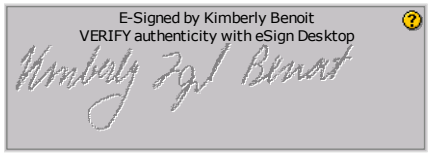
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 5, 2018

MEMORANDUM FOR: MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

FROM:



Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Management Alert – Access Issues Identified in the Mail Processing Environment (Report Number IT-MT-18-001)

This management alert presents Access Issues Identified in the Mail Processing Environment (Project Number 18TG012IT000). These issues came to our attention during our ongoing Review of Information Technology Network Performance audit (Project Number 18TG005IT000). The issues require immediate attention and remediation.

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

Attachment

cc: Postmaster General
Vice President, Network Operations
Vice President, Chief Information Security Officer
Corporate Audit Response Management

Introduction

During the Review of Information Technology Network Performance audit (Project Number 18TG005IT000), the U.S. Postal Service Office of Inspector General (OIG) found access control issues in the mail processing environment. The issues identified were not directly related to the scope of the audit; however, they pose security weaknesses that we believe warrant management's attention. The purpose of this alert is to bring these issues to your attention and make recommendations for corrective action.

The Mail Processing Equipment (MPE)/Mail Handling Equipment (MHE) environment includes networks, computer systems, and equipment that manage, monitor, and control mail processing functions. In this environment, there are

The objective of this alert is to inform the Postal Service of access control issues associated with . Specifically, we identified access control issues with the
While the scope of this alert is limited to issues related to at the sites we visited, these weaknesses at mail processing facilities with an .

Conclusion

We identified access control weaknesses related to the .
Specifically, Postal Service management authorizes the use of
In addition, management allows r

These issues occurred because management did not that are in accordance with Postal Service policy and used outdated hardware that cannot support

[1] .

Shared Usernames and Passwords

The Postal Service does not require unique login credentials[2] for standard access[3] to the [redacted] switches. Additionally, the password for [redacted] Furthermore, both passwords are [redacted].

Postal Service policy[5] states that passwords for privileged[6] and maintenance accounts must be held at a higher level of control and account management documented to ensure information resource integrity, availability, and confidentiality. In addition, passwords used to connect to information resources must be treated as sensitive information and not disclosed.[7] Finally, shared accounts must be logged to manage individual accountability and must not include access to production systems.[8]

This occurred because [redacted] Furthermore, the Postal Service discloses passwords for standard and privileged access to the [redacted], which is accessible to anyone on the Postal Service intranet. [redacted]

> **Recommendation #1:** The **Vice President, Engineering Systems,** [redacted]

[2] For the purpose of this report, "credentials" refers to usernames and passwords.
[3] The normal operation mode used to remotely access [redacted].
[4] The advanced operation mode designed to restrict access to commands that can have adverse effects on the [redacted].
[5] [redacted]
[6] Privileged accounts (e.g., administrator or maintenance accounts) allow access to users to change data, alter configuration settings, run programs, or permits unrestricted access to view data.
[7] [redacted].

Recommendation #2: The **Vice President, Engineering Systems,** remove [redacted].

Recommendation #3: The **Vice President, Engineering Systems,** change [redacted].

Network Device Controls

The Postal Service does not have [redacted] We identified [redacted] that were inaccessible[10] because of a [redacted] Network administrators could not [redacted].

Postal Service policy[11] states that information resources must be able to generate event logs whenever a MPE/MHE device is connected to the Postal Service infrastructure. Additionally, best practices[12] recommend identifying and verifying users prior to granting access to the network.

This occurred because the [redacted].

[redacted] In addition, when activities are not appropriately logged, it limits the Postal Service's ability to investigate the cause of malfunctions or compromises.

Recommendation #4: The **Vice President, Engineering Systems,** update the [redacted].

[redacted]

[12] *Cisco Security Architecture for the Enterprise (SAFE) Reference Guide, Network Foundation Protection, Enforce Authentication, Authorization and Accounting (AAA),* dated October 2013.

Unencrypted Communication Protocols

[redacted]. Best practices[13] recommend the use of a secure protocol, such as Secure Shell[14] so that usernames and passwords are encrypted.

This occurred because the [redacted]

> **Recommendation #5:** The **Vice President, Engineering Systems,** should upgrade the [redacted]

Management's Comments

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

Regarding recommendation 1, management is evaluating a replacement for the legacy [redacted] as part of the [redacted] Technology Refresh upgrade deployment. The target implementation date is [redacted]

Regarding recommendation 2, management will work with the Maintenance Technical Support Center to revise [redacted]. The target implementation date is [redacted]

Regarding recommendation 3, management will replace the legacy [redacted] with hardware that supports updates to the [redacted] The target implementation date is [redacted].

Regarding recommendation 4, management will replace the legacy [redacted] with hardware that will [redacted]. The target implementation date is [redacted]

Regarding recommendation 5, management will replace the legacy [redacted] with hardware that [redacted] The target implementation date is [redacted]

[13] *Cisco Guide to Harden Cisco IOS Devices, Secure Operations, Use Secure Protocols When Possible*, dated April 2017.
[14] A protocol that provides a secure remote access connection to network devices.

Evaluation of Management's Comments

OIG considers management's comments responsive to recommendations 1, 2, 4, and 5. We recognize the technology refresh includes updating the legacy [redacted]; however, based on the target implementation dates, management should consider compensating controls to [redacted].

Regarding recommendation 3, management should [redacted].

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. 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.

Appendix A: Management's Comments

MICHAEL J. AMATO
VICE PRESIDENT
ENGINEERING SYSTEMS

UNITED STATES POSTAL SERVICE

August 27, 2018

MONIQUE COLTER
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Management Alert – Access Issues Identified in the Mail Processing Environment (Report Number IT-MA-18-DRAFT)

Engineering Systems management has reviewed Inspector General (OIG) Draft Management Alert – Access Issues Identified in the Mail Processing Environment. In general, we agree with the recommendations.

[redacted]

The following is management's response to the numbered recommendations contained in the management alert:

Recommendation #1:
The **Vice President, Engineering Systems**, configure the [redacted]

Management's response:
Engineering Systems Management agrees with the Recommendation.

Prior to this audit, Engineering Systems began evaluating a replacement for the legacy switches as part [redacted]

Target Implementation Date:
[redacted]

Recommendation #2:
The **Vice President, Engineering Systems**, remove the [redacted] switch [redacted]

Management's response:
Engineering Systems Management agrees with the Recommendation.

Engineering Systems will work with the Maintenance Technical Support Center to revise [redacted].

8403 LEE HIGHWAY
MERRIFIELD, VA 22082-8101

Target Implementation Date:
[redacted]

Recommendation #3:
The **Vice President, Engineering Systems**, change the [redacted]

Management's response:
Engineering Systems Management partially agrees with the Recommendation.

As part of our technology refresh for the [redacted] the replacement hardware will [redacted]

Target Implementation Date:
[redacted]

Recommendation #4:
The **Vice President, Engineering Systems**, update the [redacted]

Management's response:
Engineering Systems Management partially agrees with the Recommendation.

As part of our technology refresh for the [redacted] the replacement hardware will [redacted]

Target Implementation Date:
[redacted]

Recommendation #5:
The **Vice President, Engineering Systems**, should [redacted]

Management's response:
Engineering Systems Management agrees with the Recommendation.

As part of our technology refresh for the [redacted] the replacement hardware will use [redacted]

Target Implementation Date:
October 1, 2019

Michael J. Amato
Vice President, Engineering Systems

08/27/2018
Date

cc: Vice President, Network Operations
Vice President, Chief Information Security Officer
Corporate Audit Response Management

8403 LEE HIGHWAY
MERRIFIELD, VA 22082-8101