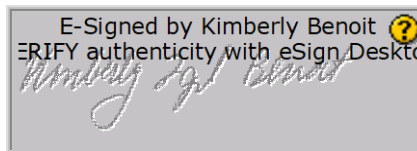




June 19, 2019

MEMORANDUM FOR: PRITHA N. MEHRA
ACTING VICE PRESIDENT, INFORMATION
TECHNOLOGY

GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY
OFFICER



FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Management Alert – [REDACTED]
(Report Number IT-MT-19-001)

This management alert presents an issue that came to our attention during the ongoing audit of the U.S. Postal Service's Response to an [REDACTED]. The objective of this management alert is to provide Postal Service officials immediate notification of the issue identified and recommend corrective actions. The issue requires immediate attention and remediation.

We identified these issues while conducting our performance audit in accordance with generally accepted government auditing standards. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

cc: Postmaster General
Chief Information Officer
Corporate Audit Response Management

Introduction

During the audit of the U.S. Postal Service's response to an [REDACTED], we found a security weakness in a portion of the [REDACTED] that was [REDACTED] information. This issue is outside the scope of the audit; however, it poses a security weakness that warrants management's immediate attention. We notified the Vice President, Chief Information Security Officer, on April 9, 2019, and met with the Manager, Cybersecurity Operations, on April 10, 2019, regarding this matter.

While reviewing [REDACTED] to determine if the Postal Service adequately remediated the vulnerability [REDACTED] we identified a portion of the [REDACTED] indicating that the [REDACTED] was [REDACTED]. This data was transmitted to the [REDACTED]

[REDACTED] The Postal Service uses [REDACTED] to maintain [REDACTED]

The objective of this alert is to notify the Postal Service of [REDACTED]
[REDACTED]

[REDACTED]

The Postal Service is [REDACTED] We identified [REDACTED] results that contained [REDACTED] from a query of [REDACTED]. The results included [REDACTED]
[REDACTED]

Since the Postal Service [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

Postal Service policy requires there be security controls sufficient to satisfy baseline security requirements in all information resources. Additional security is required to adequately protect the [REDACTED]. Storing customer and employee [REDACTED].

[REDACTED]

Additionally, [REDACTED]. Exposure of this [REDACTED] could have a serious negative impact to the Postal Service brand. Additionally, the [REDACTED].

[REDACTED]

We are currently working to determine the number of Postal Service employees and contractors who have access to [REDACTED] and how it may have been used.

Recommendation #1: We recommend the **Vice President, Chief Information Security Officer**, determine the source, purpose, and root cause of [REDACTED].

Recommendation #2: We recommend the **Acting Vice President, Information Technology**, immediately remove or encrypt and limit access to indexes containing [REDACTED].

[REDACTED]

Recommendation #3: We recommend the **Acting Vice President, Information Technology**, require users to [REDACTED].

[REDACTED]

Recommendation #4: We recommend the **Vice President, Chief Information Security Officer**, determine if [REDACTED] was accessed or exported and, if so, implement incident response protocols.

[REDACTED]

Management's Comments

Management generally agreed with the findings and recommendations in the alert.

Regarding recommendation 1, management agreed to complete a formal After Action Report to remediate the source, purpose, and root cause for [REDACTED]. Management included the After Action Report with a request to close out this recommendation. The target implementation date is June 30, 2019.

Regarding recommendation 2, management agreed to [REDACTED]. [REDACTED] CISO will complete this validation. The target implementation date is June 30, 2019.

Regarding recommendation 3, management agreed they will [REDACTED] by July 20, 2019 and notify [REDACTED] of the option to [REDACTED] by September 30, 2019. The target implementation date is September 30, 2019.

Regarding recommendation 4, management agreed and stated that no [REDACTED] were observed of the [REDACTED]. Management included details of the activities performed to determine whether [REDACTED] of concern occurred in the After Action Report, which was submitted with the request to close out this recommendation. The target implementation date is June 30, 2019.

See [Appendix A](#) for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments generally responsive to all recommendations. Postal Service management provided the After Action Report as resolution of recommendations 1 and 4. The OIG agrees to immediate closure of recommendation 1 upon report issuance. However, additional information is required to close recommendation 4.

The remaining 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



June 7, 2019

Lazerick C. Poland
Director, Audit Operations

SUBJECT: Management Alert – [REDACTED]
(Report Number IT-MT-19-DRAFT)

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) [REDACTED] Management Alert. Postal management is dedicated to the continuous safe-guarding and modernization of our information security framework to better protect customers, employees, and the enterprise data.

Management understands the intent of the draft report is to inform and help improve the overall security posture and capabilities for strengthening security controls in all information. Management generally agrees with the findings of the audit. Management has taken proactive steps to address and remediate the [REDACTED]. Management looks forward to working in partnership with the Postal Service Office of the Inspector General to advance leading practices throughout the enterprise.

Management is providing the following response to address the findings and recommendations cited in the Management Alert – [REDACTED]

Recommendation [1]:

We recommend the Vice President, Chief Information Security Officer determine the source, purpose, and root cause of [REDACTED]

Management Response/Action Plan:

Management agrees with this recommendation. The CISO department has completed a formal After Action Report against the findings, analysis and actions taken to remediate the source, purpose and root cause of [REDACTED]. Management is requesting closure of this recommendation upon delivery of the After Action Report.

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

-2-

Target Implementation Date:
June 30, 2019

Responsible Official:
Vice President, Chief Information Security Officer

Recommendation [2]:
We recommend the Acting Vice President, Information Technology, immediately remove or encrypt and limit access to indexes containing [REDACTED]

Management Response/Action Plan:
Management agrees with recommendation #2. USPS has [REDACTED] CISO will complete validation.

Target Implementation Date:
June 30, 2019

Responsible Official:
Acting Vice President, Information Technology

Recommendation [3]:
We recommend the Acting Vice President, Information Technology, require [REDACTED]

Management Response/Action Plan:
Management agrees with the intent of the recommendations, however there was [REDACTED]
As part of our regular security initiatives [REDACTED] will be changed by July 20th. [REDACTED] will be notified of the [REDACTED] change option by September 30th.

Target Implementation Date:
September 30, 2019

-3-


Responsible Official:
Acting Vice President, Information Technology

Recommendation [4]:
We recommend the Vice President, Chief Information Security Officer, determine if [REDACTED] was accessed or exported and, if so, implement incident response protocols.

Management Response/Action Plan:
Management agrees with and has confirmed no [REDACTED] of concern were observed as documented in the After Action Report. Management is requesting closure of this recommendation upon delivery of the After Action Report.

Target Implementation Date:
June 30, 2019

Responsible Official:
Vice President, Chief Information Security Officer



Pritha N. Mehra
Acting Vice President, Information Technology



Gregory S. Crabb
Vice President, Chief Information Security Officer

cc: copy those that were copied on the OIG draft audit report, plus
Manager, Corporate Audit Response Management