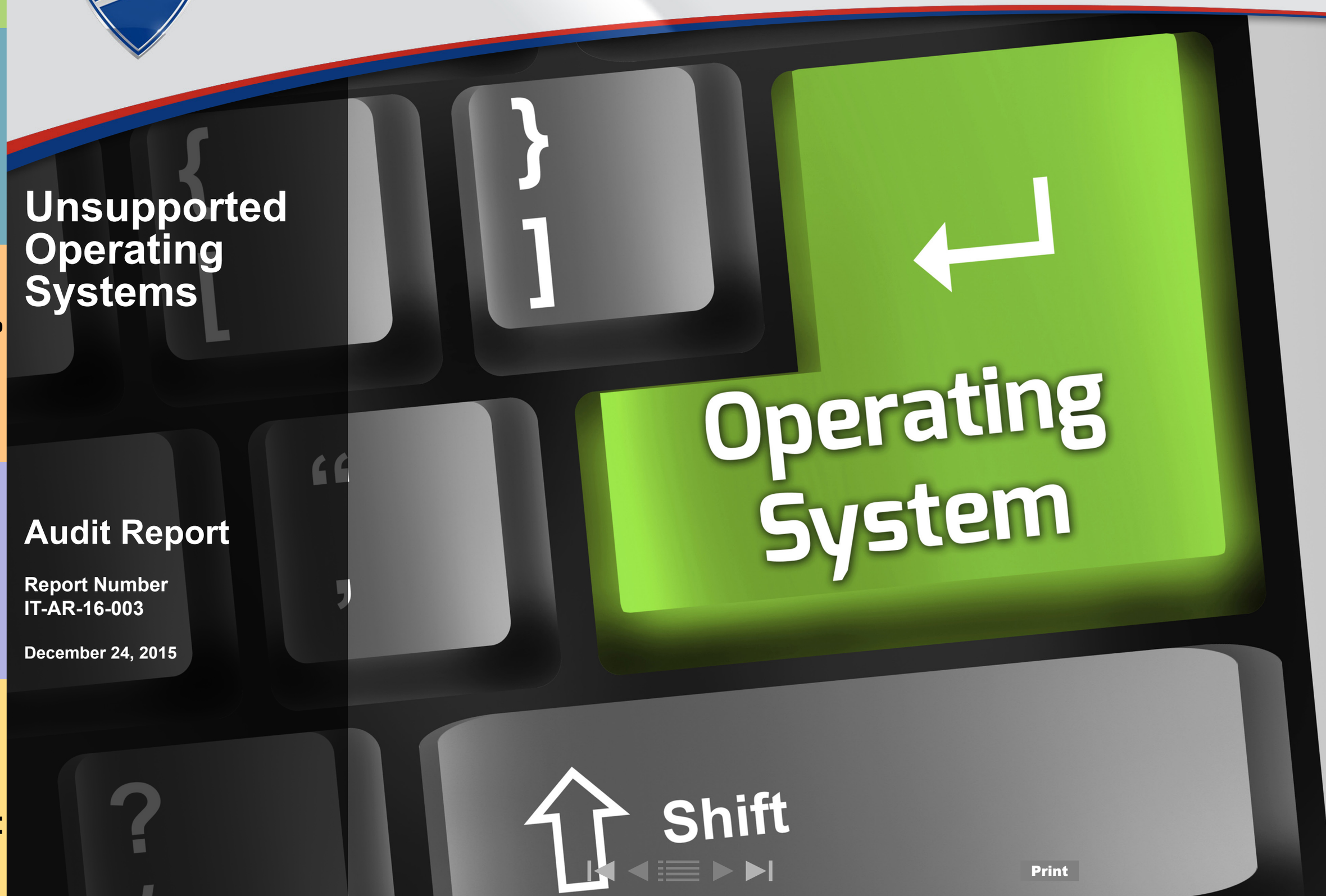
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Unsupported Operating Systems

Audit Report

Report Number
IT-AR-16-003

December 24, 2015



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Postal Service security policy does not provide detailed guidance for managing OS such as tracking vendor end-of-support dates, identifying risks associated with running outdated OS, and developing strategies for migrating to another OS when vendor support ends.

Background

Operating systems (OS) consist of software that manages the memory, processes, and hardware of a computer system. Through their lifecycle, OS require vendor support in the form of upgrades, fixes, and new versions. An OS lifecycle begins upon its release and ends when the vendor support ends. When the OS lifecycle ends, it becomes an unsupported OS. Vendors publish end-of-support dates on their websites to inform the public when their OS support will end.

Vendors may charge fees to extend support or provide additional capabilities beyond the original end date. Users can still run the OS without purchasing this additional support; however, it increases risk to the system. U.S. Postal Service Handbook AS-805, *Information Security,* allows the use of unsupported software with Information Technology management's approval.

Our objective was to determine how the Postal Service manages unsupported OS, identify associated risks, and review management's actions to mitigate or accept those risks.

What The OIG Found

Handbook AS-805 does not provide detailed guidance for managing OS such as tracking vendor end-of-support dates, identifying risks associated with running outdated OS, and developing strategies for migrating to another OS when vendor support ends. As a result, management does not have an inventory of OS and is not tracking and maintaining documentation associated with the risk of running unsupported OS.

We determined the Postal Service is currently using at least [redacted] unsupported OS versions on almost [redacted] devices, such as servers and desktop computers. In addition, they are using at least [redacted] unsupported OS versions on about [redacted] mail-processing computer systems.

This occurred because Handbook AS-805 is not aligned with best practices, which recommend organizations assign a single group to manage all software on their network, including monitoring vendor end-of-support dates and developing strategies for replacing unsupported software. Without adequate management of unsupported OS, the Postal Service network is at an increased risk of unauthorized access, disclosure, and modification of sensitive customer data.

What The OIG Recommended

We recommended management revise Handbook AS-805 to provide detailed guidance for managing OS such as assigning a single group the responsibility for managing unsupported OS, tracking vendor end-of-support dates, identifying risks associated with running unsupported OS, and developing strategies for moving to another OS when vendor support ends. We also recommended management develop a current inventory of unsupported OS and either document the acceptance of the risk of continued usage or migrate to a supported OS.

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

THE OIG DETERMINED

CLICK THE ICONS BELOW TO REVEAL THE FINDINGS

The Postal Service is currently using at least  unsupported OS versions on almost  devices, such as servers and desktop computers. In addition, they are using at least  unsupported OS versions on about  mail processing computer systems.

RESET BUTTONS

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 24, 2015

MEMORANDUM FOR: GREGORY S. CRABB
ACTING CHIEF INFORMATION OFFICER AND
EXECUTIVE VICE PRESIDENT

BRIAN W. CARNELL
ACTING VICE PRESIDENT, INFORMATION TECHNOLOGY

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktop

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – Unsupported Operating Systems
(Report Number IT-AR-16-003)

This report presents the results of our audit of the U.S. Postal Service's Unsupported Operating Systems (Project Number 15TG029IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean Balduff, acting director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

We determined the Postal Service is currently using at least [redacted] unsupported OS versions on almost [redacted] devices, and using at least [redacted] unsupported OS versions on about [redacted] mail processing computer systems.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's unsupported operating systems (OS) (Project Number 15TG029IT000). Our objective was to determine how the Postal Service manages unsupported OS, identify associated risks, and review management's actions to mitigate or accept those risks. See Appendix A for additional information about this audit.

OS consist of software that manages the memory, processes, and hardware of a computer system. They handle input and output, send messages to each application, and manage the sharing of internal memory. All Postal Service information resources must use an approved OS configured to comply with security requirements to ensure the integrity of the OS environment. Through their lifecycle, OS require vendor support in the form of upgrades, fixes, and new versions. An OS has a lifecycle, which begins upon release and ends when vendor support, such as software updates or online technical assistance, ends.

OS vendors publish dates on their websites to inform users of vendor end-of-support dates and may charge fees for extended support beyond the expiration date. Knowing when the OS lifecycle ends could help the Postal Service make informed decisions about when to upgrade the OS software and avoid extended support costs. Users may continue to run unsupported OS without the latest software updates; however, users will no longer receive security updates that can help protect Postal Service information resources from the high-risk vulnerabilities[1] associated with running unsupported OS on the network.

Summary

Postal Service security policy[2] does not provide detailed guidance for managing OS such as tracking vendor end-of-support dates, identifying risks associated with running outdated OS, and developing strategies for migrating to another OS when vendor support ends. As a result, management does not have an inventory of OS and is not tracking and maintaining documentation associated with the risk of running unsupported OS.

We determined the Postal Service is currently using at least [redacted] unsupported OS versions on almost [redacted] devices, such as servers and desktop computers. In addition, they are using at least [redacted] unsupported OS versions on about [redacted] mail processing computer systems. See Appendix B for additional information on the unsupported OS we identified.

This occurred because Handbook AS-805 does not align with best practices,[3] which recommend organizations assign a single group to manage all software on their network, including monitoring vendor end-of-support dates and developing strategies for replacing unsupported software. Without adequate management of unsupported OS, the Postal Service network is at an increased risk of unauthorized access, disclosure, and modification of sensitive customer data.

Policy Requirements for Operating Systems Management

Handbook AS-805 does not provide detailed guidance for managing OS such as tracking vendor end-of-support dates, identifying risks associated with running outdated OS, and developing strategies for migrating to another OS when vendor support ends. As a result, management does not have an inventory of OS and is not tracking and maintaining documentation associated with the risk of running unsupported OS.

1 A flaw in code or design that creates a potential point-of-security compromise for a computer network that would allow an intruder to gain access.
2 Handbook AS-805, *Information Security*, dated May 2015.
3 The Center for Internet Security Critical Security Controls (CSC) for Effective Cyber Defense, Version 6.0, Section CSC 2: Inventory of Authorized and Unauthorized Software, CSC 2.3, dated October 15, 2015 and SANS Institute: CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.

Maintaining an Operating System Inventory

The Postal Service does not have an enterprise-wide inventory of OS including devices associated with the OS and vendor end-of-support dates. The Information Technology (IT) group[4] provided data extracted from the Configuration Management Database (CMDB)[5] for the IT-managed network and the Engineering Systems group provided a manual listing[6] of OS versions for their network. However, the data provided were not a complete inventory of OS versions enterprise-wide and did not include vendor end-of-support dates. For example, we found that the [redacted] group is running [redacted] unsupported OS versions[7] on [redacted] devices, which were not included in the data IT provided. Based on the information provided by management, we determined the Postal Service is currently using at least [redacted] unsupported OS versions on almost [redacted] devices, such as servers and desktop computers. In addition, they are using at least [redacted] unsupported OS versions on about [redacted] mail-processing computer systems. See Appendix B for a listing of the unsupported OS we identified.

Handbook AS-805[8] requires executive sponsors to maintain an accurate inventory of information resources. In addition, best practices[9] recommend organizations actively manage all OS software on the network to include assigning responsibility for establishing a software inventory and tracking relevant vendor support information.

Risk Acceptance Documentation

Management is not appropriately managing the risk of running unsupported OS versions on the Postal Service network in accordance with established risk acceptance processes. They are not tracking and maintaining documentation regarding risk acceptance as required by Handbook AS-805[10] or developing strategies for moving to another OS when vendor support ends. For example, the [redacted] group is running two unsupported OS versions and they are not maintaining the required risk acceptance documentation. These issues occurred because Handbook AS-805 does not align with best practices,[11] which recommend organizations assign a single group to manage all software on their network, including monitoring vendor end-of-support dates and developing strategies for replacing unsupported software.

The Corporate Information Security Office (CISO) is coordinating an effort to remove [redacted] devices[12] from the IT and Engineering Systems networks. This effort includes tracking devices running [redacted] coordinating with business owners to migrate from this OS version, and preparing documentation showing that management accepts any risk if it is not feasible to migrate. However, we found the CISO is not tracking other OS versions such as [redacted][13] [redacted],[14] and [redacted] and their associated devices, vulnerabilities, or vendor end-of-support dates.

---

4 This group is a part of IT Performance Achievement and its duties include managing change control and configuration management, enterprise system monitoring, and capacity and performance management.
5 The system of record for IT configuration information for IT assets.
6 The Mail Processing Equipment Subsystem Breakdown spreadsheet, which lists the OS managed by Engineering Systems.
7 The [redacted] unsupported OS are [redacted] and [redacted]
8 Handbook AS-805, Section 2-2.11, Executive Sponsors.
9 The Center for Internet Security CSC for Effective Cyber Defense, Version 6.0, Section CSC 2: Inventory of Authorized and Unauthorized Software, CSC 2.1, CSC 2.3.
10 Handbook AS-805, Section 4-3, Information Risk Management.
11 The Center for Internet Security CSC for Effective Cyber Defense, Version 6.0, Section CSC 2: Inventory of Authorized and Unauthorized Software, CSC 2.3 and SANS Institute: CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
12 Devices include computer desktops and laptops and mail processing/material handling equipment.
13 A large freeware product with many extensions and new ideas provided in a variety of versions of [redacted] by different companies, universities, and individuals.
14 A [redacted] designed to provide companies a free or very low-cost OS comparable to traditional and usually more expensive [redacted] systems.
15 Developed by [redacted] as a [redacted].

In addition, the Postal Service is working with the Department of Homeland Security (DHS) on the Continuous Diagnostics and Monitoring (CMD)[16] program, which, once implemented, should provide the Postal Service with a real-time inventory system of all information resources.

Without adequate management of unsupported operating systems, the Postal Service network is at an increased risk of unauthorized access, disclosure, and modification of sensitive customer data.

16 The CDM program is a DHS program that enhances government network security through automated control testing and progress tracking.

Recommendations

We recommend management revise Handbook AS-805 to provide detailed guidance for managing OS, develop a current inventory of unsupported OS, and either document acceptance of the risk of continued usage or migrate to a supported operating system.

We recommend the acting chief information security officer and Digital Solutions vice president:

1. Revise Handbook AS-805, *Information Security*, to provide detailed guidance for managing operating systems, such as assigning a single group responsibility for managing unsupported operating systems, tracking vendor end-of-support dates, identifying risks associated with running unsupported operating systems, and developing strategies for moving to another operating system when vendor support ends.

We recommend the acting chief information security officer and Digital Solutions vice president, in coordination with the acting vice president, Information Technology, and vice president, Engineering Systems:

2. Develop a current inventory of unsupported operating systems and either document acceptance of the risk of continued usage or migrate to a supported operating system.

Management's Comments

Management generally agreed with the findings and recommendations in the report. See Appendix C for management's comments in their entirety.

Regarding recommendation 1, management partially agreed and stated they will update guidance specific to the management of operating systems to include tracking vendor end-of-support dates, identifying risks associated with running unsupported operating systems, and developing strategies for moving to another operating system when vendor support ends. Management plans to update guidance by September 30, 2016. Management also stated they have already assigned the Chief Information Officer (CIO) oversight over all systems and does not see a need to write a new policy to cover this responsibility.

Regarding recommendation 2, management will develop a current inventory of unsupported operating systems and either document acceptance of the risk for continued use or migrate to a supported operating system by September 2017.

Evaluation of Management's Comments

The OIG considers management's comments generally responsive to the recommendations and corrective actions should resolve the issues identified in the report.

Regarding recommendation 1, CIO office management could not provide us with a complete listing of unsupported operating systems running on the Postal Service network. Specifically, assigning the responsibility for managing unsupported operating systems in accordance with the current policy follows best business practices and may have resulted in a better inventory. However, the other policy updates that management plans to implement should resolve the issues we identified.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

The IT and Engineering Systems groups manage Postal Service networks and provide OS support for their business applications and infrastructure equipment. Several types of OS reside on both the IT-managed and Engineering Systems-managed networks. For example, the IT-managed network includes [redacted][17] The Engineering Systems-managed network also includes [redacted], as well as [redacted] to support their mail processing equipment/mail handling equipment (MPE/MHE).[19]

Executive sponsors, as representatives of the vice presidents (VP) of IT and Engineering Systems, have oversight responsibility for maintaining an inventory of Postal Service information resources and coordinating hardware and software upgrades. Both the IT and Engineering Systems VPs are responsible for securing the Postal Service computing environment, which includes information resources and infrastructure, by implementing appropriate technical and operational security processes and practices that comply with Postal Service information security policies. In addition, the manager, CISO, is responsible for providing consulting support for securing the network perimeter, infrastructure, integrity controls, and asset inventory.

Objective, Scope, and Methodology

Our objective was to determine how the Postal Service manages unsupported OS, identify associated risks, and review management's actions to mitigate or accept those risks. This audit focused on unsupported OS versions residing on the IT and Engineering Systems network that had a vendor end-of-support date earlier than December 31, 2015. To accomplish our objective we:

- Researched IT and Engineering Systems policies and best practices to identify requirements for maintaining inventories of information resources, monitoring OS vendor end-of-support dates, and managing risk associated with running outdated OS.
- Interviewed CISO, IT, and Engineering Systems management and personnel to determine if they maintain an inventory of OS and obtain an understanding of how they manage unsupported OS.
- Analyzed about 667,000 records from the Postal Service's CMDB to identify the number of unique OS versions and associated devices, system platform, owners, and current applications supporting the devices on the IT-managed network.
- Obtained a partial listing of OS versions supporting the Engineering Systems-managed network.
- Researched vendor end-of-support dates for OS versions identified on the IT- and Engineering Systems-managed network.
- Interviewed selected business application owners from IT and Engineering Systems to determine why an unsupported OS version is on the network and obtain related risk documentation that supports the decision.

17 [redacted] is a distribution of the [redacted] developed for the business market. The OS supports diverse workloads in physical, virtualized, and cloud environments.
18 [redacted] operating system targets specific-use enterprise devices such as industrial controllers, communications hubs, and point-of-sale terminals; and runs disconnected from other computers.
19 MPE/MHE includes the computer systems and networks that manage, monitor, and control mail processing functions including facing, canceling, optical character reading, address lookup, bar code sorting, letter sorting, flat sorting, parcel sorting, sack sorting, mail tray transport, mail forwarding, mail weighing, electronic mail processing, and electronic monitoring.

We conducted this performance audit from June through December 2015, 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 the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective. We discussed our observations and conclusions with management on November 18, 2015, and included their comments where appropriate.

We did not assess the reliability of the computer-generated data obtained from the Postal Service's system of record used to manage IT assets. IT and Engineering Systems personnel were unable to provide an accurate inventory of the OS versions running on their networks. While the audit project did not evaluate the accuracy or completeness of the system of record, we validated any original system of record data used for the audit conclusions or appearing in the report through interviews with Postal Service personnel knowledgeable about the OS versions and the associated devices.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
U.S. Postal Service Cybersecurity Functions	IT-AR-15-008	7/17/2015	None
South Florida District Vulnerability Assessment	IT-AR-14-001	10/22/2013	None

Appendix B: Unsupported Operating System Versions

Table 1 shows the number of unsupported OS versions we identified on the IT-managed network.[20] It includes the OS platform, name, version, vendor end-of-support date,[21] and total number of devices associated with each unsupported OS version.

Table 1: Unsupported OS Versions on the IT-Managed Network

OS Count	OS Platform	OS Name	OS Version	Vendor End-of-Support Date	Number of Devices Running OS
[redacted]					

20 Table 1 and Table 2 represent the number of unsupported OS versions we identified; however, there may be additional unsupported OS on the IT and Engineering Systems-managed networks.
21 If the vendor end-of-support date ended on or before December 31, 2015, we determined the OS version is currently unsupported.
22 The CMDB data received from the IT group did not include [redacted]. The [redacted] group is currently managing this OS independent of the IT group.

OS Count	OS Platform	OS Name	OS Version	Vendor End-of-Support Date	Number of Devices Running OS
[redacted]					

Source: CMDB Data from Postal Service and U.S. Postal Service Office of Inspector General (OIG) analysis.

Table 2 shows the number of unsupported OS versions we identified on the Engineering Systems-managed network. It includes the OS platform, name, version, vendor end-of-support date, and total number of devices associated with each unsupported OS version.

Table 2: Unsupported OS Versions on the Engineering Systems-Managed Network

OS Count	OS Platform	OS Name	OS Version	Vendor End-of-Support Date	Number of Devices Running OS
[redacted]					

Source: MPE Breakdown Spreadsheet and OIG analysis.

23 The CMDB data received from the IT group did not include the version of [redacted] managed by the [redacted] group.
24 Engineering Systems confirmed they are not receiving any OS support for [redacted]. These are legacy OS versions that were released in [redacted]

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Unsupported Operating Systems (IT-AR-16-DRAFT), Project Number 15TG029IT000

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report to help improve the overall posture and capabilities of the Postal Service to defeat and otherwise mitigate cybersecurity risks.

Protecting the privacy of customer, employee, supplier and Postal Service information has been and always will be a priority for the Postal Service. USPS manages one of the largest information networks in the world and is constantly making updates and applying patches to operating systems and will continue to do so. USPS has implemented numerous security measures that provide multiple layers of protection across its entire network and information assets. The identified Unsupported Operating Systems exist within the Postal environment, and are protected by a variety of different tools and security controls to help mitigate against threats and vulnerabilities. In addition, USPS has developed and is executing an aggressive multi-phased cybersecurity improvement strategy to meet its security objectives and to further protect information and assets across the enterprise. The response to the recommendations in this report fall under the Monitoring Project, which is 1 of the 15 major project initiatives within the USPS cybersecurity improvement strategy.

One of the key activities of the Monitoring Project is to improve our capabilities to collect, record, and distribute information about USPS networks, information systems, and critical infrastructure. This includes the work USPS is doing with the Department of Homeland Security (DHS) on Continuous Diagnostics & Mitigation (CDM). The CDM toolset will allow USPS to improve its capabilities and have a real-time inventory of the systems and the operating systems (OS) that are on the USPS network. It allows USPS to evaluate the end-of-life scenarios and remediate them or document the usage risks as highlighted in the OIG report. The CDM efforts with DHS are already in progress and the initial implementation will be completed in 2016.

Management agrees with the findings identified in this report. Management would like to note that the number of devices running an unsupported OS as is documented in Table 1: Unsupported OS Version on the IT-Managed Network only represents roughly 3.6% of total devices on the IT network. This illustrates that USPS is currently running supported OS on 96%+ of total devices and will continue to make efforts to increase this number with the assistance of the DHS CDM program.

Recommendation [1]:
Revise Handbook AS-805, Information Security, to provide detailed guidance for managing operating systems, such as assigning a single group responsibility for managing unsupported operating systems, tracking vendor end-of-support dates, identifying risks associated with running unsupported operating systems, and developing strategies for moving to another operating system when vendor support ends.

Management Response/Action Plan:

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-5000
WWW.USPS.COM

Management agrees that policy guidance can be further improved in regards to management of operating systems. Currently AS-805 does include extensive guidance on management and execution of information security for the organization yet improvements can always be made. USPS will develop updated policy guidance specific to the management of operating systems to include tracking vendor end-of-support dates, identifying risks associated with running unsupported operating systems, and developing strategies for moving to another operating system when vendor support ends.

Management disagrees with the recommendation to assign a single group responsibility for managing unsupported operating systems as that has already been done within the USPS.

The USPS organization has already consolidated oversight over all systems under the Chief Information Officer (CIO) and thus we do not see a need to write policy to cover an organizational responsibility that is already in place.

Target Implementation Date:
September 30, 2016

Responsible Official:
(A) Chief Information Security Officer & Digital Solutions, Vice President

Recommendation [2]:
Develop a current inventory of unsupported operating systems and either document acceptance of the risk of continued usage or migrate to a supported operating system.

Management Response/Action Plan:
Management agrees with the intent of the recommendation and will develop a current inventory of unsupported operating systems and either document acceptance of the risk of continued usage or migrate to a supported operating system by the target implementation date.

Target Implementation Date:
Phase 1 – Inventory of all unsupported operating systems - November 30, 2016
Phase 2 – Migrate to supported operating systems or document acceptance of risk – September 30, 2017

Responsible Official:
Vice President, Engineering Systems
(A) Vice President, Information Technology
(A) Chief Information Security Officer & Digital Solutions, Vice President

Michael J. Amato
Vice President, Engineering Systems

Brian W. Carnell
(A) Vice President, Information Technology

Gregory S. Crabb
(A) Chief Information Security Officer & Digital Solutions, Vice President

cc: *Manager, Corporate Audit Response Management*

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100