Office of Inspector General | United States Postal Service

Audit Report

# U.S. Postal Service Protection Against External Cyberattacks

Report Number 20-277-R21 | August 31, 2021

# Table of Contents

Cover
Highlights....1
Objective....1
Findings....1
Recommendations....2
Transmittal Letter....3
Results....4
Introduction/Objective....4
Background....4
Findings Summary....4
Finding #1: Effective Security Controls to Defend Against External Attacks....5
Finding #2: Security Awareness Training Records....5
Recommendation #1....5
Finding #3: Vulnerability Management Program....5
Recommendation #2....7
Recommendation #3....8
Recommendation #4....8
Management's Comments....8
Evaluation of Management's Comments....8
Appendices....9
Appendix A: Additional Information....10
Scope and Methodology....10
Appendix B: Management's Comments....12
Contact Information....15

# Highlights

## Objective

Our objective was to determine if the U.S. Postal Service has an effective security posture to protect its Information Technology (IT) infrastructure from external cyberattacks and prevent unauthorized access to restricted data.

In the past two years, 51 percent of organizations have experienced a cybersecurity incident that resulted in a significant disruption to their IT & business processes. With one of the largest IT networks in the world, the Postal Service faces ongoing cyberthreats and challenges that could negatively impact its customers, partners, and employees.

Ninety-one percent of cyberattacks weaponize email through phishing campaigns to gain unauthorized access to an organization's IT infrastructure. Phishing is when an attacker pretends to be a trusted individual and tricks a victim into opening a malicious email. A security awareness program, including training and simulated phishing campaigns, is critical to supporting a strong security posture.

A way to test an organization's defenses against potential cyberattacks is through a penetration test, which involves trusted individuals using known attack methods to identify exploitable network vulnerabilities. Vulnerabilities identified through simulated phishing campaigns and penetration tests should be tracked by a vulnerability management program until each vulnerability has been mitigated.

We contracted with a provider to conduct a simulated phishing campaign and an external penetration test targeting the Postal Service's internet-facing systems from November 30, 2020, to February 9, 2021. We also reviewed the Postal Service's information security awareness program.

## Findings

The Postal Service generally has an effective security posture and security awareness program to protect its IT infrastructure from external cyberattacks. However, [redacted]

We determined the Postal Service established a security awareness program aligned with industry best practices. Additionally, we found Postal Service employees performed better than industry benchmarks during our phishing campaign.

> *"We determined the Postal Service established a security awareness program aligned with industry best practices."*

While the security awareness program aligned with best practices, we found that the Corporate Information Security Office (CISO) did not update the access management system to ensure that it removed all excluded employees from reports reflecting completion rates. Best practices indicate that records should be accurate and provide relevant information to support management's decisions.

We also found the Postal Service effectively minimized its internet exposure and most web servers were securely configured. However, the Postal Service does not have an [redacted] During our external penetration test, [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

These issues occurred because the [redacted] team does not have the [redacted] Rather than utilizing an [redacted]. Further, management stated that the [redacted]. Finally, the [redacted]

According to best practices, [redacted] essential elements is key to an efficient [redacted]. In addition, [redacted]

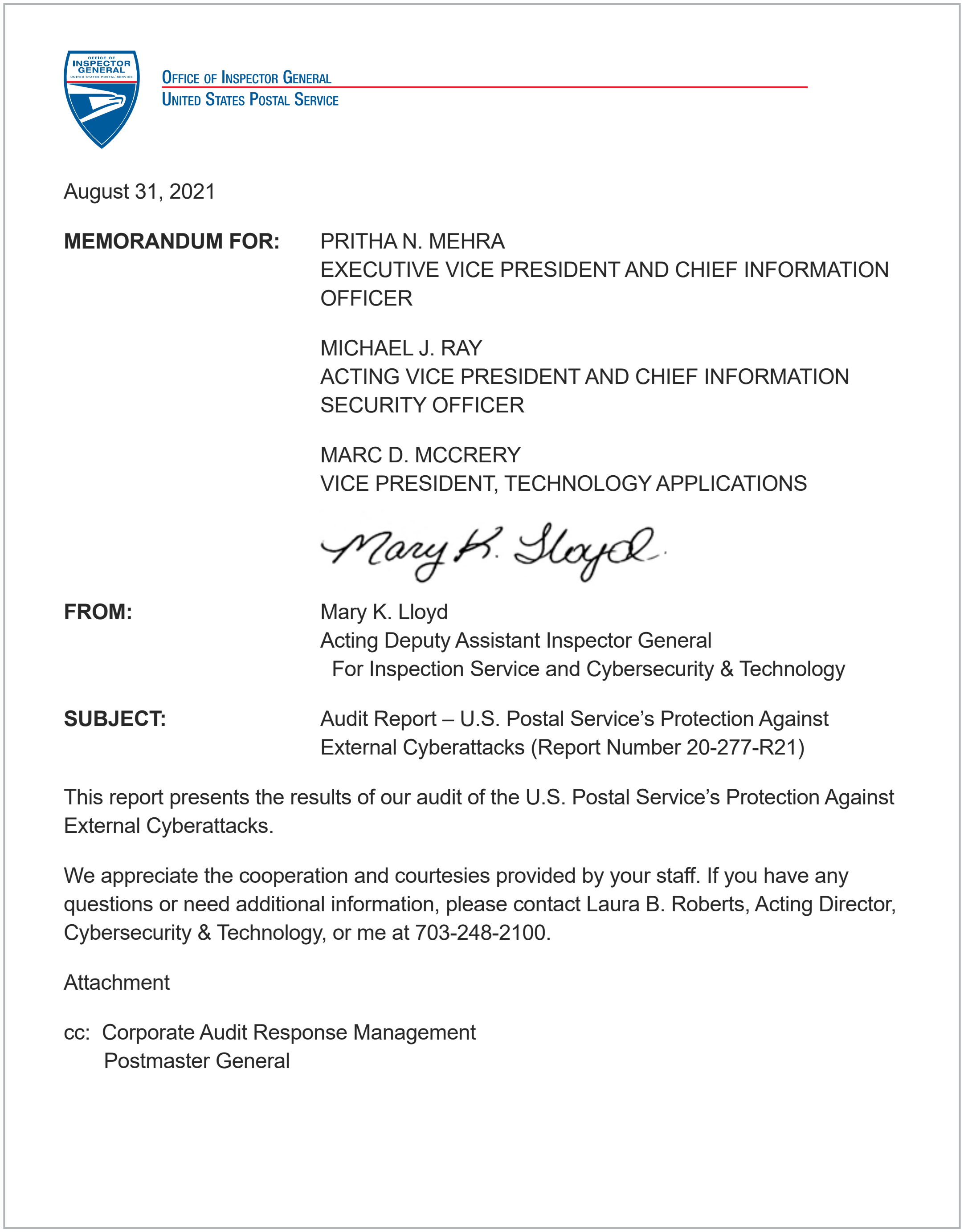
An effective [redacted] is critical to reducing cybersecurity risk within the USPS enterprise. Lack of an effective [redacted]

## Recommendations

We recommended management:

1. Implement a consistent process to approve and update the access management system for all employees excluded from mandatory security awareness training and update information security policy to reflect the process.
2. Update and verify [redacted]
3. Once [redacted]
4. Implement a [redacted]

# Transmittal Letter



Office of Inspector General
United States Postal Service

August 31, 2021

**MEMORANDUM FOR:** PRITHA N. MEHRA
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

MICHAEL J. RAY
ACTING VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER

MARC D. MCCRERY
VICE PRESIDENT, TECHNOLOGY APPLICATIONS

Mary K. Lloyd

**FROM:** Mary K. Lloyd
Acting Deputy Assistant Inspector General
For Inspection Service and Cybersecurity & Technology

**SUBJECT:** Audit Report – U.S. Postal Service's Protection Against External Cyberattacks (Report Number 20-277-R21)

This report presents the results of our audit of the U.S. Postal Service's Protection Against External Cyberattacks.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Laura B. Roberts, Acting Director, Cybersecurity & Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management
Postmaster General

# Results

## Introduction/Objective

This report presents the results of our self-initiated U.S. Postal Service's Protection Against External Cyberattacks (Project Number 20-277). Our objective was to determine if the Postal Service has an effective security posture to protect its Information Technology (IT) infrastructure from external cyberattacks and prevent unauthorized access to restricted data. See Appendix A for additional information about this audit.

## Background

The Postal Service faces ongoing cyber threats and challenges that could directly impact customers, partners, and employees while maintaining one of the largest IT networks in the world. This network supports the secure connection to over 260,000 mobile delivery devices, 152,000 computers, 46,000 point-of-sale terminals, 2,700 self-service retail kiosks, and 31,000 facilities.

Threat actors are increasingly taking advantage of current events and leveraging interest in the COVID-19 pandemic to exploit vulnerable assets and launch phishing[1] emails.[2] In fact, 91 percent of cyberattacks weaponize email through phishing campaigns to gain unauthorized access to an organization's IT infrastructure. The Postal Service manages over 216,000 email accounts, receiving over 5.3 million legitimate emails a day while blocking over two million emails monthly containing spam and malware.[3] This large internet exposure can lead to a major disruption due to a cyberattack of the Postal Service's IT or Engineering network and could cost the organization more than [redacted] A security awareness program, including training and simulated phishing campaigns, is critical to supporting a strong security posture. Simulated phishing campaigns are frequently used to test technical network controls and assess user information security awareness.

A method to measure the effectiveness of an organization's ability to defend itself from a cyberattack is performing a penetration test. A penetration test can provide objective insights regarding an organization's policies, processes, and defenses to improve organizational readiness and evaluate performance levels[5] against potential cyber threats.

Vulnerabilities identified through simulated phishing campaigns and penetration tests should be tracked by a vulnerability management program until each vulnerability has been mitigated. To assess the security posture of the Postal Service's IT Infrastructure, we contracted with a provider to conduct a simulated phishing campaign and an external penetration test targeting the Postal Service's internet-facing systems from November 30, 2020, to February 9, 2021. We also reviewed the Postal Service's information security awareness program.

## Findings Summary

The Postal Service generally has an effective security posture and security awareness program to protect its IT infrastructure from external cyberattacks. However, [redacted]

[redacted]

[1] When an attacker pretends to be a trusted individual to trick a victim into opening a malicious email.
[2] Bitsight, Coronavirus Pandemic Leads to New and Evolving Cyber Threats, dated April 1, 2020.
[3] *Postal Facts 2020 Companion*, dated April 2020.
[4] [redacted]
[5] Center for Internet Security, Penetration Tests and Red Team Exercises, dated April 1, 2019.
[6] [redacted]

## Finding #1: Effective Security Controls to Defend Against External Attacks

We determined that the Postal Service established a security awareness program aligned with industry best practices.[7] We also found that Postal Service employees[8] performed better than industry benchmarks[9] during our phishing campaign. Specifically, we sent phishing emails to a sample of 2,000 employees and [redacted]) clicked on the link. The industry benchmark is 5.8 percent for large government organizations with 1,000 or more employees and at least one year of ongoing training and simulated phishing tests.

In addition, our external penetration test found the IT infrastructure is adequately protected from external cyberattacks. We found security administrators limited internet exposure by closing unnecessary ports and disabling unnecessary services. These security controls align with the Postal Service's information security policies and procedures.[10]

## Finding #2: Security Awareness Training Records

While the security awareness program aligned with best practices, the Corporate Information Security Office (CISO) did not update the access management system[11] to accurately reflect all employees excluded from mandatory security awareness training. Management provided a list of employees excluded from taking FY 2020 mandatory security awareness training. Based on this information, we determined that 148,149 of 194,365 employees (76.22 percent) required to take the training completed it. However, CISO management subsequently provided three revised lists of exclusions during the audit but couldn't provide evidence of management approvals for all exclusions. This led to updated results showing that 124,627 of 133,046 employees (93.67 percent) completed training as required.[12] As a result, we found that the reports[13] used to track security awareness training records were not updated to reflect all employee exclusions. According to best practices, training records should contain accurate data to measure performance, support management decisions,[14] and distinguish mandatory from voluntary training assignments.[15]

This occurred because management has an approval process for excluding employees from taking mandatory security awareness training. For example, some employees may not use a computer to perform their job duties; however, the process does not ensure that all employees excluded from mandatory training are distinguished in the training reporting system. Additionally, the process is not documented in information security policy.[16] When the approval and update process does not ensure that the system of record accurately distinguishes employees who are excluded from mandatory training, this may skew metrics used to evaluate training effectiveness.

### Recommendation #1

We recommend the **Vice President, Chief Information Security Officer,** implement a consistent process to approve and update the access management system for all employees excluded from mandatory security awareness training and update information security policy to reflect the process.

## Finding #3: Vulnerability Management Program

We found that the Postal Service effectively minimized its internet exposure and most web servers were securely configured; however, the Postal Service [redacted]. During our external penetration test against

[7] National Institute of Standards and Technology, Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, dated October 2003.
[8] Includes USPS employees and contract workers.
[9] *2020 Phishing by Industry Benchmarking Report*, KnowBe4, Inc., dated March 2020.
[10] Handbook AS-805, *Information Security*, Section 1.1, Purpose, dated November 2019
[11] [redacted] is the system for managing access to Postal Service applications and resources and is used to generate reports on security awareness completion.
[12] Handbook AS-805, Section 6-5.3, Training Requirements, dated November 2019.
[13] Education Awareness Status Reports: FY20 CyberSafe Fundamentals for Employees and FY20 Contractor-CyberSafe Fundamentals, Parts I and II
[14] Performance Measurement & Metrics, Association Forum, Professional Practice Statement, dated October 2013.
[15] The Importance of Tracking Employee Training, Power DMS Training Management article, dated December 2020.
[16] Handbook AS-805, Section 6-5, Information Security Awareness and Training, dated November 2019.

internet-facing systems, [redacted]

> *“During our external penetration test,* [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

During our audit, Postal Service management began prioritizing some of the OIG-identified [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

These issues occurred because the [redacted] Rather, the program relies on [redacted] The team is currently [redacted]

[17] [redacted]
[18] [redacted]
[19] [redacted].
[20] [redacted]
[21] [redacted]
[22] [redacted]

[redacted]. Further, management stated that the [redacted] Finally, the [redacted]. See Figure 1 for information on the [redacted]

[redacted]

[redacted]

[redacted]

According to best practices,[24] [redacted]

In a prior audit,[27] we identified a similar issue with maintaining a complete inventory of internet-facing systems to include key data elements such as stakeholders. As a result, CISO management enhanced standard operating procedures to manually review and update the Configuration Management Database inventory on a quarterly basis. However, we determined that the key data elements, such as stakeholders, are not consistently complete and accurate to effectively remediate identified vulnerabilities.

An effective vulnerability management program is critical to reducing cybersecurity risk within the Postal Service enterprise. The [redacted]. In addition, [redacted] This decreases program effectiveness, [redacted]

**Recommendation #2**

We recommend the **Executive Vice President, Chief Information Officer**, update and verify [redacted]

[23] [redacted]

[24] *5 Best Practices to* [redacted] February 2021.

[25] [redacted]

[26] Carnegie Mellon, Cyber Resilience Review Supplemental Resource Guide, Vol. 4, V 1.1, Vulnerability Management, dated 2016.

[27] *Internet-Facing Devices*, dated November 3, 2016.

### Recommendation #3

We recommend the **Vice President, Chief Information Security Officer**, once [redacted]

### Recommendation #4

We recommend the **Vice President, Technology Applications**, coordinate with the **Vice President, Chief Information Security Officer**, to implement a [redacted]

## Management's Comments

Management agreed with findings 1, 2 and 3; and agreed with recommendations 1, 2, 3, and 4. However, management contends that footnotes 16, 17, and 27 referenced by the OIG team are inappropriate for use as best practice criteria.

Regarding recommendation 1, management agreed and stated that they will update Handbook AS-805 to include supporting language allowing CISO to grant certain Postal Service personnel exemptions from security and awareness training. The target implementation date is June 30, 2022.

Regarding recommendation 2, management agreed and stated that they will create and implement a standard operating procedure (SOP) to periodically review [redacted] The target implementation date is July 29, 2022.

Regarding recommendation 3, management agreed and stated that they will prioritize remediation based on the established [redacted] The target implementation date is June 30, 2022.

Regarding recommendation 4, management agreed and stated they will implement the [redacted]. The target implementation date is July 29, 2022.

See Appendix B 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 and their action plans to address these recommendations should resolve the issues identified in this report.

Regarding sources for footnotes referenced by the OIG team, well known and widely recognized industry standards around data quality support the concept that training records should be accurately tracked to support management decisions. Distinguishing between mandatory and voluntary training is an expansion of data quality principles as it relates to relevancy of the data. In addition, automation of vulnerability tracking is a widely recommended practice to improve the efficiency and effectiveness of vulnerability management programs. The reference cited reflects these practices and our use of this reference does not suggest or imply the OIG recommends the use of any product.

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.

BACK to COVER

# Appendices

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

Appendix A: Additional Information .......... 10
Scope and Methodology .......... 10
Appendix B: Management's Comments .......... 12

# Appendix A: Additional Information

## Scope and Methodology

Our scope included Postal Service internet accessible systems and a sample of Postal Service employees who have network authentication IDs and email access.

To accomplish our objective, we contracted with a provider to (1) conduct an email phishing campaign against Postal Service employees and (2) perform an external penetration test against Postal Service internet accessible systems from November 30, 2020, to February 9, 2021. These assessments used manual and automated tools to identify servers, databases, and applications that are internet accessible, as well as open-source frameworks to test user susceptibility to phishing.

In addition, the audit team:

- Collaborated with the CISO and the OIG contractor to develop the Technical Assessment Plan for the phishing campaign and Rules of Engagement for the external penetration test. The Technical Assessment Plan describes the methodology, timeline, and tools used to conduct the assessment. Rules of Engagement identify the general rules and expectations documented and approved including:
  - Roles and responsibilities
  - Scope of the penetration test
  - Communication Plan-established notification protocols and emergency contacts.
- Interviewed key personnel to gain an understanding of security awareness training and penetration test policies and procedures.
- Evaluated the Postal Service's security awareness program and determine if it includes social engineering.
- Determined the number of employees with active Postal Service network authentication IDs and email addresses and selected a stratified simple random sample of 2,000 employees to test technical network controls and assess user information security awareness.
- Reviewed Postal Service policies and procedures associated with protecting sensitive information and training requirements.

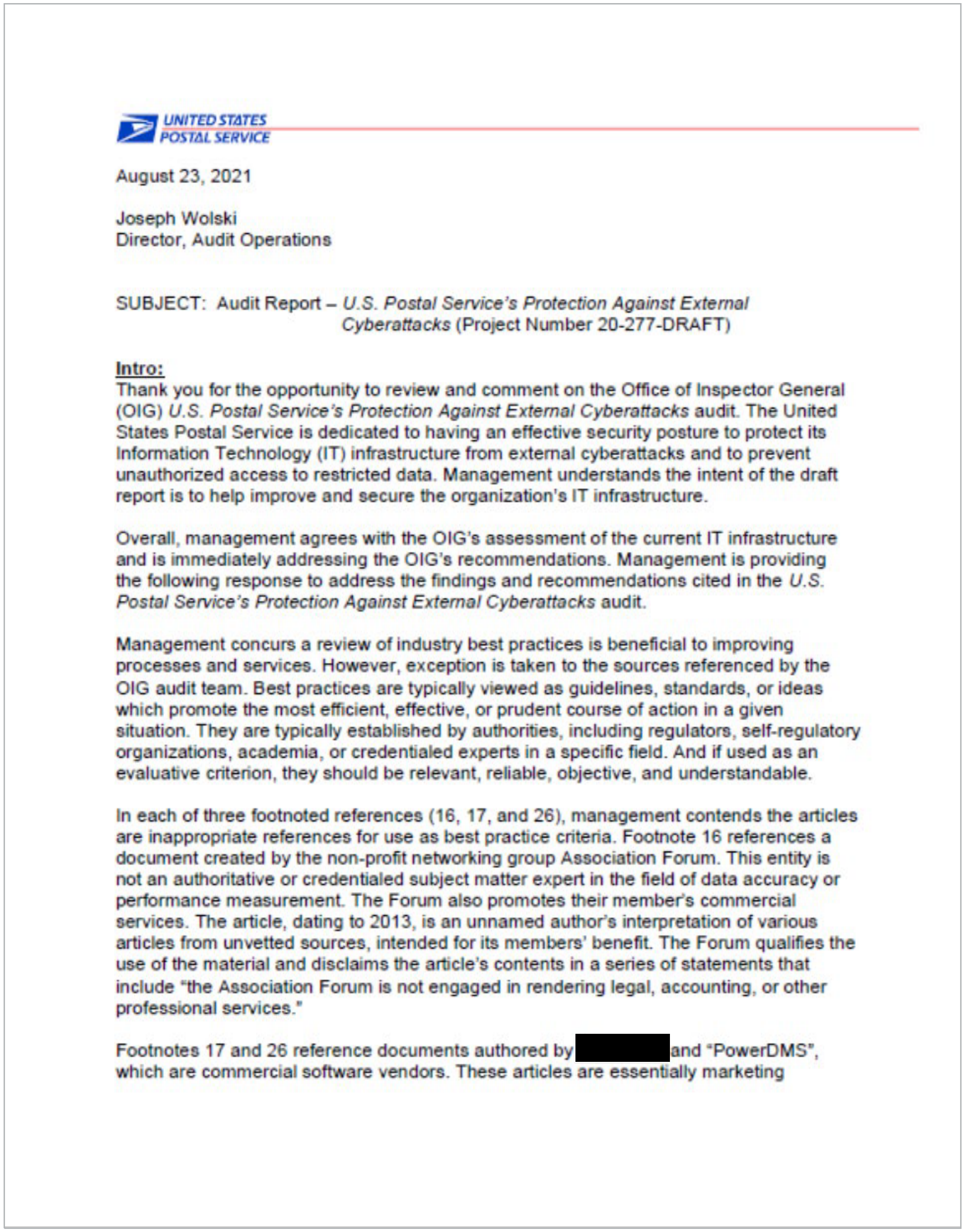
We conducted this performance audit from August 2020 through August 2021 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain 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 29, 2021 and included their comments where appropriate.

We assessed the reliability of computer-generated data that resulted from our automated testing by analyzing and reviewing the raw data, performing automated and manual reviews to supporting documents or systems, and interviewing personnel knowledgeable about the data. 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 |
|---|---|---|---|---|
| *Internet-Facing Devices* | Identify internet-facing hosts connected to the Postal Service network and determine if a complete inventory exists. | IT-AR-17-001 | 11/32016 | None |
| *Cybersecurity Incident Detection and Response Capability* | Determine if the Postal Service has a cybersecurity incident response capability to effectively detect, analyze, and respond to cyber threats. | 19-012-R20 | 7/29/2020 | None |
| *Security Assessment of a U.S. Postal Service Information Technology Application* | Determine if the Postal Service has effective security controls to protect a Postal Service IT system from cyberattacks and prevent unauthorized access to restricted data. | 19-018-R20 | 8/11/2020 | None |

# Appendix B: Management's Comments



UNITED STATES POSTAL SERVICE

August 23, 2021

Joseph Wolski
Director, Audit Operations

SUBJECT: Audit Report – *U.S. Postal Service's Protection Against External Cyberattacks* (Project Number 20-277-DRAFT)

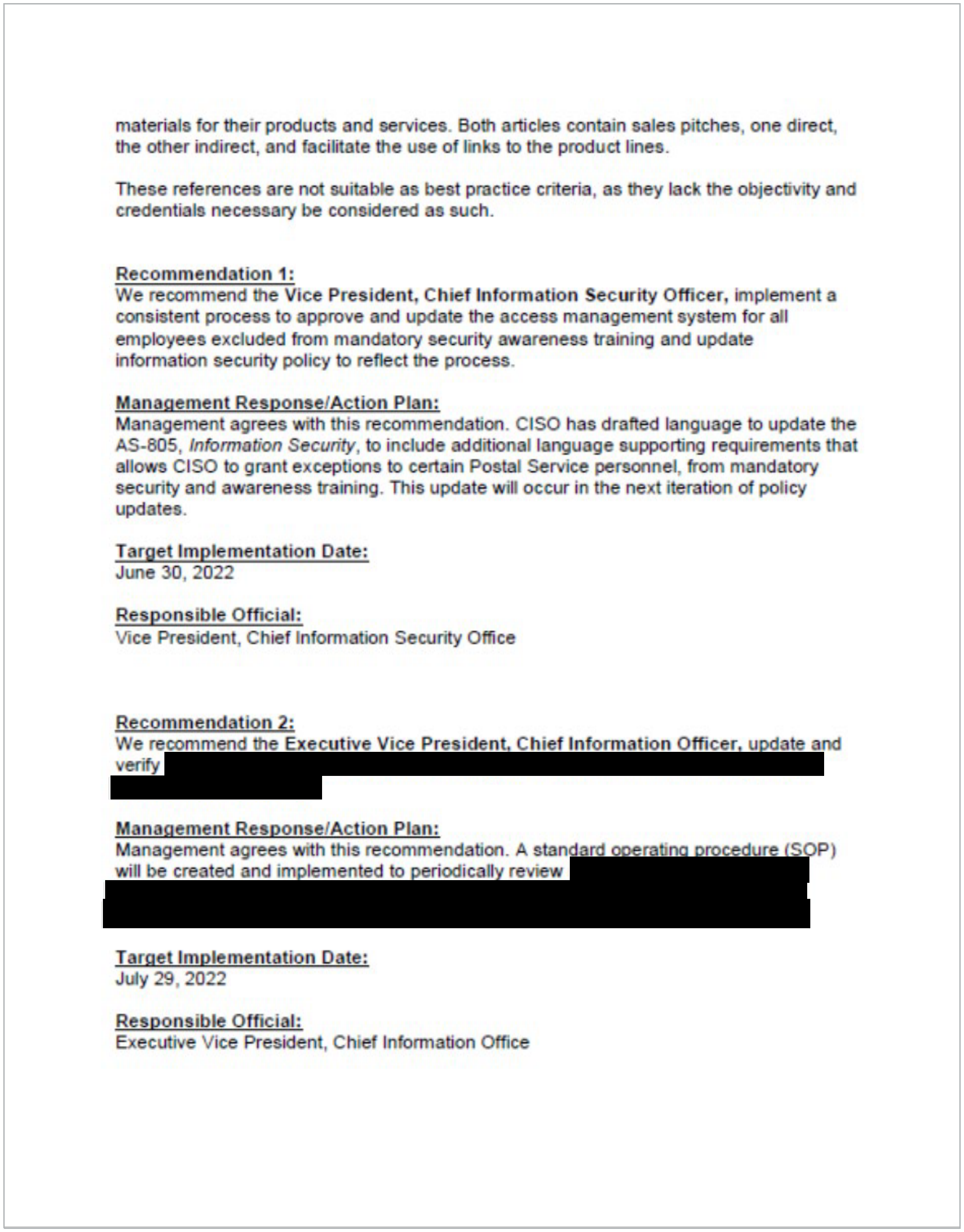
**Intro:**
Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) *U.S. Postal Service's Protection Against External Cyberattacks* audit. The United States Postal Service is dedicated to having an effective security posture to protect its Information Technology (IT) infrastructure from external cyberattacks and to prevent unauthorized access to restricted data. Management understands the intent of the draft report is to help improve and secure the organization's IT infrastructure.

Overall, management agrees with the OIG's assessment of the current IT infrastructure and is immediately addressing the OIG's recommendations. Management is providing the following response to address the findings and recommendations cited in the *U.S. Postal Service's Protection Against External Cyberattacks* audit.

Management concurs a review of industry best practices is beneficial to improving processes and services. However, exception is taken to the sources referenced by the OIG audit team. Best practices are typically viewed as guidelines, standards, or ideas which promote the most efficient, effective, or prudent course of action in a given situation. They are typically established by authorities, including regulators, self-regulatory organizations, academia, or credentialed experts in a specific field. And if used as an evaluative criterion, they should be relevant, reliable, objective, and understandable.

In each of three footnoted references (16, 17, and 26), management contends the articles are inappropriate references for use as best practice criteria. Footnote 16 references a document created by the non-profit networking group Association Forum. This entity is not an authoritative or credentialed subject matter expert in the field of data accuracy or performance measurement. The Forum also promotes their member's commercial services. The article, dating to 2013, is an unnamed author's interpretation of various articles from unvetted sources, intended for its members' benefit. The Forum qualifies the use of the material and disclaims the article's contents in a series of statements that include "the Association Forum is not engaged in rendering legal, accounting, or other professional services."

Footnotes 17 and 26 reference documents authored by [redacted] and "PowerDMS", which are commercial software vendors. These articles are essentially marketing



materials for their products and services. Both articles contain sales pitches, one direct, the other indirect, and facilitate the use of links to the product lines.

These references are not suitable as best practice criteria, as they lack the objectivity and credentials necessary be considered as such.

**Recommendation 1:**
We recommend the **Vice President, Chief Information Security Officer,** implement a consistent process to approve and update the access management system for all employees excluded from mandatory security awareness training and update information security policy to reflect the process.

**Management Response/Action Plan:**
Management agrees with this recommendation. CISO has drafted language to update the AS-805, *Information Security*, to include additional language supporting requirements that allows CISO to grant exceptions to certain Postal Service personnel, from mandatory security and awareness training. This update will occur in the next iteration of policy updates.

**Target Implementation Date:**
June 30, 2022

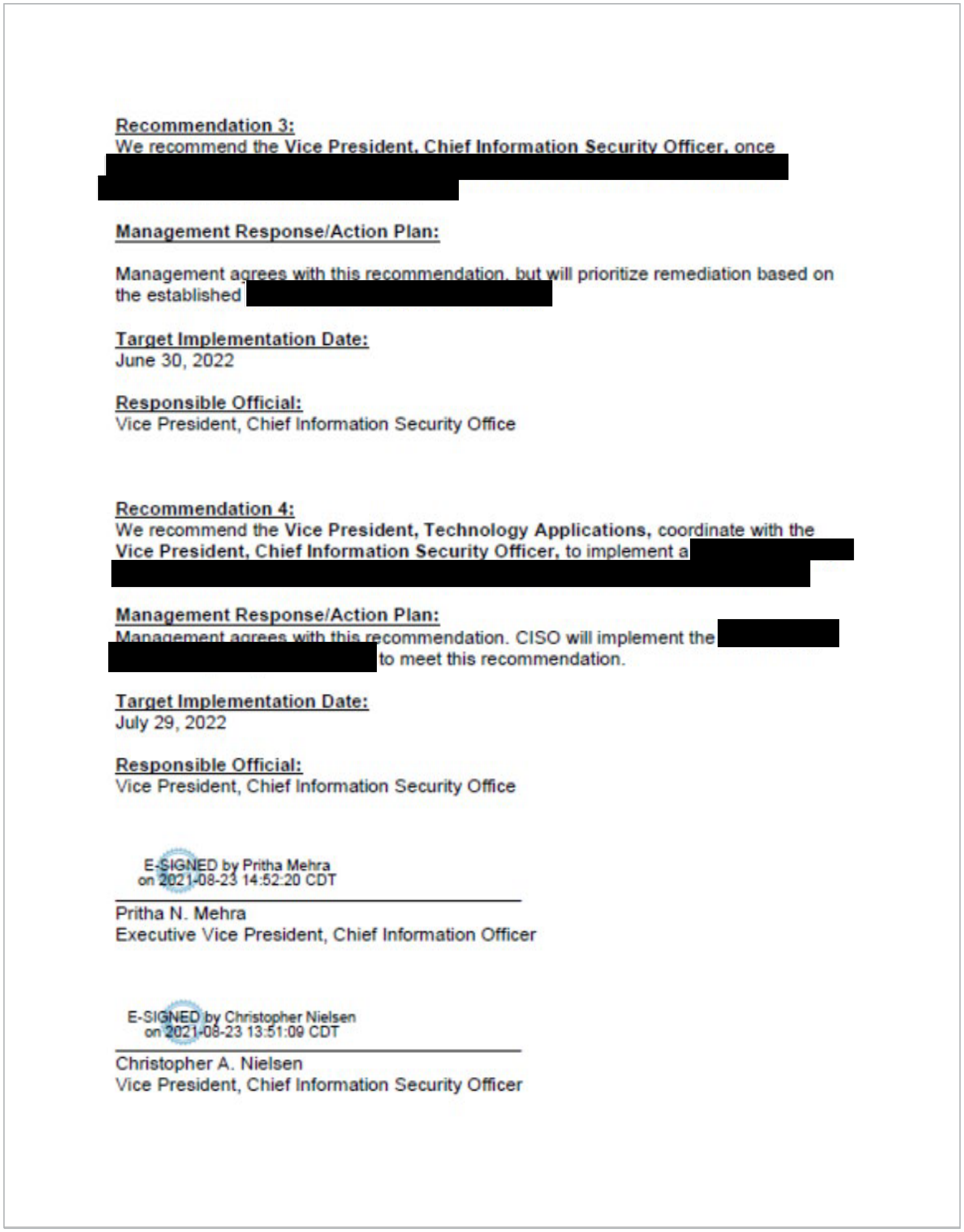
**Responsible Official:**
Vice President, Chief Information Security Office

**Recommendation 2:**
We recommend the **Executive Vice President, Chief Information Officer,** update and verify [redacted]

**Management Response/Action Plan:**
Management agrees with this recommendation. A standard operating procedure (SOP) will be created and implemented to periodically review [redacted]

**Target Implementation Date:**
July 29, 2022

**Responsible Official:**
Executive Vice President, Chief Information Office



**Recommendation 3:**
We recommend the **Vice President, Chief Information Security Officer**, once [redacted]

**Management Response/Action Plan:**

Management agrees with this recommendation, but will prioritize remediation based on the established [redacted]

**Target Implementation Date:**
June 30, 2022

**Responsible Official:**
Vice President, Chief Information Security Office

**Recommendation 4:**
We recommend the **Vice President, Technology Applications**, coordinate with the **Vice President, Chief Information Security Officer**, to implement a [redacted]

**Management Response/Action Plan:**
Management agrees with this recommendation. CISO will implement the [redacted] to meet this recommendation.

**Target Implementation Date:**
July 29, 2022

**Responsible Official:**
Vice President, Chief Information Security Office

E-SIGNED by Pritha Mehra
on 2021-08-23 14:52:20 CDT

Pritha N. Mehra
Executive Vice President, Chief Information Officer

E-SIGNED by Christopher Nielsen
on 2021-08-23 13:51:09 CDT

Christopher A. Nielsen
Vice President, Chief Information Security Officer

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, please email
press@uspsoig.gov or call 703-248-2100