



# OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

## System Vulnerability Assessment

### Audit Report

Report Number  
IT-AR-17-004

April 7, 2017







# OFFICE OF INSPECTOR GENERAL

## UNITED STATES POSTAL SERVICE

### Highlights

*While the Postal Service has made efforts to improve the security of the travel voucher system, opportunities exist to strengthen the system's security posture.*

### Background

The U.S. Postal Service's electronic travel voucher system, is a web-based travel system used by about [REDACTED] employees. The system allows employees and managers to, respectively, create and approve travel vouchers online. [REDACTED]

[REDACTED] During fiscal year 2016, the system processed over [REDACTED] travel vouchers totaling [REDACTED] million.

In order for travel voucher payments to be accurate and timely, the system must be secured to ensure the confidentiality, integrity, and availability of system resources. The Confidentiality, Integrity, and Availability Triad is a model designed to guide policies for information security within an organization and its three elements are regarded as the most crucial to security.

Our objective was to assess travel voucher system servers and databases to determine whether they comply with current Postal Service security requirements and industry best practices; and whether they pose a risk to the confidentiality, integrity, and availability of the system.

### What the OIG Found

While the Postal Service has made efforts to improve the security of the travel voucher system, opportunities exist to strengthen the system's security posture. Specifically, we found [REDACTED] unique vulnerabilities on the servers and databases that adversely impact the confidentiality, integrity, and availability of the system. [REDACTED] of the [REDACTED] were critical vulnerabilities, but [REDACTED] of those can be corrected with a software upgrade. The remaining [REDACTED], while critical, do not pose an immediate threat to the system.

[REDACTED] of the [REDACTED] servers and databases comprising the travel voucher system were not secured in accordance with current Postal Service information security requirements and industry best practices. Specifically, risks to system confidentiality exist because data can be sent and received through insecure connections. System integrity and availability could be impacted by [REDACTED] operating systems running vulnerable software versions.

We also found servers and databases that were placed into the production environment prior to having approved security standards. Specifically, we identified [REDACTED] servers running a [REDACTED] operating system that was secured using [REDACTED] standards, which were not all compatible and lacked the enhanced security features of newer releases. Also, databases were configured using Postal Service security standards designed for prior database versions.



# OFFICE OF INSPECTOR GENERAL

## UNITED STATES POSTAL SERVICE

These issues occurred because management did not provide appropriate oversight to ensure the required system configurations were applied, and management did not implement approved security standards because they are still testing the settings to ensure system compatibility.

These vulnerabilities could increase the risk of unauthorized disclosure of sensitive data, data corruption, and denial of service and could adversely impact the confidentiality, integrity, and availability of the travel voucher system.

### What the OIG Recommended

We recommended management configure servers and databases that comprise the travel voucher system according to requirements outlined in Handbook AS-805, *Information Security*, requirements and platform-specific security standards. We also recommended management review software installed on the [REDACTED] operating systems hosting the travel voucher system and remove or update vulnerable software. Management should also develop and issue enterprise-wide security standards for the [REDACTED] operating system.

# Transmittal Letter



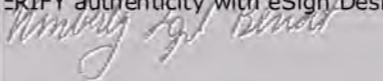
OFFICE OF INSPECTOR GENERAL  
UNITED STATES POSTAL SERVICE

April 7, 2017

**MEMORANDUM FOR:** JEFFREY C. JOHNSON  
VICE PRESIDENT, INFORMATION TECHNOLOGY

MAURA A. MCNERNEY  
VICE PRESIDENT, CONTROLLER

GREGORY S. CRABB  
CHIEF INFORMATION SECURITY OFFICER AND  
VICE PRESIDENT, DIGITAL SOLUTIONS

E-Signed by Kimberly Benoit  
VERIFY authenticity with eSign Desktop  


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

**SUBJECT:** Audit Report – System Vulnerability Assessment  
(Report Number IT-AR-17-004)

This report presents the results of the System Vulnerability Assessment  
(Project Number 16TG019IT000).

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

Attachment

cc: Corporate Audit and Response Management  
Deputy Chief Information Security Officer  
Manager, Cybersecurity Engineering  
Manager, Computer Operations

# Table of Contents

Cover	
Highlights.....	1
Background.....	1
What the OIG Found.....	1
What the OIG Recommended.....	2
Transmittal Letter.....	3
Findings.....	5
Introduction.....	5
Summary.....	6
System Vulnerabilities and Compliance Settings.....	6
Approved Security Standards.....	8
Other Matters.....	8
Recommendations.....	9
Management’s Comments.....	9
Evaluation of Management’s Comments.....	10
Appendices.....	11
Appendix A: Additional Information.....	12
Background.....	12
Objective, Scope, and Methodology.....	12
Prior Audit Coverage.....	13
Appendix B: Management’s Comments.....	14
Contact Information.....	19



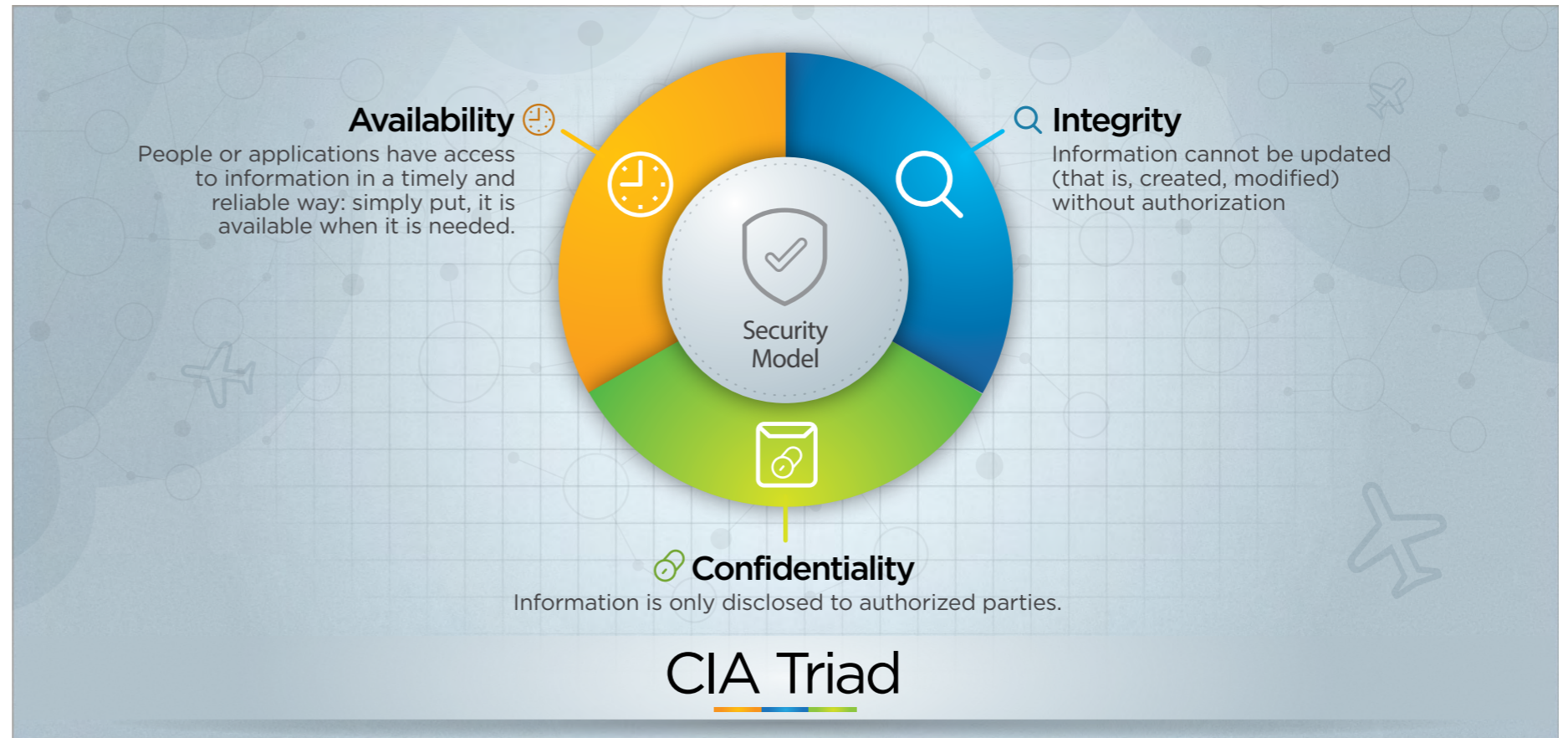
# Findings

## Introduction

This report presents the results of our self-initiated vulnerability assessment of the U.S. Postal Service's electronic travel voucher system (Project Number 16TG019IT000). Our objective was to assess travel voucher system servers and databases to determine whether they comply with current Postal Service security requirements and industry best practices and whether they pose any risk to the confidentiality, integrity, and availability of the system. See [Appendix A](#) for additional information about this audit.

The Postal Service's travel voucher system is a web-based travel request and voucher reimbursement management system that supports about [REDACTED] employees and managers and allows them to, respectively, create and approve travel vouchers. [REDACTED]. However, the system does not contain credit card information.

Safeguarding information resources is essential to maintaining the trust of the Postal Service's customers and ensuring these resources are available is critical to business continuity. The Confidentiality,<sup>2</sup> Integrity,<sup>3</sup> and Availability<sup>4</sup> Triad is a model designed to guide policies for information security within an organization and its three elements are regarded as the most crucial to security. We performed this vulnerability assessment to determine what risks in these areas exist for the system.



- 1 Any data that could potentially identify a specific individual.
- 2 A set of rules that limits access to information.
- 3 The assurance that the information is trustworthy and accurate.
- 4 A guarantee of reliable access to the information by authorized people.

***For the [REDACTED] components scanned, we identified [REDACTED] unique vulnerabilities that present either a critical, high, or medium risk that could impact system functionality and data integrity if exploited.***

## Summary

While the Postal Service has made efforts to improve the security of its travel voucher system, opportunities exist to strengthen the system's security posture. Specifically, [REDACTED] of [REDACTED] servers and databases comprising the system were not secured in accordance with current Postal Service information security requirements and industry best practices. We also found [REDACTED] unique<sup>5</sup> vulnerabilities and non-compliant settings on the servers and databases we scanned. In addition, we found servers and databases that were placed into the production environment before they had approved security standards for [REDACTED] and [REDACTED].

These issues occurred because Computer Operations management did not provide appropriate oversight to ensure required system configurations were applied.

In addition, management did not have approved security standards<sup>6</sup> because the Corporate Information Security Office (CISO) is still testing settings to ensure system compatibility.

These vulnerabilities adversely impact the confidentiality, integrity, and availability of the travel voucher system. Compromise of the system could result in [REDACTED], inability to process travel requests, and delays in payment of travel vouchers.

## System Vulnerabilities and Compliance Settings

Servers and databases comprising the travel voucher system were not appropriately secured and were not in compliance with current Postal Service security requirements and industry best practices.<sup>7</sup> For the [REDACTED] components scanned, we identified [REDACTED] unique vulnerabilities that present either a critical, high, or medium risk that could impact system functionality and data integrity if exploited.

For example, we found:

- The web application uses an insecure encryption version [REDACTED] for moving data across the network.
- Outdated anti-virus software installed on servers running [REDACTED] operating systems.
- Database settings that allow data to be sent and received through insecure connections.

Table 1 shows a summary of the critical, high, and medium-risk vulnerabilities identified.

<sup>5</sup> The number of single instances, by application, of identified vulnerabilities. Some vulnerabilities may exist on multiple servers and databases.

<sup>6</sup> Postal Service security standards provide the requirements for ensuring all unnecessary services are disabled, security-related patches are applied, configuration settings are set up correctly, and additional measures are taken.

<sup>7</sup> Handbook AS-805, *Information Security*, Section 10-2.3.1, Hardening Servers, and Section 8-2.4.4, Patch Management, dated May 2015. Security Standards for [REDACTED]

After we notified management of these vulnerabilities, system administrators took corrective action to remediate [REDACTED] of the [REDACTED] vulnerabilities.

**Table 1. System Vulnerabilities by Level of Severity**

System	Number of Systems Scanned	Vulnerabilities by Level of Severity			Total Unique Vulnerabilities
		Critical	High	Medium	
[REDACTED]	1	1	1	1	1
[REDACTED]	1	1	1	1	1
[REDACTED]	1	1	1	1	1
[REDACTED]	1	1	1	1	1
[REDACTED]	1	1	1	1	1

Source: U.S. Postal Service Office of Inspector General (OIG) Nessus, GFI Languard, HP WebInspect, and AppDetective scanning tool results.

These vulnerabilities occurred because management did not provide ongoing oversight to ensure appropriate system configurations were applied. Specifically, an outdated version of [REDACTED] accounted for [REDACTED] percent of the vulnerabilities for the [REDACTED] operating system. In addition, some software updates were not applied because the Information Technology Engineering and Architecture group had not completed testing of the settings to ensure system compatibility.

[REDACTED] Compromise of these vulnerabilities could also put the availability of the system at risk by allowing unauthorized changes to the system or disruption of service.

After we notified management of these vulnerabilities, system administrators took corrective action to remediate [REDACTED] of the [REDACTED] vulnerabilities:

- [REDACTED] critical-risk and four high-risk vulnerabilities for [REDACTED]
- [REDACTED] medium-risk vulnerabilities relating to the web application and insecure encryption
- [REDACTED] medium-risk vulnerabilities relating to [REDACTED]

8 OIG WebInspect scans identified a critical vulnerability on the travel voucher web page. The Postal Service was aware of the vulnerability from prior internally conducted scans and intends to fix it. Based on the Postal Service’s existing knowledge of the critical vulnerability, we will not make a recommendation for it.



***If outdated hardening standards are used to configure the travel voucher system servers and databases, the system could be susceptible to vulnerabilities that are not accounted for in the outdated hardening standards.***

## Approved Security Standards

Management did not have approved security standards (referred to as “hardening standards”) in place prior to placing travel voucher system servers and databases into production, as required by policy.<sup>9</sup> Specifically, we identified:

- [REDACTED] operating systems that were secured using [REDACTED] security standards. We identified [REDACTED] configuration settings that did not comply with these standards. Also, the [REDACTED] operating system has features that are not in the [REDACTED] standards, such as a more restrictive maximum password age of [REDACTED], a maximum password length of [REDACTED] characters, and enhanced features for [REDACTED] and [REDACTED].
- [REDACTED] databases were configured using Postal Service security standards designed for prior database versions.<sup>12</sup> Management has not approved an [REDACTED] security standard.

This occurred because the [REDACTED] security standard is still in draft and undergoing testing to ensure the settings are compatible. Further, [REDACTED] databases were configured using security standards for a previous version because CISO has not approved security standards for the current [REDACTED] version. If outdated hardening standards are used to configure the travel voucher system servers and databases, the system could be susceptible to vulnerabilities that are not accounted for in the outdated hardening standards.

## Other Matters

During our audit, it came to our attention that management did not track and decommission assets timely.<sup>13</sup> We identified four servers running the [REDACTED] operating system that were assigned to the travel voucher system production environment in May 2014. Although these assets were accounted for under the travel voucher system inventory, they were not used for over two years and were only decommissioned in response to this audit. This delay occurred because business owners opted to migrate directly from [REDACTED] to [REDACTED] and did not coordinate the decommissioning of these servers.

Decommissioning unused servers reduces costs and eliminates a prime target for hackers, who could exploit them for distributed-denial-of-service attacks, sending spam, or staging points for the exfiltration of stolen data. In response to our audit, the Postal Service performed corrective action by decommissioning unused servers running [REDACTED].

<sup>9</sup> Handbook AS-805, Section 10-2.3.1, Hardening Servers.

<sup>10</sup> Allows for advanced firewall configuration settings.

<sup>11</sup> Enables administrators to apply access-control permissions and restrictions based on well-defined rules.

<sup>12</sup> Security Hardening Standards [REDACTED]

<sup>13</sup> Handbook AS-805, Section 8-2.4.1, Configuration Component Inventory.

# Recommendations

***We recommend management configure servers and databases that comprise the travel voucher system according to requirements, review software installations, and remove or update vulnerable software.***

We recommend the Vice President, Information Technology, direct the Manager, Computer Operations, to:

1. Configure the travel voucher [REDACTED] operating systems according to Handbook AS-805, *Information Security*, requirements and approved platform specific security standards.
2. Review installed software on travel voucher servers hosting the [REDACTED] operating systems and apply current security updates.
3. Configure the travel voucher system database servers according to Handbook AS-805, *Information Security*, requirements and approved platform-specific security standards.

We recommend the Chief Information Security Officer and Vice President, Digital Solutions, direct the Manager, Cybersecurity Engineering, to:

4. Finalize testing and issue enterprise-wide hardening standards for the [REDACTED] operating systems.
5. Develop and issue enterprise-wide hardening standards for the [REDACTED] databases.

## Management's Comments

Management agreed with the findings and recommendations in the report and stated they have begun to take corrective action.

Regarding recommendation 1, management is currently finalizing the [REDACTED] Hardening Standards. Once finalized, Enterprise Access Infrastructure will configure the travel voucher [REDACTED] operating systems in accordance with the finalized hardening standards. Management plans to complete these actions by September 30, 2017.

Regarding recommendation 2, management plans to apply the recommended security updates for the travel voucher servers in the next change release by April 30, 2017.

Regarding recommendation 3, management has finalized [REDACTED] database hardening standards and is in the process of configuring the travel voucher system [REDACTED] databases accordingly. Management plans to complete these actions by September 30, 2017.

Regarding recommendation 4, management has drafted [REDACTED] hardening standards. [REDACTED] has reviewed the draft, which is based on best practices from the National Institute of Standards and Technology and Defense Information Systems Agency's *Security Technical Implementation Guide*. The hardening standards are currently undergoing testing. A risk acceptance letter is also being drafted until additional updates can be issued and distributed enterprise-wide. Management plans to complete these actions by June 30, 2017.

Regarding recommendation 5, management stated they have developed and issued enterprise-wide hardening standards for the [REDACTED] databases. Management stated they have completed the actions for this recommendation and requested closure upon issuance of the final report.

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 the corrective action proposed should resolve the issues identified.

Regarding recommendation 5, management has provided us a copy of the hardening standards for [REDACTED] databases, but has not provided support showing they have distributed these standards enterprise-wide. Therefore, this recommendation will remain open until we receive support showing these standards have been distributed.

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.



# Appendices

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

Appendix A: Additional Information.....	12
Background .....	12
Objective, Scope, and Methodology .....	12
Prior Audit Coverage.....	13
Appendix B: Management's Comments .....	14

## Appendix A: Additional Information

### Background

The Postal Service relies solely on its travel voucher system to process travel requests and reimburse travel expenses. The travel voucher system is a web-based travel and expense voucher management system that is [REDACTED]. This system is owned and maintained by the Postal Service's chief financial officer and executive vice president, and is part of the Finance Relationship Management portfolio. The travel voucher system allows employees and managers to, respectively, create and approve travel vouchers online through the web browser at their workstation.

This system should be appropriately secured to ensure the confidentiality, integrity, and availability of system data and resources. Interruptions in system availability could cause delays for employees requesting travel expense reimbursement. In fiscal year 2016, the system processed [REDACTED] travel vouchers totaling [REDACTED].

The OIG conducts security vulnerability assessment tests to ensure computer systems provide an appropriate level of security commensurate with the criticality of the system and the information contained on the system. The tools used to perform the vulnerability scans are AppDetective,<sup>14</sup> GFI Languard,<sup>15</sup> HP WebInspect,<sup>16</sup> and Nessus.<sup>17</sup>

### Objective, Scope, and Methodology

The objective of this audit was to assess the security of the servers and databases comprising the travel voucher system and to determine if they comply with current Postal Service's security requirements and industry best practices to ensure the confidentiality, integrity, and availability of the system. We limited the scope of our scans to production servers and databases comprising the travel voucher system application. In addition, we used the Postal Service's customer acceptance testing (CAT) environment to scan the web application to prevent disruption to the production environment.

In order to accomplish our objective, we:

- Obtained and reviewed Postal Service policies, procedures, and security standards relevant to this audit.
- Extracted data for servers and databases comprising the travel voucher system from network diagrams, [REDACTED]. We used this information to identify the system attributes, IP address subnet ranges, asset inventory, and other relevant information.
- Used information from the Information Technology Performance and Risk Information System Risk Model to determine if the travel voucher system was affected by any known security incidents or malware.

---

14 Database vulnerability assessment software used to identify and remediate vulnerabilities, configuration errors, rogue installations, and access issues in database deployments.

15 A network security scanner and patch management tool that allows the ability to scan, detect, assess, and rectify security vulnerabilities.

16 An automated and configurable web application security and penetration testing tool that mimics real-world hacking techniques and attacks, enabling the user to thoroughly analyze complex web applications and services for security vulnerabilities.

17 A vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.

[REDACTED]

[REDACTED]

[REDACTED]

- Performed automated scans using Nessus, GFI Languard, HP WebInspect, and AppDetective on the [REDACTED] servers and databases that comprise the travel voucher system. Prior to conducting the scans, we tested the tools in the CAT environment.
- Analyzed scan results and compared them to Postal Service policies and industry best practices to measure compliance and identify vulnerabilities on resources supporting the travel voucher system.
- Identified Center for Information Security best practices to configure scanning tools where specific Postal Service criteria was not in place.
- Leveraged advanced techniques to analyze data using tools such as PERL, MySQL, Microsoft SQL, and Excel to generate our results. Based on our analysis, we determined the severity ranking and Common Vulnerabilities and Exposures (CVE) and mapped them to the Confidentiality, Integrity, and Availability Triad.
- Provided the data analysis to appropriate Postal Service management. We conducted interviews with Postal Service management to determine the root cause for non-compliance with Postal Service policy and identified potential compensating controls for the confirmed vulnerabilities.

We conducted this performance audit from September 2016 through April 2017, 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 February 27, 2017, and included their comments where appropriate.

We assessed the reliability of computer-generated data by reviewing related documentation, interviewing knowledgeable Postal Service officials, reviewing related internal controls, and analyzing scan data. We determined that the data was 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.



## Appendix B: Management's Comments



March 28, 2017

LORI LAU DILLARD  
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: ██████████ Vulnerability Assessment (IT-AR-17-DRAFT), Project Number 16TG019IT000

Thank you for the opportunity to respond to the ██████████ Vulnerability Assessment audit report. The Postal Service prioritizes the protection of customers' and employees' Personally Identifiable Information (PII) and the integrity of its information systems. Management's focus and commitment is demonstrated by the implementation of a multi-year transformation effort to modernize the existing information security framework. As we continue to upgrade our IT assets and system controls, management's primary focus is to better protect customers, employees, and the enterprise from present-day and future threats. The ██████████ Vulnerability Assessment audit helps to facilitate the realization of this goal shared by stakeholders across the Postal Organization.

Management agrees with the findings in this audit report, understanding the intent of this engagement is to assess the design and operating effectiveness of the ██████████ system. As detailed below, prior to the issuance of the ██████████ audit, management took proactive steps to comply with current Postal Service security requirements and industry leading practices. Actions taken to date are as follows:

1. As part of efforts to modernize the information security framework, the Postal Service stood up Initiative #14 (Asset, Change, and Configuration Management) to prioritize cybersecurity as it relates to change and configuration management. This initiative devotes resources to developing and adapting plans to ensure that networked systems operate in accordance with approved configurations.
2. While the audit was ongoing, management took steps to decrease risk exposure to the Postal Organization by promptly remediating critical deficiencies. As a result, the Postal Service resolved 25% of identified vulnerabilities during the engagement. Remediation of the remaining vulnerabilities is in process.

The Postal Service's commitment to protecting PII and maintaining the integrity of its information systems and assets is unwavering. Management looks forward to working in partnership with the Postal Service Office of the Inspector General to advance leading practices throughout the enterprise.

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

Recommendation [1]:

Configure the [REDACTED] operating systems according to Handbook AS-805, Information Security, requirements and approved platform specific security standards.

Management Response/Action Plan:

Management agrees with this recommendation. Cybersecurity Engineering (CISO) is in the process of finalizing the [REDACTED] Hardening Standard. As a result, Enterprise Access Infrastructure will align [REDACTED] server settings to the hardening standard and document approved exceptions, where applicable.

Target Implementation Date:

September 30, 2017

Responsible Official:

Vice President, Information Technology

Recommendation [2]:

Review installed software on [REDACTED] servers hosting the [REDACTED] operating systems and apply current security updates.

Management Response/Action Plan:

Management agrees with this recommendation. Business Relationship Management and Computer Operations will apply updates to [REDACTED] and [REDACTED] in the next change release.

Target Implementation Date:

April 30, 2017

Responsible Official:

Vice President, Information Technology

Recommendation [3]:

Configure the [REDACTED] database servers according to Handbook AS-805, Information Security, requirements and approved platform-specific security standards.

Management Response/Action Plan:

Management agrees with this recommendation. Cybersecurity Engineering (CISO) has finalized the [REDACTED] Database Hardening Standard. Computer Operations (IT) is in the process of aligning the [REDACTED] databases with new entries in the [REDACTED] Database Hardening Standard as well as the database items identified in the OIG report (specifically Table 4).

Target Implementation Date:

September 30, 2017

Responsible Official:

Vice President, Information Technology

Recommendation [4]:

Finalize testing and issue enterprise-wide hardening standard for the [REDACTED] operating systems.

Management Response/Action Plan:

Management agrees with the intent of this recommendation. CISO has a draft of [REDACTED] that has been reviewed by [REDACTED] and leverages NIST and the DISA STIG. All settings are at NIST or higher and we are going through a final validation of the settings. USPS is also leveraging a new testing tool to test the standard and will complete the testing by implementation date. In addition, a Risk Acceptance Letter (RAL) is being created until additional updates are issued and distributed enterprise-wide.

Target Implementation Date:

June 30, 2017

Responsible Official:

Chief Information Security Officer & Digital Solutions, Vice President

Recommendation [5]:

Develop and issue enterprise-wide hardening standards for the [REDACTED] databases.

Management Response/Action Plan:

Management agrees and has already completed this recommendation. CISO has developed, issued, and distributed enterprise-wide hardening standard for the [REDACTED] databases. Management requests closure of the recommendation with issuance of the final audit report.



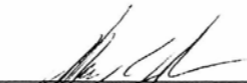
- 4 -

Target Implementation Date:

March 16, 2017


Responsible Official:

Chief Information Security Officer & Digital Solutions, Vice President



---

Jeffrey C. Johnson  
Vice President, Information Technology



---

Maura A. McNerney  
Vice President, Controller



---

Gregory S. Crabb  
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.  
Stay informed.

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