems; and have provisions for managing the life cycle of operating systems. Unmanaged legacy systems leave the Postal Service's systems and data vulnerable to known security exploits, which could allow attackers access to sensitive data or other systems.

Recommendations and Management Comments

We made two recommendations to address managing and mitigating risks associated with legacy systems. Postal Service's management disagreed with the recommendations. Management's comments and our evaluation are at the end of the finding and recommendations. The Office of Inspector General considers management's comments nonresponsive and will work with management through the formal audit resolution process.
See Appendix B for management's comments in their entirety.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 3, 2024

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

WILLIAM E. KOETZ,
VICE PRESIDENT, NETWORK & COMPUTE TECHNOLOGY

LINDA M. MALONE,
VICE PRESIDENT, ENGINEERING SYSTEMS

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

SUBJECT: Audit Report – Legacy Systems at the U.S. Postal Service
(Report Number 24-010-R24)

This report presents the results of our audit of Legacy Systems at the U.S. Postal Service.

All recommendations require U.S. Postal Service Office of Inspector General (OIG) concurrence before closure. Recommendations 1 and 2 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. Consequently, the OIG requests written confirmation when corrective actions are completed. See Appendix B for management's comments in their entirety

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Service's legacy systems (Project Number 24-010). Our objective was to assess legacy systems at the Postal Service and address the Postal Service's mitigation of risks for these systems. See Appendix A for additional information about this audit.

Background

The Postal Service owns the third largest information technology infrastructure in the world that, as of December 2023, included 761 information systems. All Postal Service operations — including mail processing, human resources, and finance — rely on this infrastructure. Customers also rely on this infrastructure to provide services essential to the reliable delivery of mail, such as change-of-address requests and Post Office Box payments. However, this large infrastructure leaves the Postal Service vulnerable to cyberattacks. Because of this, an effective risk management program is imperative to mitigate potential threats that could impact the confidentiality, integrity, and availability of these systems. In support of the Delivering for America plan, the Postal Service plans to invest in enhanced cybersecurity technologies, which is critical for the Postal Service to deliver excellent, secure, and cost-efficient services in a financially sustainable manner.

Definition of Legacy Systems

The Corporate Information Security Office (CISO) defines legacy systems as those systems that are using end-of-life[1] (EOL) operating systems.[2] As of December 2023, at least [redacted] of the Postal Service's 761 information systems fit this definition of legacy systems. See Table 1 for examples of Postal Service systems with EOL operating systems.

Table 1. Examples of Postal Service Systems With Outdated Operating Systems

System	Description
[redacted]	[redacted]

Source: Postal Service Enterprise Information Repository as of March 2024.

1 Software that is unsupported and no longer receiving security updates from the vendor.
2 Provides an environment in which a user can execute applications. For example, [redacted] operating system.

Roles and Responsibilities

USPS Handbook AS-805, Information Security, dated September 2022, sets policy and defines roles and responsibilities for Information Security. CISO is responsible for setting the strategic and operational direction of the Postal Service's information security programs, communicating and enforcing compliance throughout the Postal Service, and protecting the proprietary data and systems of the enterprise. CISO is also responsible for informing executive leadership of new and emerging cybersecurity threats, issues, and potential risks including any risks related to legacy systems.

CISO relies on its Vulnerability Remediation Management program[3] to identify and manage risks associated with legacy systems. Specifically, the CISO identifies vulnerabilities using methods such as automated or manual vulnerability scans[4] and penetration testing.[5] Then they aggregate, analyze, and prioritize these vulnerabilities before using specific criteria to prioritize risks. Finally, system owners must decide to eliminate, mitigate, or accept and monitor each risk.

3 Process for prioritizing discovered vulnerabilities, identifying vulnerable system owners and remediation resources, guiding stakeholders through the remediation process, reporting remediation statuses and changes to campaign scope, and verifying the results of remediation efforts.
4 Vulnerability scans are required to systematically examine an information system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
5 A test methodology in which assessors attempt to circumvent or defeat the security features of an information system.

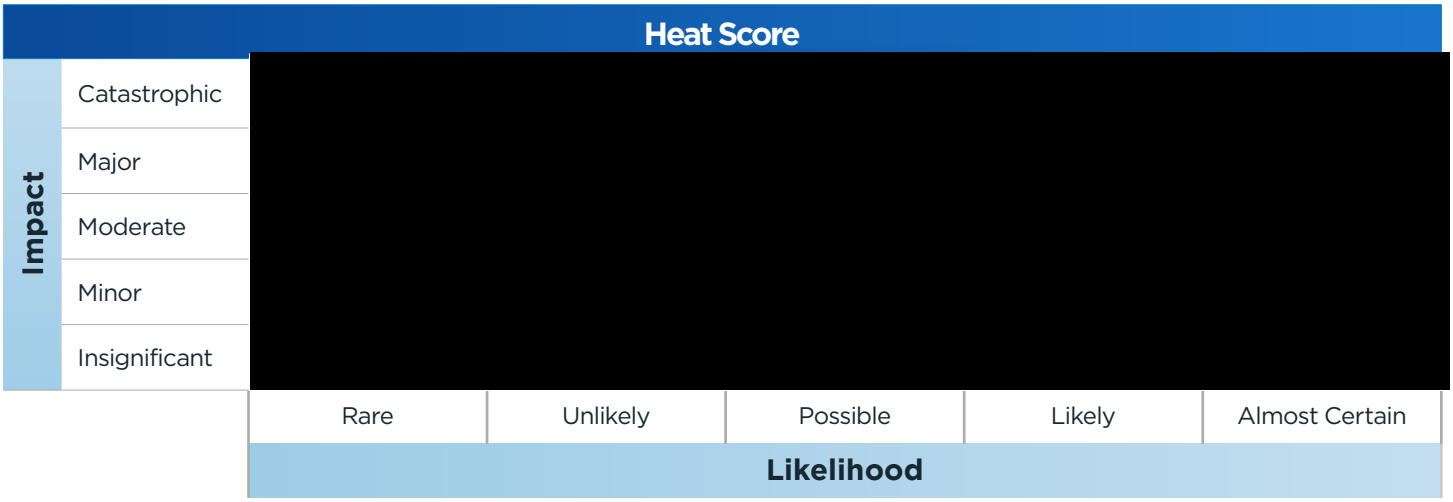
Finding: Legacy System Management

We found the Postal Service did not properly manage its legacy systems and associated risks. Specifically, CISO tracked legacy operating systems as enterprise risks for [redacted] but hasn't completed actions to address these issues. The enterprise risks are rated a heat score of [redacted], which is based on the deficiencies' impact level and possibility of occurrence specified in the Cyber Risk Heat Score matrix (see Table 2). Specifically, the impact level was determined to be [redacted] related to legacy operating systems.

CISO provided Risk Summary Reports showing that they have been tracking EOL operating systems for [redacted] as an enterprise risk since [redacted] and since [redacted], for servers on the rest of the Postal Service environment (i.e., [redacted] servers). The latter report stated that [redacted] They further stated that the risk could result in [redacted] The CISO stated they implemented security controls to isolate and reduce risk related to legacy systems. However, they did not provide support for which systems were isolated, when these controls were implemented, or enough detail to verify whether these controls were effective in mitigating legacy system risks.

A January 5, 2024, update to the Risk Summary Report for [redacted] servers contains the following recommendations: 1) create plans to upgrade or decommission all legacy operating systems within the USPS enterprise, 2) execute the plans to upgrade or decommission all legacy operating system servers that exist in the environment, 3) assign a champion to manage lifecycle management for operating systems across the enterprise, 4) establish a governing process that oversees all operating systems and tracks them throughout the entire lifecycle, and 5) establish a reporting cadence and thresholds to keep leaders informed to enable decision-making. However, the Postal Service only identified a completion date to upgrade the legacy operating systems in the [redacted]

Table 2. Cyber Risk Heat Score Matrix



Note: The black box indicates the heat score for the legacy systems enterprise risks.
Source: Postal Service Cyber Risk Management Program.

Prior U.S. Postal Service Office of Inspector General (OIG) work also identified issues with CISO's risk management process and management of legacy systems. In 2022, an OIG Management Alert[6] found that CISO did not always ensure that security control deficiencies were properly mitigated within established timelines. In that alert, we recommended the Postal Service implement a process to ensure security control deficiencies were remediated. As a result, CISO adjusted its documented risk assessment process to include a review of risks that were not addressed within established completion dates.

In another recent audit,[7] we found legacy code in the Postal Service's payroll system resulted in increased timelines for processing retroactive pay. That report noted that the Postal Service intends to acquire a new system to fully automate, integrate, and streamline the payroll process.

Finally, another audit[8] found that some equipment on the [redacted] was too fragile to scan using traditional scanning and that some [redacted] could not use secure configurations without impacting critical functionality of the equipment due to their age. We recommended that the Postal Service develop a plan to address all critical and high vulnerabilities and document any exceptions. We also recommended conducting recurring scan and remediation procedures for all [redacted] and documenting exceptions. The Postal Service stated that it is working towards full implementation of these recommendations by September 30, 2026, and September 30, 2024, respectively.

The Postal Service did not properly manage its legacy systems because it did not sufficiently define legacy systems, did not identify all systems that were using legacy operating systems, and did not effectively manage the life cycle of operating systems; all of which are outlined below.

Legacy Systems Definition

CISO's definition of legacy systems did not align with industry best practices. Specifically, CISO limited the definition of legacy systems to only those using EOL operating systems. However, best practices[9] consider more than operating systems for defining legacy systems. For example, a Government Accountability Office[10] audit stated that older languages, unsupported hardware and software, and known security vulnerabilities should all be considered when defining legacy systems.

Legacy System Identification

Additionally, CISO does not have a complete inventory of all legacy systems in the Postal Service network. For example, compounding the effect of its limited definition of legacy systems, we identified discrepancies in the information used to track EOL operating systems. We reviewed a list of 3,245 host names[11] provided by CISO identifying devices using an EOL operating system and found [redacted] did not specify which Postal Service system the host names were assigned to. On January 4, 2024, CISO

6 *Mitigation of Findings Identified During Assessment and Authorization Process* (Report Number 22-063-R22, dated May 5, 2022).
7 *Processing of Retroactive Pay* (Report Number 23-060-R24, dated October 24 ,2023).
8 *Site Technical Assessment Review (STAR)* (Report Number 22-199-R24, dated January 25, 2024).
9 *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers* (National Institute of Standards and Technology (NIST) Special Publication 800-70 Revision 4, dated, February 2018).
10 *Agencies Need to Continue Addressing Critical Legacy Systems* (Report Number GAO-23-106821 dated, May 10, 2023).
11 A unique name for a computer or a device on a network.

agreed this is an issue and reported they are working to identify these systems.

The list of EOL operating systems CISO provided was also incomplete. On March 21, 2024, CISO confirmed that three systems containing [redacted] servers were using [redacted], which is an EOL operating system. These were not included in the list that CISO provided in December 2023.

Postal Service policy[12] requires all operating systems to have proper controls in place and for management to maintain risk mitigation plans for any operating systems that are not supported by the vendor. However, when the operating system is not associated with a system, no one is responsible for managing risks.

Operating Systems Life Cycle Management

Finally, the Postal Service did not effectively manage the life cycle of operating systems. Specifically, CISO monitored and notified system owners of the risks of EOL operating systems but did not enforce mitigation of identified risks. System owners did not always take action to mitigate the risks because in some cases they were not aware of the most recent vulnerability data and in other cases they provided inaccurate completion dates.

[redacted] systems we sampled had outstanding critical vulnerabilities identified by the most recent continuous monitoring scan [redacted] which is an EOL operating system. Additionally, [redacted] was using EOL operating systems impacted by multiple high vulnerabilities, which could allow attackers [redacted]

CISO policy[14] requires that all critical vulnerabilities be remediated within 30 days and all high vulnerabilities be remediated within 60 days of the vendor-released security updates.[15] According to NIST,[16] security updates are important to help prevent compromises, data breaches, operational disruptions, and other adverse events.

According to the White House's National Cybersecurity Strategy, the federal government must replace or update systems that are not defensible against sophisticated cyber threats.[17] Although this does not apply to the Postal Service as a requirement, it can be considered a best practice. The Government Accountability Office found that the consequences of not updating legacy systems contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs.[18]

Impacts of Ineffective Legacy System Management

As a result of these issues, known critical and high vulnerabilities associated with legacy systems have been left unaddressed. Without a complete inventory of legacy systems and mitigation of the associated risks, the Postal Service's systems and data are vulnerable to known security exploits, which could allow attackers to access sensitive data or other systems on the network. According to a risk summary report from CISO, [redacted] of legacy operating systems in the Postal Service environment are [redacted], which increases the likelihood of a cyberattack. A cyberattack in the [redacted] could disrupt mail operations and impact the Postal Service's reputation. In addition, the Postal Service may not be able to prevent similar problems from occurring when other operating systems become unsupported in the future.

> "As a result of these issues, known critical and high vulnerabilities associated with legacy systems have been left unaddressed."

12 Handbook AS-805, *Information Security*, September 2022.
13 [redacted]
14 [redacted]
15 Security updates are patches or modifications made to software, operating systems, applications, or firmware to address vulnerabilities and improve the overall security of the system.
16 NIST SP 800-40r4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, dated April 2022.
17 National Cybersecurity Strategy, Strategic Objective 1.5: Modernize Federal Defenses, dated March 2023.
18 Agencies Need to Continue Addressing Critical Legacy Systems (Report Number GAO-23-106821, dated May 10, 2023).

Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, create a comprehensive plan to manage legacy systems to include defining legacy systems according to best practices, identifying all legacy systems, and developing a plan of action and milestones to enforce timely mitigation of identified risks related to legacy systems.

Recommendation #2

We recommend the **Vice President, Network and Compute Technology** and **Vice President, Engineering Systems**, mitigate identified risks for all legacy systems, develop a plan of action and milestones to enforce timely mitigation of identified risks related to legacy systems and report the status of mitigations as defined in the Corporate Information Security Office's plan of action and milestones to the Corporate Information Security Office.

Postal Service Response

The Postal Service disagreed with this finding and both recommendations.

Regarding the finding, management stated that they 1) track legacy systems and created a consolidated list of legacy operating systems at the server level, 2) require all information resources to have proper controls associated with risk mitigation, and 3) identify operating systems not associated with a system and assign controls based on that system's sensitivity and business criticality.

Regarding recommendation 1, management stated that the Postal Service has a risk mitigation plan for legacy operating systems. Also, management stated that the OIG did not provide additional information on how an updated definition of legacy systems would impact the Postal Service's risk landscape, nor how it would affect the business objectives of the Postal Service. Further, management stated that risks are balanced with compensating controls and business needs.

Regarding recommendation 2, management stated legacy system owners work in conjunction with the CISO to mitigate identified risks for systems, develop a plan of action and milestones to enforce timely mitigation of identified risks related to systems, and report the status of mitigations weekly.

OIG Evaluation

The OIG considers management's comments non-responsive to recommendations 1 and 2.

Regarding the finding, management did not provide documentation to support statements made in their comments.

Regarding recommendation 1, OIG reviewed risk mitigation plans for legacy operating systems and found that the planned start dates for mitigating the identified risks had already passed for [redacted] legacy operating systems. Further, while management provided a risk assessment document, included in their response, that addressed [redacted] risks, this only applies to a portion of the recommendation.

Regarding recommendation 2, management provided two risk management plans, included in their response, for select legacy operating systems. However, both plans did not have milestone dates to address vulnerabilities and were not approved by management. Further, management did not provide support for weekly mitigation status updates.

We view management's disagreement with the recommendations as unresolved and will work with management through the formal audit resolution process.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our scope included the Postal Service's processes to manage legacy systems risk and the implementation of those processes.

To accomplish our objective, we reviewed Postal Service's Vulnerability Analysis and Resolution Program. In addition, the audit team:

- Evaluated policies and practices for managing legacy systems for alignment with accepted frameworks and best practices.
- Selected a judgmental sample of 10 Postal Service systems with EOL operating systems to review security scans and review identified vulnerabilities.
- Analyzed prior audit findings and recommendations for trends related to root causes.

We conducted this performance audit from December 2023 through June 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 April 23, 2024, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the legacy systems 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, 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 applying logical tests to data such as checking for blank values. 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
Mitigation of Findings Identified During Assessment and Authorization Process	Notify Postal Service management of risks associated with security control deficiencies identified during the Assessment & Authorization (A&A) process that have not been mitigated.	22-063-R22	May 5, 2022	N/A
State of Cybersecurity	Assess the effectiveness of the Postal Service's state of cybersecurity.	21-205-R22	August 15, 2022	N/A
Processing of Retroactive Pay	Assess the United States Postal Service's processes and systems over retroactive pay.	23-060-R24	October 24, 2023	N/A
Site Technical Assessment Review	Determine whether the Postal Service established and implemented adequate controls at selected [redacted]	22-199-R24	January 25, 2024	N/A

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

May 20, 2024

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Legacy Systems at the U.S. Postal Service (24-010-DRAFT)

Thank you for providing the Postal Service an opportunity to review and comment on the findings contained in the draft audit report titled: *Legacy Systems at the U.S. Postal Service.*

Finding:

"We [OIG] found the Postal Service did not properly manage its legacy systems and associated risks. Specifically, CISO tracked legacy operating systems as enterprise risks for more than [redacted] but hasn't completed actions to address these issues."

CISO does not agree with the finding, citing the following:

- The Postal Service was tracking legacy operating systems through our Risk Register.
- The Postal Service has created a consolidated list of legacy operating systems tracked at the individual server level, which is now in place and was in place during the audit.

Finding:

"Postal Service policy requires all operating systems to have proper controls in place and for management to maintain risk mitigation plans for any operating systems that are not supported by the vendor. However, when the operating system is not associated with a system, no one is responsible for managing risks."

CISO does not agree with the finding:

- The Postal Service requires all information systems to have proper controls associated with risk mitigation. If an operating system is not associated with a system, the Postal Service identifies the correct system it is associated with and assigns to controls based on that system's sensitivity and business criticality.

Following are our comments on each of the two recommendations:

Recommendation 1: We recommend the Vice President, Chief Information Security Officer, create a comprehensive plan to manage legacy systems to include defining legacy systems according to best practices and identifying all legacy systems.

Management Response/Action Plan:
Management disagrees with this recommendation. The Postal Service has developed a risk mitigation plan for these legacy operating systems, which are scoped to the 21,672 servers identified by the Postal Service as legacy operating systems.

The cybersecurity risk of the operating systems must be continuously balanced with the business objectives of the Postal Service. Owing to that, the supporting dates for remediation of Legacy OS, especially in the [redacted] were developed with consideration of the compensating controls as well as the business objectives of the Postal Service.

The Postal Service does not agree with the recommendation to update its definition of Legacy Systems. The OIG did not provide additional information on how an updated definition would impact the Postal Service's risk landscape, nor how it would affect the business objectives of the Postal Service. The Postal Service agrees with its definition of a Legacy System based on the risk to the organization.

Additional information pertaining to the risk plans for legacy systems in the [redacted] are attached below along with the cybersecurity risk assessment pertaining to the implementation of the [redacted] as a compensating controls.

[redacted]

Target Implementation Date: N/A

Responsible Official: N/A

Recommendation 2: We recommend the Vice President, Network and Compute Technology and Vice President, Engineering Systems, mitigate identified risks for all legacy systems, develop a plan of action and milestones to enforce timely mitigation of identified risks related to legacy systems and report the status of mitigations as defined in the Corporate Information Security Office's plan of action and milestones to the Corporate Information Security Office.

Management Response/Action Plan:
Management disagrees with this recommendation. Network and Infrastructure Technology and Engineering Systems work today in conjunction with the Chief

Information Security Office to mitigate identified risks for systems, develop a plan of action and milestones to enforce timely mitigation of identified risks related to systems and report the status of mitigations weekly as outlined in the response to Recommendation 1.

Target Implementation Date: N/A

Responsible Official: N/A

E-SIGNED by HEATHER.L DYER
on 2024-05-20 15:01:04 EDT

Heather Dyer
Vice President, Chief Information Security Officer

E-SIGNED by WILLIAM.E KOETZ
on 2024-05-20 14:57:07 EDT

William Koetz
Vice President, Network and Compute Technology

E-SIGNED by LINDA.M MALONE
on 2024-05-20 16:37:10 EDT

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