Office of Inspector General | United States Postal Service

Audit Report

Controls Over Purchasing and Maintaining Information Technology Equipment

Report Number 19-017-R20 | August 17, 2020

Table of Contents

Highlights

Objective

Our objective was to determine if controls for purchasing and maintaining information technology (IT) equipment, specifically printers, webcams, and [redacted] cameras, are effective in identifying, assessing, and mitigating vulnerabilities and related cybersecurity risks to the U.S. Postal Service's IT infrastructure.

The Postal Service purchases IT equipment, such as webcams and printers, through the eBuy Plus system. As of April 2020, the Postal Service had about 73,000 printers. Of these, 63,357 are categorized as [redacted] which are maintained by local information specialists. The remaining 9,352 are categorized as managed printers because they are managed and maintained using enterprise tools by [redacted], including application of firmware updates. Firmware is a software program embedded on a device that gives instructions for how to communicate with other devices.

> *"Postal Service has about 73,000 printers, 4,512 webcams and over 11,000 [redacted] cameras on its network."*

As of November 2019, the Postal Service had 4,512 webcams to monitor customers' wait times at retail facilities. Each district controls and maintains its own webcams. The Corporate Information Security Office (CISO) scans these webcams regularly to identify security vulnerabilities and directs districts to apply appropriate firmware updates when needed.

In addition, the [redacted] cameras are used inside and on the [redacted] The Inspection Service, Facilities group, and U.S. Postal Service Office of Inspector General funded procurement and maintenance of the [redacted] cameras, including firmware updates, through the [redacted]. Although these organizations funded the [redacted] cameras, they are owned, operated, and controlled by the Postal Inspection Service. As of January 2020, there were over 11,000 [redacted] cameras connected to the Postal Service's internal network.

Our fieldwork was planned before the President of the United States issued the national emergency declaration concerning the novel coronavirus outbreak (COVID19) on March 13, 2020. The results of this audit do not reflect operational changes and/or service impacts that may have occurred as a result of the pandemic.

Findings

The Postal Service has effective controls over purchasing IT equipment; however, controls for identifying, assessing, and mitigating cybersecurity risks associated with [redacted] and [redacted] cameras are not effective.

The Postal Service did not update firmware on any [redacted] since mid-2018. In addition, the CISO did not perform vulnerability scans of most of the [redacted] and did not maintain a comprehensive list of active firmware versions to determine if an update was required.

> *"Postal Service has effective controls over purchasing IT equipment; however, controls for identifying, assessing, and mitigating cybersecurity risks associated with [redacted] and [redacted] cameras are not effective."*

Postal Service information security policy and industry standards require evaluation and application of compatible firmware updates as they are made available to mitigate vulnerabilities. Failure to apply these updates occurred because the IT group did not establish a process and assign responsibility for updating firmware versions for [redacted]. This could lead to potential data compromise or loss of access to network resources supporting business operations.

The Inspection Service did not always apply firmware updates to its [redacted] cameras. In June 2020, CISO scanned all 11,808 [redacted] cameras and identified 2,815 cameras with the same critical vulnerability. The firmware update to mitigate that vulnerability has been available since June 2018; however, the firmware was never updated.

Industry standards recommend applying firmware updates as they are released to mitigate security risks and vulnerabilities. In addition, the [redacted] camera manufacturer recommends updating firmware to the most current version. Failure to apply these updates occurred because the Inspection Service has not upgraded the video management software system to enable the supplier to apply firmware updates.

In addition, the Inspection Service does not track and maintain [redacted] cameras in an inventory system but instead keeps a list of the cameras in a manual file that does not meet Postal Service hardware inventory policy. This occurred because the Inspection Service has not defined the roles and responsibilities for creating and maintaining an inventory management system.

Without timely firmware version updates and an inventory system to track cameras and their firmware versions, there is an increased risk that a remote attacker could gain unauthorized system-level access and take control of camera operations, potentially impeding investigations.

Finally, the CISO Vulnerability Assessments Team could not always complete the weekly vulnerability scans to identify outdated versions of firmware. Postal Service information security policy and management instruction require regularly conducted scans to identify vulnerabilities and assess cybersecurity threats.

This occurred because the Telecommunication Services group intermittently blocked vulnerability scans by changing firewall security settings since October 2017. The CISO vulnerability scans were blocked because they disrupted phone services and the Retail System Software business application that processes retail transactions. The CISO attempted to coordinate a resolution with the Telecommunication Services group; however, the vulnerability scans continued to be intermittently blocked without advance notice.

When vulnerabilities are not detected and corrected, there is an increased potential for loss of confidentiality, data integrity or system availability which may result in degraded customer service and loss of goodwill and brand value.

Recommendations

We recommended management:

- Establish a process to periodically evaluate current and updated firmware versions and apply timely firmware updates to [redacted].
- Upgrade the video management software system and apply firmware updates for the [redacted] cameras.
- Establish an inventory system for the [redacted] cameras that meets the hardware asset inventory policy requirements outlined in Handbook AS-805, *Information Security*.
- Develop a process to scan the Postal Service network for vulnerabilities without negatively affecting the performance of the network and applications.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 17, 2020

MEMORANDUM FOR: MARC D. MCCRERY
ACTING VICE PRESIDENT, INFORMATION TECHNOLOGY

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service & Information Technology

SUBJECT: Audit Report – Controls Over Purchasing and Maintaining Information Technology Equipment (Report Number 19-017-R20)

This report presents the results of our audit of Controls Over Purchasing and Maintaining Information Technology Equipment.

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

Attachment

cc: Corporate Audit Response Management
Vice President, Facilities
Vice President, Supply Management
Executive Vice President, Chief Financial Officer
Executive Vice President, Chief Information Officer

Results

Introduction/Objective

This report presents the results of our self-initiated audit of Controls Over Purchasing and Maintaining Information Technology (IT) Equipment (Project Number 19-017). Our objective was to determine if controls for purchasing and maintaining IT equipment, specifically printers, webcams, and [redacted] cameras, are effective in identifying, assessing, and mitigating vulnerabilities and related cybersecurity risks to the U.S. Postal Service's IT infrastructure.

Our fieldwork was planned before the President of the United States issued the national emergency declaration concerning the novel coronavirus outbreak (COVID19) on March 13, 2020. The results of this audit do not reflect operational changes and/or service impacts that may have occurred as a result of the pandemic.

Background

The Postal Service purchases IT equipment such as printers, webcams, and [redacted] cameras. Webcams and printers are purchased through the eBuy Plus[1] system and [redacted] cameras are purchased directly from [redacted].

In April 2020, the Postal Service had about 73,000 printers, 63,357 of which are [redacted] maintained by the local information specialists. The remaining 9,352 printers are categorized as managed. These printers are managed and maintained using enterprise tools by [redacted] is the company responsible for applying firmware updates.

"Webcams are installed at post offices and other retail facilities to monitor customer wait times."

In November 2019, the Postal Service had 4,512 webcams at post offices and other retail facilities to monitor customer wait times. These webcams are on the Postal Service's internal network and each district controls and maintains the webcams in their area. [redacted] cameras are used for [redacted] The Inspection Service, Facilities group, and the U.S. Postal Service Office of Inspector General funded the procurement and maintenance of the [redacted] cameras, including firmware updates, through the [redacted] Though funding came from the three organizations, the [redacted] cameras are owned, operated, and controlled by the Postal Inspection Service. As of January 2020, there were over 11,000 [redacted] cameras connected to the Postal Service's internal network. The Postal Service contracted with [redacted] to manage the process for procurement, installation, and maintenance, including firmware updates for [redacted] cameras.

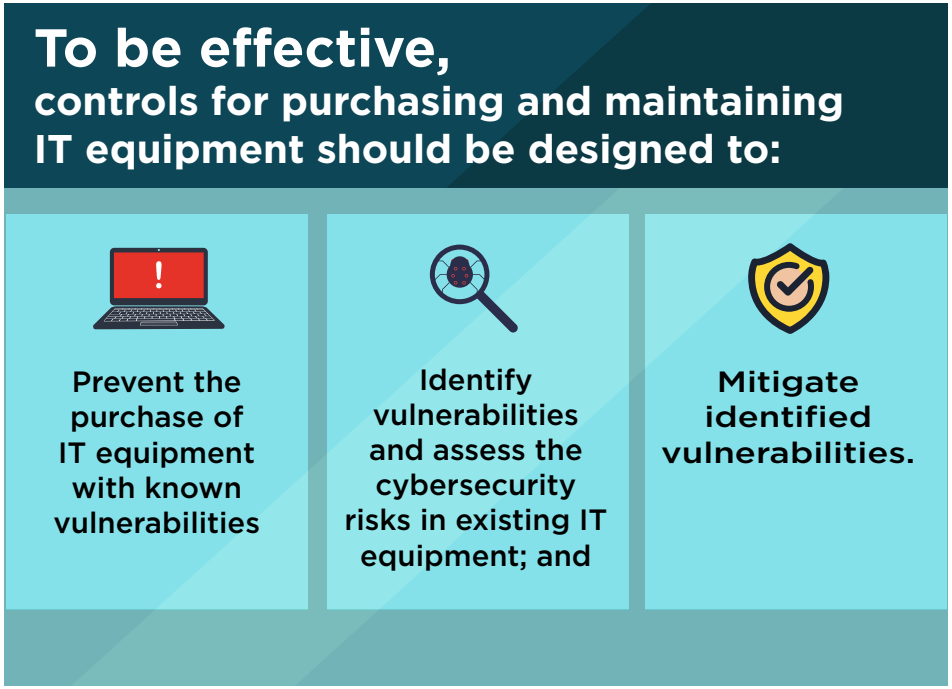
The Corporate Information Security Office (CISO) scans webcams on the Postal Service network regularly to identify security vulnerabilities for cybersecurity risks such as a denial of service. If the scans identify a security vulnerability, the CISO directs districts to apply corrective action, such as applying appropriate firmware updates. Firmware is a software program embedded on a device that provides instructions for how it communicates with other devices. Using the most updated firmware version has proven to mitigate vulnerabilities tracked by the National Institute Standards and Technology (NIST).

To be effective, controls for purchasing and maintaining printers, webcams, and [redacted] cameras should be designed to:

- Prevent the purchase of IT equipment with known vulnerabilities;
- Identify vulnerabilities and assess the cybersecurity risks in existing IT equipment; and
- Mitigate identified vulnerabilities.

1 Knowledge Base Article 26101, *eBuy Plus - Application Name, Purpose, Website*, February 28, 2020.

The Postal Service has effective controls over purchasing IT equipment, such as updating catalogs and removing webcam models that are no longer supported by the supplier. However, controls for identifying, assessing, and mitigating cybersecurity risks associated with [redacted] and [redacted] cameras are not effective.



Finding #1: Firmware Not Updated for [redacted]

The Postal Service did not update firmware on any of its 63,357 [redacted] since mid-2018. The Postal Service did not maintain a comprehensive list of active firmware versions on [redacted] to determine if updates were required to mitigate vulnerabilities. In addition, the Postal Service cannot perform vulnerability scans of these printers to identify the vulnerabilities associated with firmware versions because the scans caused adverse actions on most of the [redacted], such as taking the printers off-line. Although the Postal Service has not thoroughly assessed the risks associated with the [redacted] firmware versions, they stated the risks were not high enough to warrant concern from the organization and did not update the firmware to the most current version.

Postal Service information security policy[2] and industry standards[3] require evaluation of firmware compatibility and application of firmware updates as they are made available to mitigate potential vulnerabilities. Failure to apply these updates occurred because the IT group did not establish a process and assign responsibility for performing firmware version updates on [redacted].

Without timely firmware version updates, the Postal Service is at an increased risk of an attacker injecting a malicious file that can be used to gain control of a printer and pivot from that device to access the network. This could result in potential data compromise or loss of access to network resources that support business operations.

Recommendation #1

We recommend the **Acting Vice President, Information Technology**, coordinate with the **Vice President, Chief Information Security Officer**, to establish a process to periodically evaluate current and updated firmware versions and apply timely firmware updates to [redacted].

2 Handbook AS-805, *Information Security*, Section 8-2.4.4, November 2019.
3 NIST Special Publication 800-40, Revision 3.

Finding #2: [redacted] Camera Firmware Not Updated and Inventory Not Established

The Inspection Service did not always apply firmware updates to its [redacted] cameras. In June 2020, the CISO scanned all 11,808 [redacted] cameras to identify vulnerabilities. The scans did not identify vulnerabilities on 8,993 of these cameras; however, the remaining 2,815 cameras had the same critical vulnerability. The firmware version update to mitigate that critical vulnerability has been available since June 2018; however, the firmware was never updated (see Appendix B).

Postal Service policy[4] and NIST[5] recommend updating firmware timely to avoid security risks and vulnerabilities. [redacted] recommends updating firmware to the most current version to mitigate vulnerabilities. Failure to apply these updates occurred because the Inspection Service has not upgraded the video management software system to enable the supplier to apply the firmware updates.

> *"Inspection Service did not track and maintain [redacted] cameras in an inventory management system because roles and responsibilities were not established."*

In addition, the Inspection Service did not track and maintain [redacted] cameras in an inventory management system and instead kept a list of the cameras in a manual file that did not meet Postal Service hardware asset inventory policy.[7] This occurred because the Inspection Service has not established the roles and responsibilities for maintaining an inventory management system.

Without timely firmware updates and an inventory system to identify cameras and verify firmware versions are up to date, there is an increased risk that a remote attacker could gain unauthorized system-level access and take control of camera operations, potentially impeding investigations.

Recommendation #2

We recommend the **Chief Postal Inspector** upgrade the video management software system and apply firmware updates to [redacted] cameras.

Recommendation #3

We recommend the **Chief Postal Inspector** establish an inventory system for the [redacted] cameras that meets Handbook AS-805, *Information Security*, Section 10-2.7, Hardware Asset Inventory Policy requirements.

Finding #3: CISO Vulnerability Scans Blocked

The CISO Vulnerability Assessments Team could not complete weekly vulnerability scans of specific network segments to identify outdated, vulnerable versions of firmware. Postal Service policy[8] and management instruction[9] require regularly conducted scans to identify vulnerabilities and assess cybersecurity threats.

This occurred because, since October 2017, the Telecommunication Services group intermittently blocked vulnerability scans by changing firewall security settings. The CISO vulnerability scans were disrupting phone services and the Retail System Software business application that processes retail transactions. The CISO attempted to coordinate a resolution with the Telecommunication Services group; however, the vulnerability scans continued to be intermittently blocked without advance notice.

4 Handbook AS-805, Section 8-2.4.4.
5 NIST Special Publication 800-40, Revision 3.
6 [redacted].
7 Handbook A- 805, Section 10-2.7 Hardware Asset Inventory.
8 Handbook AS-805, Section 10-4.6, Scanning Hardware and Software for Vulnerabilities.
9 Management Instructions AS-800-2019-1, dated May 1, 2019, and AS-862-2017-1, dated May 2017.

When vulnerability scanning cannot be performed, there is a risk that the Postal Service will not detect and correct vulnerabilities, potentially resulting in a loss of confidentiality, integrity, or system availability of Postal Service data or systems. This impact on Postal Service data or systems could result in degraded customer service and loss of goodwill and brand value.

Recommendation #4

We recommend the **Acting Vice President, Information Technology**, coordinate with the **Vice President, Chief Information Security Officer**, to develop a process to scan the Postal Service network for vulnerabilities without negatively affecting network and application performance.

Management's Comments

Management agreed with the findings and recommendations in the report.

Regarding recommendation 1, management stated that they will formalize a process to evaluate firmware updates for the [redacted] models supported by IT and update the firmware to address any critical vulnerabilities to the extent enabled with automated updates. The target implementation date is April 30, 2021.

Regarding recommendations 2 and 3, the Chief Postal Inspector will work with various entities to upgrade the video management software system and apply firmware updates to and establish an inventory system for the [redacted] cameras that meets Handbook AS-805, Section 10-2.7, Hardware Asset Inventory Policy requirements. The target implementation date is August 31, 2021.

Finally, for recommendation 4, management stated that CISO and IT will collaboratively review and update current procedures to address vulnerability assessment activities to ensure that assessments are non-disruptive to applications, services, and network performance across the enterprise. In addition, CISO will develop metrics to validate completeness for scanning the entire USPS address space and operational impacts validated by root cause analysis to maintain continuous monitoring of environment scanning. The target implementation date is June 30, 2021. See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report.

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

Appendices

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

Appendix A: Additional Information

Scope and Methodology

We reviewed controls for purchasing and using webcams, [redacted] cameras, and printers. These controls include preventive controls to prevent purchasing IT equipment with known vulnerabilities, detective controls to identify existing vulnerabilities and assess cybersecurity risks, and corrective controls to mitigate risks from identified vulnerabilities.

We did not include IT asset management in our review including software patch management controls, unsupported operating system, controls over software applications purchases, servers that support the [redacted] camera formerly called Closed-Circuit Television System, and computers.

To accomplish our objective, we:

- Interviewed management to discuss IT equipment purchase processes and controls;
- Reviewed Postal Service policy for purchasing IT equipment;
- Analyzed IT equipment purchased during fiscal years 2018 and 2019; and
- Assessed vulnerabilities using the NIST National Vulnerability Database.

We conducted this performance audit from November 2019 through August 2020 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 July 24, 2020 and included their comments where appropriate.

We assessed the reliability of IT equipment data by running the script used by Postal Service management against the IT equipment database and compared the results to the reports received from Postal Service management. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this audit within the last five years.

Appendix B: Additional Information

Table 1. Number of [redacted] Cameras with Critical Vulnerabilities by Model

Model & Version	Number of Cameras
[redacted]	2
	1
	3
	2
	4
	16
	5
	4
	3
	2
	14
	2
	5
	1
	7
	41
	1,598
	17
	6
	194
	47
	4
[redacted]	9
	9
	2
	3
	311
	22
	1
	5
	327
	2
	1
	7
	11
	4
	42
	11
	1
	2
	4
	63
Total	**2,815**

Source: CISO, June 18, 2020.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

August 12, 2020

Lazerick C. Poland
Director, Audit Operations

SUBJECT: Audit Report – Controls Over Purchasing and Maintaining Information Technology Equipment (Project Number 19-017-DRAFT)

Management has reviewed the Security Assessment of a U.S. Postal Service Information Technology Application. This letter provides the OIG Management's Response. In general, Management agrees with the findings provided by the OIG team.

Recommendation #1:
We recommend the **Vice President, Information Technology,** coordinate with the **Vice President, Chief Information Security Officer,** to establish a process to periodically evaluate current and updated firmware versions and apply timely firmware updates to [redacted]

Management Response/Action Plan:
Management agrees with this recommendation and will formalize a process to evaluate firmware updates for the [redacted] models supported by IT. For these devices, USPS agrees to update the firmware to address any critical vulnerabilities to the extent enabled with automated updates.

Target Implementation Date:
April 30, 2021

Responsible Officials:
Manager, Enterprise Access Infrastructure
Manager, CyberSecurity Risk

Recommendation #2:
We recommend the **Chief Postal Inspector** upgrade the video management software system and apply firmware updates to [redacted] cameras.

Management Response/Action Plan:
Management agrees with this recommendation. The Chief Postal Inspector will work with the various entities to upgrade the video management software system and apply firmware updates to the [redacted] cameras.

Target Implementation Date:
August 31, 2021

Responsible Official:
Inspector in Charge, Security Group

Recommendation #3:
We recommend the **Chief Postal Inspector** establish an inventory system for the [redacted] cameras that meets Handbook AS-805, *Information Security*, Section 10-2.7, Hardware Asset Inventory Policy requirements.

Management Response/Action Plan:
Management agrees with this recommendation. The Chief Postal Inspector will establish an inventory system for the [redacted] cameras in accordance with Handbook AS-805, Information Security, Section 10-2.7, Hardware Asset Inventory Policy requirements.

Target Implementation Date:
August 31, 2021

Responsible Official:
Inspector in Charge, Security Group

Recommendation #4:
We recommend the **Vice President, Information Technology,** coordinate with the **Vice President, Chief Information Security Officer**, to develop a process to scan the Postal Service network for vulnerabilities without negatively affecting network and application performance.

Management Response/Action Plan:
Management agrees with this recommendation. CISO and IT will collaboratively review and update current procedures to address vulnerability assessment activities to ensure that assessments are non-disruptive to applications, services, and network performance across the enterprise. CISO will develop metrics to validate completeness of scanning of the entire USPS address space and operational impacts validated by root cause analysis to maintain continuous monitoring of environment scanning.

Target Implementation Date:
June 30, 2021

Responsible Officials:
Manager, Enterprise Access Infrastructure
Manager, CyberSecurity Risk

E-SIGNED by Marc.D Mccrery
on 2020-08-11 16:59:47 CDT

Marc D McCrery
Vice President, Information Technology (A)

E-SIGNED by Gregory.S Crabb
on 2020-08-11 14:01:41 CDT

Gregory S. Crabb
Vice President, Chief Information Security Officer

E-SIGNED by Gary.R Barksdale
on 2020-08-11 15:25:58 CDT

Gary R. Barksdale
Chief Postal Inspector

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

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, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov